February 5, 2015

©2015 AccessData Group, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

For the latest FAQ content, see https://support.accessdata.com/hc/en-us/articles/204123005-MPE-FAQ

For more information, contact Support at support@accessdata.com or 800-658-5199.
# Table of Contents

Mobile Forensics Background Knowledge .............................................................................................................. 3  
System Requirements .................................................................................................................................................. 4  
Licensing ................................................................................................................................................................. 5  
Installing & Running MPE+ ......................................................................................................................................... 6  
MPE+ nFIELD ............................................................................................................................................................. 8  
MPE+ Velocitor ............................................................................................................................................................ 10  
Drivers....................................................................................................................................................................... 13  
Cables ......................................................................................................................................................................... 14  
Phones .......................................................................................................................................................................... 15  
SIM Cards ................................................................................................................................................................. 16  
Android Devices .......................................................................................................................................................... 18  
Apple Devices ............................................................................................................................................................. 24  
BlackBerry Devices ..................................................................................................................................................... 33  
iDEN Devices ............................................................................................................................................................. 34  
Windows Mobile Devices .......................................................................................................................................... 35  
General Troubleshooting .......................................................................................................................................... 37
Mobile Forensics Background Knowledge

What is the difference between Computer Forensics and Mobile Phone Forensics?
In computer forensics, the devices that we are imaging are static storage devices; this means that with we will obtain the same image every time. In mobile phone forensics, the devices that we are imaging are full dynamic systems; this means that, while we may support the phone, we might only extract the contacts, SMS, and call logs but not the calendar or any other combination of this information. This may come as a shock to many customers that have never dealt with any mobile forensic software or haven’t had any type of mobile forensic training; but for those customers that understand mobile phone forensics, they should only see MPE+ as a tool that can help them fill the voids of other software they use and become their main tool.

What is CDMA?
CDMA stands for Code Division Multiple Access and is a cellular technology used for communication. CDMA is usually only used in the USA. CDMA phones typically do not use SIM cards, unless they are world phones (which rely on GSM technology outside of the USA). More information about CDMA can be obtained at http://en.wikipedia.org/wiki/Code_division_multiple_access.

What is GSM?
GSM stands for Global System for Mobile Communications and is a worldwide standard for cellular communication. GSM phones use SIM cards, whether externally accessible or not. More information about GSM can be obtained at http://en.wikipedia.org/wiki/GSM.
System Requirements

What Operating Systems are supported by MPE+?

- Windows XP Professional, 32-bit only
- Windows 7, 32- and 64-bit (not "Starter" edition)
- Windows 8, 32- and 64-bit (not "RT" edition)
- Windows 8.1, 32- and 64-bit (not "RT" edition)

Window Server iterations are not supported

What prerequisites must I install manually before installing MPE+?

In general, most prerequisites are installed automatically.

On Windows XP Professional, you will need to manually install MSMQ (Microsoft Message Queuing) as per the following instructions:

1. In Control Panel, double-click Add/Remove Programs.
2. On the left tab of the Add/Remove Programs window, click Add/Remove Windows Components.
3. Once the Windows Components Wizard opens, click to select "Message Queuing" and click Next.
4. This will start the MSMQ setup process. You may be prompted to provide your Windows XP installation CD-ROM for the necessary installation files.

Licensing

How do I move my MPE+ installation to a different computer?
If your MPE+ license is stored on a physical CodeMeter dongle, you can simply install MPE+ and the CodeMeter software on another PC and connect the dongle to that PC when you wish to run MPE+.

If your MPE+ license is stored in a Virtual CodeMeter (usually the case with the MPE+ tablet) you will first need to move your MPE+ license to a physical CodeMeter dongle through the following steps:

1. Make sure the machine with the Virtual CodeMeter is connected to the internet.
2. Open AccessData License Manager.
3. Under the Licenses tab, select the checkbox next to the entry for "FTK Mobile Phone Examiner".
4. Click "Remove License" and click "Yes" when prompted.
5. On another PC, make sure you are connected to the internet and insert a physical CodeMeter dongle.
6. Open AccessData License Manager.
7. Under the Licenses tab, click "Add Existing License".
8. On the web page that opens up, select the checkbox next to the unbound "Mobile" license.
9. Click "Bind", then switch back to License Manager and click "Yes" when prompted.
Installing & Running MPE+

How do I uninstall MPE+ 5.5.5 and earlier?
The following will allow you to cleanly uninstall MPE+.

1. Uninstall "Mobile Phone Examiner" via the Control Panel
2. Reboot
3. Delete the "%USERPROFILE%\AppData\Local\Apps\2.0" folder (make sure you don’t accidentally delete other Click-Once software)
4. Delete the "%USERPROFILE%\AppData\Local\Local\mpetempdata" folder (or any other location assigned as the MPE+ temp folder)
5. Delete the "%USERPROFILE%\AppData\Roaming\AccessData" folder
6. Delete the "%PROGRAMDATA%\AccessData\MPE" folder
7. If it exists, delete "%PROGRAMDATA%\AccessData\Products\Common\NLMPreferences.xml"

How do I install MPE+?
1. If you are upgrading from a previous version, manually uninstall the previous version using the Windows Control Panel.
2. To install MPE+, follow the instructions in the Quick Install Guide.
3. Set the proper exceptions before restarting your anti-virus.

Notes:
- If you originally performed an online installation of MPE+, but moved your PC offline before installing all needed drivers, you will need to manually import the drivers from the MPE+ DVD/ISO. From the Options menu, click "Import Driver" and point to [DVD]\Setup\Drivers\[OSversion]
- If you are prompted to reboot your PC during the installation, please choose to restart later and then restart your PC after MPE+ has run for the first time.
- Please pay attention to warnings and popups and make sure to allow any and all drivers to install.
- Some driver prompts may be covered by the MPE+ splash screen or window, so you should pay attention for installers showing up in the Task Bar.
- If you choose to reboot your PC or disallow any drivers to be installed, you may need to manually restart/resume the installation process.

How do I remove the MPE+ Tablet software?
1. Uninstall "MPE+ Tablet" or "Tablet Mobile Phone Examiner" via the Control Panel
2. Reboot
3. Delete the "%USERPROFILE%\AppData\Local\Apps\2.0" folder
4. Delete the "%USERPROFILE%\AppData\Local\Local\mpetempdata" folder (or any other location assigned as the MPE+ temp folder)
5. Delete the "%USERPROFILE%\AppData\Roaming\AccessData" folder
6. Delete the "%PROGRAMDATA%\AccessData\MPE" folder  
7. Reboot

**What is the importance of the MPE+ TEMP folder and where should I put it?**
During extraction and/or analysis, all extracted data is stored in the MPE+ TEMP folder. Due to how this data is stored, the TEMP folder may contain several times the amount of data as the device itself or the AD1 image. You should put the TEMP folder should be placed on the drive with the most free space, preferably with 100GB free space or more. MPE+ will not work properly if the TEMP folder runs out of space during extraction.

For MPE+ nFIELD, the TEMP folder will automatically be placed on the selected destination drive during extraction. The destination drive should be at least 3 times the size of the device being extracted.

**How do I change the location of my MPE+ TEMP folder?**

*MPE+:*
1. Click "Settings" under the Options menu.  
2. Click the button next to the "Temporary Data Path" field to select a new location  
3. Click "OK"

*MPE+ nFIELD:*
The TEMP folder will automatically be placed on the selected destination drive during extraction
MPE+ nFIELD

What is the MPE+ nFIELD?
MPE+ nFIELD is a new, simplified replacement for the MPE+ Tablet software, and provides the following features:

- Simplified interface with touchscreen support
- Extractions for mobile devices, SIM cards, and mass storage devices/cards
- Automatic export of images and PDF reports (if applicable) to Removable Storage
- Built-in report viewing
- Created images are fully compatible with MPE+ for review

MPE+ nFIELD can be downloaded [here](http://accessdata.com/product-download/digital-forensics). To obtain a license for MPE+ nFIELD, please contact Sales at 800-574-5199.

How do I install MPE+ nFIELD?
1. Ensure the latest versions of CodeMeter Runtime and License Manager are installed
2. Ensure your CodeMeter dongle is connected and has a current MPE+ nFIELD license
4. Insert the MPE+ nFIELD DVD or mount the ISO
5. If setup does not start automatically, run the included "autorun.exe" from the DVD/ISO
6. Select "Install MPE+ nFIELD"
7. Let the installer run all the way through, installing all prerequisites
8. Start MPE+ nFIELD and install any desired additional drivers

Notes:

- If moving from MPE+ Tablet to MPE+ nFIELD, you will need to remove the MPE+ Tablet software prior to installing MPE+ nFIELD. You may also need to speak with your account rep to obtain an MPE+ nFIELD license.
- If you are prompted to reboot your PC during the installation, please choose to restart later and then restart your PC after MPE+ has run for the first time.
- Please pay attention to warnings and popups and make sure to allow any and all drivers to install.
- Some driver prompts may be covered by the MPE+ splash screen or window, so you should pay attention for installers showing up in the Task Bar.
- If you choose to reboot your PC or disallow any drivers to be installed, you may need to manually restart/resume the installation process.

Where are extracted images and reports from MPE+ nFIELD stored?
MPE+ nFIELD is meant to be used on a pass-through device. During every extraction, MPE+ nFIELD will prompt you to insert a removal storage device (flash drive) to store the extracted image(s) and report.
**Why is my connected drive not visible as a storage destination in MPE+ nFIELD?**

MPE+ nFIELD only allows you to select storage destinations classified by Windows as "Removable Storage" (as seen in Windows Explorer). This is done to prevent images from being stored on internal drives as MPE+ nFIELD is meant to be used on pass-through devices. This may also prevent MPE+ nFIELD from being able to use certain external drives.

**How large should my storage destination be for MPE+ nFIELD?**

MPE+ nFIELD will store temporary data, the extracted image(s), and report on the selected storage destination. Therefore, you should select a storage destination whose free space is at least 3 times the total size of the device you are extracting from. If the storage destination runs out of room during extraction, the extraction process will fail.
MPE+ Velocitor

What is the MPE+ Velocitor?
The Velocitor is an appliance used in conjunctions with MPE+ to extract data from mobile devices using Chinese chipsets.

How can I obtain an MPE+ Velocitor?
The MPE+ Velocitor license and hardware can be purchased by contacting Sales at sales@accessdata.com.

Does the MPE+ Velocitor work on Windows XP?
No. Windows XP does not support the framework that the Velocitor is built on.

How can I extract data using the MPE+ Velocitor?
Devices: Most devices with chipsets from MediaTek, MStar, and Spreadtrum
Type of Capture: Physical

Procedure

1. Install the "International" drivers via the Driver Management tab in MPE+
2. Connect the MPE+ Velocitor to the PC using the provided USB cable
3. Connect the male end of the "Main Connector" to the MPE+ Velocitor
4. Remove the battery from the mobile device
5. Connect the positive and negative clips on the "Main Connector" to the proper pins on the mobile device
6. Identify the proper cable for the mobile device, and connect it both to the mobile device and to the female end of the "Main Connector"
7. On the Main toolbar in MPE+, click "Select Velocitor Device"
8. In the wizard, either check "Auto Detect Chipset" or select the proper chipset manufacturer, then click "Connect"
9. Follow the wizard's prompts to hold down the mobile device's Power button at the appropriate times
10. Once the connection has been established, either check "Auto Detect Boot" or select the proper boot loader, then click "Extract Data"
11. Follow the wizard's prompts to hold down the mobile device's Power button at the appropriate times
12. When extraction is complete, choose a location to save the image and then MPE+ will proceed to parse data from the image
Notes:

- The DC/USB Power switch (red button) should be in the up or "USB" position to draw power from the PC's USB connection. DC power is only necessary when the PC has a very low power output over USB.
- Reversing the power clips will not adversely affect the device, but will impede proper communication.
- The connection interface in the Velocitor wizard should always be set to "COM".
- If you need to stop or restart the extraction, click "Reset" before clicking "Cancel”.

**How can I parse data from physical BIN images crated by the MPE+ Velocitor?**

Source Image: Physical BIN images

Procedure

1. Install the "International" drivers via the Driver Management tab in MPE+
2. Connect the MPE+ Velocitor to the PC using the provided USB cable
3. On the Tools toolbar in MPE+, click "Parse MPE+ Velocitor Image"
4. Select a physical BIN image created by the MPE+ Velocitor

**Why does the MPE+ Velocitor wizard fail to detect the COM port?**

There may be several causes for this, including the following:

- The necessary drivers were not installed.
- The MPE+ Velocitor was not connected securely.
- The MPE+ Velocitor appliance or USB cable may be faulty.

**Why does the MPE+ Velocitor wizard fail to detect the chipset?**

There may be several causes for this, including the following:

- The power clips are reversed or connected to the wrong pins.
- You did not hold down the mobile device's Power button at the appropriated time(s).
- The MPE+ Velocitor cannot automatically detect the chipset, and you must manually select the correct chipset manufacturer.
- The device requires a UART connection to properly communicate with the MPE+ Velocitor.
- The device does not use a supported chipset.

**How do I build a UART connector to use with the MPE+ Velocitor?**

This is an advanced technique taught in AccessData's training classes. Please contact Sales atsales@accessdata.com for more information.
Why does the MPE+ Velocitor wizard seem to stall?
There may be several causes for this, including the following:

- The MPE+ Velocitor may take several minutes to determine the correct boot loader.
- Some chipsets require the mobile device's power button to be pressed before it can transmit data. If it seems to stall at a particular boot loader, release the hold the device's power button to force it to advance to the next boot loader.
- The MPE+ Velocitor has stopped functioning. Unplug then reattach the MPE+ Velocitor from both the PC and the mobile device, then click "Reset" in the wizard.
Drivers

What drivers are included with MPE+?
The Apple device drivers are installed when MPE+ is installed. Drivers for most other supported devices can be downloaded and installed from within MPE+ itself, via the "Driver Management" tab on the "Home" screen.

Do I really need the Physical Acquisition Support files?
These files are necessary only if you want to be able to extract physical images of Apple devices.

How do I modify what drivers are installed?
You can install drivers from within MPE+ itself, via the "Driver Management" tab on the "Home" screen, and uninstall drivers via the Windows Control Panel.

What do I do if I am unable to download the driver via MPE+?
Manually import them from the MPE+ DVD/ISO.

What do I do if I am unable to download the Physical Acquisition Support files via MPE+?
Contact Support at support@accessdata.com or 800-658-5199 to obtain these files another way.

Does AccessData provide drivers for every supported phone?
We try to provide as many drivers as we can. Any other drivers can be found on the internet, either from the phone manufacturers or their providers, or through a simple Google search.
Cables

Why does MPE+ prompt me for different cables than the ones included in my cable pack?
We have gone through several revisions of the cable pack, with each differing slightly. However, MPE+ is still programmed to ask for the cables from our first revision of the cable pack as more customers have that pack than the newer packs. Please see https://support.accessdata.com/hc/en-us/articles/203399139-Why-does-MPE-prompt-me-for-different-cables-than-the-ones-included-in-my-cable-pack for the MPE Cable Numbers.zip for a table comparing the contents and numbering of the different cable packs.

Can I use OEM cables with MPE+?
Yes. It is actually encouraged to obtain any cables, chargers, and accessories when seizing a phone.

Does AccessData provide cables for every supported device?
We provide cables for many supported phones, but are unable to provide cables for all supported devices. Some devices use proprietary connectors and may require that you use an OEM cable obtained elsewhere.

How do I use the Auxiliary Power Supply Cable?
The Auxiliary Power Supply Cable allows you to power a phone when you don't have its battery or charger. Please note that this cable may not work with all phones, and it will not work with phones without removable batteries. It also may not work with tablets, which usually require a larger power source. Follow the steps below to use this cable properly:

1. Connect both the "Extra Power" and "Data" USB male ends to the PC
2. Remove the battery cover from the phone
3. Find the battery pins in the device and determine which pin is positive and which pin is negative (there may be + and - symbols printed near the battery pins, or you may need to look up pictures of the device’s battery to determine the pole layout)
4. Connect one of the black (negative) alligator clips to the negative pin on the phone
5. Connect the red (positive) alligator clip to the positive pin on the phone
6. Power on the device (if the device doesn't power on, it may have two negative pins, requiring the second black alligator clip to also be connected, or you may have connected the poles backwards)
7. After the phone powers up, connect the appropriate data cable to the USB female end of the Auxiliary Power Supply Cable and then connect that to the device
8. Install the proper drivers and process the phone with MPE+
Phones

What phones/devices are supported by MPE+?
You can view a list of supported devices in MPE+ itself, or at http://accessdata.com/devices/. If a device is not listed in MPE+ it typically means that MPE+ cannot extract any data from that device. The possible exceptions to this are CDMA "dumb" phones and most smartphones.

For unsupported CDMA "dumb" phones, MPE+ might be able to have their File System extracted by selecting "Other" as the Manufacturer and "Other CDMA" as the Model in MPE+.

For unsupported smartphones, MPE+ includes generic extractions that work with most of these devices.

Why aren’t all phones supported by MPE+? Why can’t MPE+ collect all the data from every phone?
Phones are full dynamic systems rather than static storage devices. This means that every phone will store information differently, communicate differently with the computer, and require a different driver. Phone providers have even been known to change the file system structure between different firmware versions on the same model phone, further complicating the issue. There are also some providers that disable data extraction from the phone. We are constantly working to add more supported devices to our product and improve device support.

What is the general process for acquiring data from a phone?
1. Ensure the proper drivers have been installed.
2. For GSM "dumb" devices, make sure a SIM is inserted (use a forensic SIM, if possible, but do *not* use a foreign SIM).
3. Power on and unlock the device.
4. Connect the device to the PC using the appropriate cable.
5. Ensure the device is in the proper mode (almost always *not* “Mass Storage” mode).
6. Confirm that Windows can see the device properly (usually by looking under "Modems" or “Ports” in Device Manager).
7. Launch MPE+ and click the "Select Device" button on the Main toolbar in MPE+.
8. Select the appropriate Manufacturer and Model from the dropdowns.
9. Click "Connect" and proceed to acquire the data you want.
**SIM Cards**

**What are the black cards I received in the MPE+ bundle?**
The MPE+ bundle includes a blank SIM card that can be used as a forensic SIM, and a micro-SIM adapter (it looks like a SIM card but has no circuitry, and has a smaller section the size of a micro-SIM that can be popped out).

The micro-SIM adapter has two purposes: you can pop a micro-SIM into it so that it can be read by the SIM card reader, or you can use it as a template to cut a normal SIM into a micro-SIM. Additional Forensic SIM cards and adapters can be obtained by contacting Sales at 800-574-5199 or sales@accessdata.com.

**What is a forensic SIM?**
A forensic SIM is partial clone of a SIM card that contains enough data for the phone to recognize it and turn on, but will not enable the phone’s radios and does not contain user data. A forensic SIM only has IMSI (International Mobile Subscriber Identity) and ICCID (Integrated Circuit Card Identifier) data.

**What is the process for acquiring data from a SIM card?**
1. Ensure the SIM card reader driver has been installed (often installs automatically).
2. Connect the SIM card reader to your computer (usually appears as a Smart Card Reader in Device Manager).
3. Launch MPE+.
4. Insert the SIM card into the reader according to the picture on the reader (you may see a Smart Card device in Device Manager that shows it is not working, but that is fine). If the phone uses a micro-SIM, you can pop the micro-SIM into the micro-SIM adapter so it fits in the SIM card reader.
5. Select "Extract From SIM" from the Main toolbar and proceed to acquire the data you want.

**How do I create a forensic SIM?**
Automatically:

Ensure the SIM card reader driver has been installed (often installs automatically).

1. Connect the SIM card reader to your computer (usually appears as a Smart Card Reader in Device Manager).
2. Launch MPE+.
3. Insert the original SIM card into the reader according to the picture on the reader (you may see a Smart Card device in Device Manager that shows it is not working, but that is fine). If the phone uses a micro-SIM, you can pop the micro-SIM into the micro-SIM adapter so it fits in the SIM card reader.
4. Select "Read SIM" from the Tools toolbar.
5. Once it has read the IMSI and ICCID, click "Continue".
6. Insert a blank/forensic SIM into the reader and click “OK”.
7. After the values have been written to the forensic SIM, MPE+ will allow you to view and save the results.

8. (Optional) If the phone uses a micro-SIM, you can use the micro-SIM adapter as a template to cut the forensic SIM down to micro-SIM size to fit in the phone.

Manually (if you already know the correct IMSI and ICCID values):

1. Ensure the SIM card reader driver has been installed (often installs automatically).
2. Connect the SIM card reader to your computer (usually appears as a Smart Card Reader in Device Manager).
3. Launch MPE+.
4. Insert a blank/forensic SIM card into the reader according to the picture on the reader (you may see a Smart Card device in Device Manager that shows it is not working, but that is fine).
5. Select "Enter SIM" in the Tools toolbar.
6. Enter the IMSI and ICCID (either in octet form or in raw form), and click "Continue”.
7. Insert a forensic SIM into the reader and click “OK”.
8. After the values have been written to the forensic SIM, MPE+ will allow you to view and save the results.
9. (Optional) If the phone uses a micro-SIM, you can use the micro-SIM adapter as a template to cut the forensic SIM down to micro-SIM size to fit in the phone.
Android Devices

What types of data can MPE+ extract and automatically parse from supported Android devices (not including supplemental parsers)?

dLogical & dSOLO:

- Audio Media Files (audio tracked by Android’s media scanner that appear in Android’s Music app)
- Bluetooth Devices List (list of paired BT devices)
- Browser Bookmarks
- Browser History
- Call History
- Contacts
- Image Media Files (videos tracked by Android’s media scanner that appear in Android’s Gallery app)
- MMS
- SMS
- System Packages List (list of apps installed to the System partition)
- User Packages List (list of apps installed to the Data partition)
- Video Media Files (videos tracked by Android’s media scanner that appear in Android’s Gallery app)
- Wifi Hotspots (list of saved Wi-Fi networks)

Physical, using the Android parser:

- Application Data (data from supported apps like QQ and WeChat)
- Browser Bookmarks
- Browser History
- Calendar
- Call History
- Contacts
- Emails
- IM Accounts (list of usernames from supported chat apps)
- MMS
- Searches (search history from the Google app/widget, Google Now, and the browser)
- SMS
- Full File System
How can I collect logical data from an Android device with MPE+?

Devices: Most Android devices

Type of Capture: Logical

Connecting via MPE+:

1. Install the ADB (Android Debug Bridge) driver for your device. Most Android drivers can be installed via the "Driver Management" tab on MPE+'s Home screen.
2. On the device itself, enable USB Debugging.
3. On the device itself, enable app installations from Unknown Sources.
4. On the device itself, disable App Verification.
5. Connect the device with the proper cable.
6. Unlock the device.
7. Ensure the device is in "Charge Only" mode, or any mode that does not mount the device as an external drive.
8. Click the "Select Device" button on the Main toolbar in MPE+.
9. Select the device's Manufacturer and Model in the drop-downs.
10. Click "Connect".
11. If prompted on the device itself, "Trust" the connection.
12. Proceed to acquire the data you want.

Stand-alone (dSOLO):

1. Insert a blank, FAT32 formatted, SD card in your PC.
2. Click the "Configure dSOLO Mode" button on the Tools toolbar.
3. Select the data types you’d like to acquire.
4. Under "Device Selection", select the drive corresponding to your SD card.
5. Click "Create Apk".
6. On the device itself, enable USB Debugging.
7. On the device itself, enable app installations from Unknown Sources.
8. Insert the prepared dSOLO card in your device.
9. Using a file manager on the device, navigate to and install the MPE.apk from your SD card. Some devices may also let you access the APK via the Browser/Internet app with a URL like "file:///sdcard/mpe.apk".
10. Run the newly installed "AccessData MPE+" app (the app will automatically uninstall itself after running).
11. Insert the SD card in your PC.
12. Click to "Read dSOLO Files" button on the Tools toolbar.
13. Navigate to and open the .dSOLO file from your SD card.
Notes:

- dSOLO cards/apps can be used on multiple devices, as long as there is sufficient space on the card, before retrieving the collected data with MPE+. Each collection will be saved in its own .dSOLO file and named with a timestamp corresponding with the extraction time.
- When you have the proper ADB driver installed and the device is in Debugging mode, Device Manager will usually list an ADB Interface, Android Phone, or Android USB Device, and the device will not be seen as a mass storage device.
- If an Android device isn't explicitly listed as supported, you can usually still perform the extraction by selecting "Android" in the Manufacturer drop-down and "dLogical" in the Model drop-down.

How can I collect physical images from Android devices with MPE+?

Devices: Most Android devices

Type of Capture: Physical

Procedure:

1. Install the ADB (Android Debug Bridge) driver for your phone. Most Android drivers can be installed via the "Driver Management" tab on MPE+'s Home screen.
2. On the device itself, enable USB Debugging.
3. On the device itself, enable app installations from Unknown Sources.
4. On the device itself, disable App Verification.
5. Connect the device with the proper cable.
6. Unlock the device.
7. Click the "Select Device" button on the Main toolbar in MPE+.
8. Select the appropriate Manufacturer and Model, with "(Physical)" next to the model. If the device does not have its own "(Physical)" entry, you can perform a generic Android physical extraction by selecting "Android" and "Other (Physical)" in the Manufacturer and Model drop-downs, respectively.
9. If prompted on the device itself, "Trust" the connection.
10. If prompted on the device itself, grant SU/root permissions.
11. Click "Connect" and proceed to acquire the data you want.

Notes:

- When extracting physical images of Android devices, MPE+ will try to gain root access to the device in order to perform the extraction. If it is unable to gain root access, extraction will fail. You will then need to find another method to gain root access and attempt extraction again.
- When you have the proper ADB driver installed and the device is in Debugging mode, Device Manager will usually list an ADB Interface, Android Phone, or Android USB Device, and the device will not be seen as a mass storage device.
• If an Android device isn’t explicitly listed as supported, you can usually still perform the extraction by selecting "Android" in the Manufacturer drop-down and "Other (Physical)" in the Model drop-down.
• MPE+ will name an Android device’s physical images in the format [partition_name].[sector_size].[file_system] or [partition_name].[file_system]. Changing these file names may result in not being able to correctly read the images.
• Due to manufacturers’ ability to change where data is stored in Android, the Android Parser may not be able to automatically parse out all data types on all physical images.

**How can I automatically parse out extra data from an Android image?**

**Devices:** Most Android devices

**Source Image:** Physical DD "userdata" image

**Procedure:**

1. Import a physical DD image of an Android "userdata" partition by clicking the "Import Image" button on the Main toolbar.
3. Select the data types you wish to parse out and click "Extract".

**Notes:**

• MPE+ will name an Android device’s physical images in the format [partition_name].[sector_size].[file_system] or [partition_name].[file_system]. Changing these file names may result in not being able to correctly read the images.

**Which devices can MPE+ Shell Root on its own when performing physical imaging?**

This will vary depending on the version of Android on the device, and whether or not it has a locked bootloader. The best way to know if your device will work with the exploits in MPE+ is just to try getting a physical image. If MPE+ is unable to gain Shell Root, extraction will fail. You will then need to find another tool to gain Root access and attempt extraction again.

**Why does MPE+ say "ADB driver not found" when trying to connect?**

This means that either the ADB (Android Debug Bridge) driver for your phone is not installed, or that USB Debugging is not enabled on the phone to enable communication via ADB. To install the proper ADB driver you can either use the Driver Management console on MPE+’s Home screen, import the proper driver pack from the MPE+ DVD/ISO, or obtain the driver elsewhere online.

**Does AccessData provide ADB (Android Debug Bridge) drivers for all supported Android phones?**

Many ADB drivers can be installed via the Driver Management console. However, as ADB drivers can be specific to device model and carrier, we cannot provide them all. These remaining drivers can be obtained through the device carrier, the device manufacturer, or elsewhere online. Users
may be able to find help setting up their ADB drivers on YouTube or on Android developer sites like the XDA forums.

**How can I make sure my ADB driver is working?**

Usually, your phone will be listed in Device Manager under something like "Android" or "ADB Devices" when the driver is installed properly. Another way to make sure that it’s working is to use the ADB utility from the [Google Android SDK](https://developer.android.com) by running the command "adb devices" from the directory containing adb.exe. This will list any devices that are communicating over ADB.

**Can I carve for deleted user data (SMS, call history, contacts, etc.) on an Android device?**

These data types are stored in SQLite databases. Typically, when a user selects to delete one of these data types, the corresponding database entry is dropped from the appropriate database. However, any text associated with that entry may still persist, without structure, in the database's free space until the phone decides to cleanup and vacuum the database.

If you have a physical image or an image with Forensic Files from an Android device, you can right-click these SQLite files and select "Parse Database for Deleted Data" to carve for deleted data within them.

The "Deleted" button in the Main toolbar can also be used as a shortcut to automatically find and carve the appropriate SQLite files for deleted SMS and Call History. However, this shortcut may not work with all devices.

**Can MPE+ bypass PIN/password/pattern locks on an Android device?**

MPE+ can currently bypass locks and get physical images from the following devices, regardless of whether USB Debugging is enabled or if the device is in a rooted state:

- Motorola Droid 3
- Motorola Droid 4
- Motorola Droid Bionic
- Motorola Droid RAZR
- Samsung GT-I9100
- Samsung GT-I9100G
- Samsung GT-I9100M
- Samsung GT-I9100P
- Samsung GT-I9108
- Samsung GT-I9210
- Samsung GT-I9210T
- Samsung SCH-R530 (US Cellular)
- Samsung SCH-R760
- Samsung SGH-1727
- Samsung SGH-I727R
- Samsung SGH-I747
- Samsung SGH-I757M
- Samsung SGH-I777
- Samsung SGH-I9100T
- Samsung SGH-I927
- Samsung SGH-T989
- Samsung SGH-T989D
- Samsung SHV-E110S
- Samsung SHV-E120S
- Samsung SHW-M250K
- Samsung SHW-M250L
- Samsung SHW-M250S
- Samsung SPH-D710
Procedure:

1. Install the "Motorola", "Samsung", and "Samsung Physical Support" driver packs.
2. Remove any memory cards that came with the device and insert an empty "forensic" SD card.
3. Connect the device with the proper cable.
4. Click the "Select Device" button on the Main toolbar in MPE+
5. Select the proper manufacturer in the Manufacturer drop-down.
6. Select the correct device model with the "(Physical)" label in the Model drop-down.
7. Click "Connect".
8. Follow the prompts to connect to the device.
9. When prompted, proceed to acquire the data you want.
Apple Devices

List of Supported iOS Devices

<table>
<thead>
<tr>
<th>Device</th>
<th>Max Supported iOS Version</th>
<th>iLogical Extraction</th>
<th>Physical Extraction</th>
<th>iTunes Backup Parsing</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone (1st generation)</td>
<td>3.1.3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 3G</td>
<td>4.2.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 3GS</td>
<td>6.1.6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 4</td>
<td>7.1.2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 4S</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 5C</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 5S</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 6</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 6 Plus</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPad (1st generation)</td>
<td>5.1.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device</td>
<td>Version</td>
<td>Support 1</td>
<td>Support 2</td>
<td>Support 3</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>iPad 2</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPad (3rd generation)</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPad (4th generation)</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPad Mini (1st generation)</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPad Mini (2nd generation)</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPad Air</td>
<td>8.x</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPod Touch (1st generation)</td>
<td>3.1.3</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPod Touch (2nd generation)</td>
<td>4.2.1</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iPod Touch (3rd generation)</td>
<td>5.1.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPod Touch (4th generation)</td>
<td>6.1.6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
What types of data can MPE+ extract and automatically parse from supported iOS devices (not including supplemental parsers)?

iLogical:

- Application Data (data from supported apps like QQ and WeChat)
- Applications Opened
- Browser Bookmarks
- Browser History
- Calendar
- Call History
- Contacts
- Browser Cookies
- Corrected Text
- Emails
- Location Log
- MMS
- Notes (from the Notes app)
- SMS
- User Dictionary (text expansion dictionary)
- Webkit (names of databases belonging to Webkit apps)
- User Media Folder
- File System (except for locked files)

Physical, using the iOS parser:

- Application Data (data from supported apps like QQ and WeChat)
- Applications Opened
- Browser Bookmarks
- Browser History
- Calendar
- Call History
- Contacts
- Browser Cookies
- Corrected Text
- Emails
- Location Log
- MMS
Notes (from the Notes app)
- SMS
- User Dictionary (text expansion dictionary)
- Webkit (names of databases belonging to Webkit apps)
- Full File System

iTunes Backup, using the iTunes Backup parser:

- Application Data (data from supported apps like QQ and WeChat)
- Applications Opened
- Browser Bookmarks
- Browser History
- Calendar
- Call History
- Contacts
- Browser Cookies
- Corrected Text
- Emails
- Location Log
- MMS
- Notes (from the Notes app)
- SMS
- User Dictionary (text expansion dictionary)
- Webkit (names of databases belonging to Webkit apps)
- User Media Folder
- File System (except for locked files)

**How can I collect logical data from an iPhone/iPad/iPod Touch with MPE+?**

Devices & iOS Versions: See [List of Supported IOS Devices](#)

**Type of Capture: Physical**

**Procedure:**

1. Ensure both "Apple Application Support" and "Apple Mobile Device Support" have been installed (these are installed with either the MPE Smartphone Driver or iTunes).
2. Connect the device with the normal Apple USB cable.
3. Click the "Select Device" button on the Main toolbar in MPE+.
4. Select "Apple" in the Manufacturer drop-down.
5. Select the correct device with the "(Physical)" label in the Model drop-down.
6. Click "Connect" and follow the on-screen prompts to put the device in DFU mode.
7. If the device has a password, select the option to brute force the password, enter the password, or just extract the deep logical TAR files.
8. When prompted, select which partitions to acquire and proceed to acquire the data.
Notes:

- If MPE+ reports that the device is not ready, try unlocking the device and opening Settings, then trying to connect again.
- Apple Physical images will be saved in DD format.
- Apple Deep Logical images will be saved in TAR format.
- MPE+ will name an Apple device’s physical images in the format [partition_name].[timestamp].[image_type].[segment_number]. Changing these file names may result in not being able to correctly read the images.
- The OS partition will usually require at least 1 GB of disk space on the destination PC. The other partitions require at least as much space as the Apple device is rated to hold. This means that selecting to acquire the OS Partition, User Partition, Decrypted User Partition, and Full Disk from a 32 GB Apple device will result in about 96 GB worth of image files.
- The iOS Parser may not be able to automatically parse out all data types on all images.

How can I collect physical images from an iPhone/iPad/iPod Touch with MPE+?

Devices & iOS Versions: See List of Supported iOS Devices

Type of Capture: Physical

Procedure:

1. Ensure both "Apple Application Support" and "Apple Mobile Device Support" have been installed (these are installed with either the MPE Smartphone Driver or iTunes).
2. Connect the device with the normal Apple USB cable.
3. Click the "Select Device" button on the Main toolbar in MPE+.
4. Select "Apple" in the Manufacturer drop-down.
5. Select the correct device with the "(Physical)" label in the Model drop-down.
6. Click "Connect" and follow the on-screen prompts to put the device in DFU mode.
7. If the device has a password, select the option to brute force the password, enter the password, or just extract the deep logical TAR files.
8. When prompted, select which partitions to acquire and proceed to acquire the data.

Notes:

- If MPE+ reports that the device is not ready, try unlocking the device and opening Settings, then trying to connect again.
- Apple Physical images will be saved in DD format.
- Apple Deep Logical images will be saved in TAR format.
- MPE+ will name an Apple device’s physical images in the format [partition_name].[timestamp].[image_type].[segment_number]. Changing these file names may result in not being able to correctly read the images.
- The OS partition will usually require at least 1 GB of disk space on the destination PC. The other partitions require at least as much space as the Apple device is rated to hold. This...
means that selecting to acquire the OS Partition, User Partition, Decrypted User Partition, and Full Disk from a 32 GB Apple device will result in about 96 GB worth of image files.

- The iOS Parser may not be able to automatically parse out all data types on all images.

**How can I parse out data from an Apple physical image?**

Source Image: Physical DD "userpartition" images or Logical TAR "logicaluserpartition" image

Procedure:

1. Import a physical DD "userpartition" image or logical TAR "logicaluserpartition" image by clicking the "Import Image" button in the Main toolbar.
2. Select the parser for "iOS" from the Tools toolbar.
3. Select the data types you wish to parse out and click "Extract".

**How can I parse out data from an iTunes backup?**

Devices & iOS Versions: See [List of Supported IOS Devices](#)

Source Data: iTunes Backup

Procedure:

1. Import an iTunes backup by clicking the "Import Folder" button on the Main toolbar.
2. Select the parser for "iTunes Backup" from the Tools toolbar.
3. Select the top level folder from the backup, then click "OK".
4. When prompted, enter the iTunes backup password if applicable.
5. Select the data types you wish to parse out and click "Extract".

**Can MPE extract data from my iOS device if it has an unknown PIN/password?**

If you do not know the PIN/password to unlock the device, the "iLogical" extraction allows you to use a pairing record, obtained from the device owner's PC, to bypass the lock and perform a logical extraction. See [What Is A Pairing Record And Where Are They Stored?](#)

If your device supports physical extraction (see [List Of Supported IOS Devices](#)) and uses a simple password (4 digits), MPE+ will also allow you to brute force the password, or just extract the deep logical TAR files. If your device uses an unknown complex password, MPE+ will allow you to extract the deep logical TAR files.

**What is a pairing record and where are they stored?**

Pairing records are used to identify which PCs are "trusted" by a device. They are created by iTunes whenever a device is connected to a PC and unlocked (iOS 7+ also requires tapping "Trust" on the device). Pairing records are saved as PLIST files, and are named using each device's unique identifier (UDID, see [How Can I Determine The Unique Identifier (UDID) Of A Locked Device?](#)).
They can be found in the following locations:

Windows: %ProgramData%\Apple\Lockdown

OS X: /var/db/lockdown

**How can I determine the unique identifier (UDID) of a locked device?**

**Windows:**

1. Connect the device to the PC
2. Open Windows Device Manager
3. Expand "Universal Serial Bus Controllers"
4. Right-click "Apple Mobile Device USB Driver", and click "Properties"
5. Under the "Details" tab, select "Device Instance Path" in the drop-down
6. The 40 characters after the last "\" under "Value" is the device's UDID

**OS X:**

1. Connect the device to the PC
2. Click the Apple icon in the Menu Bar
3. Select "System Information"
4. Expand "Hardware" and select "USB"
5. Find and select your device under the "USB Device Tree"
6. The value listed as the "Serial Number" is not really the device's serial number, but is its UDID

**MPE+ can't connect, and iTunes reports the device is "supervised with another computer and cannot be used with this computer." What does this mean, and is there a way around this?**

This is caused by an app called **Apple Configurator**, which is often used to mass configure and administer iOS devices. This app allows the administrator to configure a "Supervisor" computer, preventing the device from communicating with any other computer. MPE+ can bypass this "lock" by pointing it to the pairing record obtained from the "Supervisor" computer.

**In the logical image of my Apple device, all the emails are blank. What causes this?**

Full email messages can only be extracted in a physical image, because email is protected by iOS. When doing a logical extraction, iOS only allows access to the EnvelopelIndex database, which mainly tracks dates of emails, and no real message content.

**Why does the DFU wizard keep looping?**

This usually means that you are using a device that's not supported for physical extraction. See [List Of Supported IOS Devices](#).
**How do I get my device out of DFU mode?**
If your device does not reboot itself after extraction, hold down the Home button and Power button together for about 15 seconds until the device reboots to get out of DFU mode.

**What are the .IOS_KEYS files created during physical extractions?**
These contain the key bundles that MPE+ and FTK will use to decrypt the physical image(s).

**Why can’t FTK display some files in a physical DD image from an Apple device?**
All devices that shipped with or were restored to iOS 4+ encrypt the majority of their data. Because of this, you may not be able to view the contents of some files in FTK unless your images were created with MPE+ 4.7 or later (to obtain the decryption keys) and you are using FTK 4.0.2 or later. An alternative to getting these physical DD images would be to get the deep logical TAR images, which are not encrypted.

**Why can’t FTK display some PNG graphics in a physical iOS image even after decryption?**
Many of the PNG graphics built into iOS and also used in apps are actually using Apple’s proprietary modification to the PNG format, referred to as CgBI. The modifications to this format prevent them from being viewed by many standard graphic viewers unless they are first converted back to standard PNG format using the iOS SDK. More information about the CgBI file format can be found [here](#).

**Can I recover deleted data on an iOS device?**
Yes and no.

**Deleted user data (SMS, call history, contacts, etc.):**

These data types are stored in SQLITE databases. Typically, when a user selects to delete one of these data types, the corresponding database entry is dropped from the appropriate database. However, any text associated with that entry may still persist, without structure, in the database’s free space until the phone decides to cleanup and vacuum the database. If you an image of an iOS device, you can right-click these SQLite files and select "Parse Database for Deleted Data" to carve for deleted data within them. Even logical images of iOS devices contain many of these SQLite databases, allowing you to find deleted data.

The "Deleted" button in the Main toolbar can also be used as a shortcut to automatically find and carve the appropriate SQLite files for deleted SMS and Call History. However, this shortcut may not work with all devices.

**Deleted files (old file versions from factory resets, photos taken with the camera, etc.):**

All Apple mobile devices shipped with or restored to iOS 4 or later employ file-level encryption for most files on the device. It is nearly impossible to find and carve out these files after they are deleted. This is not a limitation of our software but is because Apple removes the key files from the device for files in unallocated space. You can, however, still...
attempt to carve for and find unencrypted files within the file system. On legacy and pre-iOS 4 devices, file carving will yield more results. This limitation imposed by Apple should not stop you from attempting a recovery, but should explain why recovery cannot be accomplished on certain devices.
BlackBerry Devices

How can I collect logical data from a BlackBerry with MPE+?

Devices: Most BlackBerry Phones, Prior to BlackBerry OS 10

Type of Capture: Logical

Procedure:

1. Install the "BlackBerry" and "BlackBerry (COM support)" drivers via Driver Management in MPE+.
2. Power on the phone.
3. Connect the device with the proper cable.
4. Click the "Select Device" button on the Main toolbar in MPE+.
5. Select "BlackBerry" in the Manufacturer drop-down.
7. Click "Connect".
8. When prompted in MPE+, enter the phone’s password/PIN. If the device has no password/PIN, leave this field blank. If the device is also using encryption, enter the password/PIN on the device itself.
9. Proceed to acquire the data you want.

Notes:

- BlackBerry keyboards contain both letters and numbers on the same keys, using the ALT key to switch between the two. Often, the device password/PIN is actually comprised of letters even though you might think you’re entering numbers. For example, the password/PIN '1234' might actually be actually 'wers'.

MPE+ does not properly display the natural previews of files from an encrypted BlackBerry?

BlackBerry appends the file extension .REM to files that it encrypts. When MPE+ extracts these files, even though the files have been decrypted, they will retain this .REM extension. This can cause them to render incorrectly in the Natural Preview pane. To get around this, you can either use file carving in MPE+ to carve out those files and assign them correct file extensions, or process the image with FTK which will identify the files by header rather than file extension.

How do I extract files from an encrypted SD card?

If a BlackBerry is configured to encrypt the contents of its SD card, you can extract decrypted copies of contained files by leaving the SD card in the device during extraction. The contents of the SD card will usually appear in a folder called "SDCard" in the root of the File System.
**iDEN Devices**

**How can I collect logical data from an iDEN device with MPE+?**

**Devices:** Supported iDEN devices

**Type of Capture:** Logical

**Procedure:**

2. Power on the phone.
3. Set the phone to connect as a modem (typically Menu > Settings > Connections > USB > Data Modem).
4. Connect phone with the proper cable. Windows will likely try to automatically install the driver. Whether this installation fails or not, we need to change the driver.
5. Open the Device Manager and find the iDEN Device entry (may be under Modems).
6. Right-click the iDEN Device entry and select "Update Driver Software".
7. Tell Windows to browse your computer for driver software.
8. Tell Windows to let you pick from a list of drivers.
9. Click "Have Disk" and browse to the "iDEN" folder extracted from step 1 and select "iDEN_USB_Device.inf", and click "OK" then "Next".
10. When prompted, allow the driver to install. When the installation completes, Device Manager should now list a device called "iDEN USB Device" under "libusb-win32 devices". In MPE+, click the "Select Device" button on the Main toolbar.
11. Select the proper manufacturer in the Manufacturer drop-down.
12. Select the proper device in the Model drop-down.
13. Click "Connect" and proceed to acquire the data you want.
14. Part way through acquiring data (usually after acquiring the phone book), progress will stop, the phone screen may turn white, and Windows will likely try to automatically install another driver. Whether this installation fails or not, we need to change the driver.
15. Open the Device Manager and find the iDEN Device entry.
16. Right-click the iDEN Device entry and select "Update Driver Software".
17. Tell Windows to browse your computer for driver software.
18. Tell Windows to let you pick from a list of drivers.
19. Click "Have Disk" and browse to the "FlashPatriot" folder extracted from step 1 and select "Flash_P2K_Patriot.inf", and click "OK" then "Next".
20. When prompted, allow the driver to install. When the installation completes, Device Manager should list a device called "Flash P2K Patriot" under "libusb-win32 devices" and MPE+ should continue and finish the extraction.
Notes:

- MPE+ only supports extraction of Contacts from most iDEN phones.

**Windows Mobile Devices**

**How can I collect logical data from a Windows Mobile device with MPE+?**

Devices: Supported Windows Mobile OS devices (Not Windows Phone OS)

Type of Capture: Logical

Procedure:

1. Install the Windows Mobile drivers from the MPE+ Driver Pack.
2. Power on the device.
3. In the "USB to PC" options on the phone, enable "ActiveSync" and "Enable faster data synchronization".
4. Connect the device with the proper cable. Windows Mobile Device Center should see the device, but do not tell it to connect.
5. Click the "Select Device" button on the Main toolbar in MPE+.
6. Select the proper Manufacture and Model from the dropdowns.
7. Click "Connect".
8. If prompted on the phone to install the OxygenEngine.dll, accept and allow the installation.
9. Proceed to acquire the data you want.

Notes:

- If a Windows Mobile device isn't explicitly listed as supported, you can often still perform the extraction by selecting "Windows Mobile Phone" in the Manufacturer drop-down and "Generic Windows Mobile Phone" in the Model drop-down.

**MPE+ pushes the agent to my phone, but then says it cannot find the device. Why is this happening?**

This occurs if a Windows Mobile phone has locked down access to its data. You can perform the following steps to gain full access to the phone and resolve this.

1. Download the following Windows Mobile Exploit.zip
   
2. Connect the phone to the PC.
4. If the phone has a touchscreen, copy "ClearSecurity(Touchscreen).cab" to the root of the phone’s storage. If the phone does not have a touchscreen, copy "ClearSecurity.cab" to the root of the phone’s storage.

5. On the phone, run "File Explorer" (usually under the Start menu) and navigate to and run the CAB file that you copied over.

6. When prompted, allow the program to install then click "OK". This changes the permissions on the phone and unlocks the necessary data.

7. Now, uninstall the program we just installed, "SOTI MobileControl Device Agent"

8. Proceed to use MPE+ and extract the desired data.
General Troubleshooting

**Why does MPE+ say my device is not ready or otherwise unable to connect?**

There could be many causes for this:

- Ensure the device is on and unlocked.
- For GSM "dumb" phones, make sure a SIM is inserted. Use a forensic SIM if possible but do *not* use a foreign SIM from another phone or provider.
- The drivers may not be installed or may be corrupt. Reinstall the drivers and ensure the device's ports show up in Device Manager.
- Ensure the phone is supported by MPE+ and you have selected the correct Manufacturer and Model.
- Try connecting over a different port.
- MPE+ sometimes requires that the device be connected before launching MPE+.
- You can contact AccessData Support at 800-658-5199 if you continue to have problems after following these points.

**Why did MPE+ fail to collect some data from my device?**

This could be because this device doesn't have any of the specified types of data stored on it, which you can verify by looking through the device itself or using the SQLite parser on the extracted file system.

It may also be due to a file system change in a specific firmware version that MPE+ cannot read/parse yet. If this is the case, other methods not involving MPE+ can be used to report on the missing data. You can learn about these other methods in our Mobile Forensics training courses.

**Why did MPE+ pull all the data off my device when I only selected to acquire the File System?**

If MPE+ has any difficulty in acquiring the File System of a device, it will automatically try another method of acquiring the File System. The second method will automatically collect all the data from the device.

**I told MPE+ to acquire all data from my supported CDMA phone, but the extraction failed?**

If this happens, completely close and restart MPE+, and reboot the phone. Try extracting data again, but rather than selecting all data, select only the File System. After the File System extracts you can click the "Extract Device Data" button to extract the remaining data.