MPE+ Frequently Asked Questions & Troubleshooting

MPE+ 5.1.2.447

Table of Contents

Mobile Forensic Background Knowledge

Q. What is the difference between Computer Forensics and Mobile Phone Forensics?

A. 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.

Q. What is CDMA?

A. 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 cars, unless they are world phones (which rely on GSM technology outside of the USA). More information about CDMA can be obtained here.

Q. What is GSM?

A. 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 here.

System Requirements

Q. What Operating Systems are supported by MPE+?

Windows XP Professional (32-bit only)
Windows 7 Home Premium (32- and 64-bit)
Windows 7 Professional (32- and 64-bit)
Windows 7 Enterprise (32- and 64-bit)
Windows 7 Ultimate (32- and 64-bit)

Q. What prerequisites must I install manually before installing MPE+?

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 the Message Queuing Services item.
   Click Next.
4. This will start the MSMQ 2.0 setup process. Your Windows XP installation CD-ROM, network share, or
   install point must be available.
5. MSMQ will display an installation dialog box. You will be prompted to install either an MSMQ server or a
   dependent client.
6. You can install MSMQ 2.0 in Workgroup mode by selecting "Message Queuing Will Not Access a Directory Service".

If you have Windows 7 N, you will need to manually install Windows Media Player via Microsoft's Media Feature Pack here.

Q. Can I use the Home Edition of Windows XP with MPE+?

A. No. MPE+ utilizes MSMQ (Microsoft Message Queuing) which is not available in XP Home Edition.

Licensing

Q. How do I move my MPE+ installation to a different computer?

A. 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 Manger.
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+

Q. How do I install MPE+?

Online:

1. Uninstall any versions of MPE+ prior to version 4.6
2. Ensure CodeMeter Runtime is installed
3. Ensure your CodeMeter dongle is connected and has a current MPE+ license
4. In a browser, go to http://accessdata.com/MPE-clickonce
5. Select either "Install MPE+" or "Install Tablet MPE+"
6. Let the installer run all the way through, installing all prerequisites
7. If prompted, allow MPE+ to download and install the newest version of iTunes
8. Open iTunes and confirm automatic syncing is disabled (under Edit > Preferences > Devices)
9. In MPE+, set the TEMP folder path appropriately
10. Install the Apple Physical Support Files
    MPE+: From the Home screen, open the "Physical Acquisition Support" tab and select what packages to install
    MPE+ Tablet: From the Tools menu, click the "Physical Acquisition Files" button and select what packages to install
11. Install any desired additional drivers
    MPE+: From the Home screen, open the "Driver Management" tab and select what packages to install
    MPE+ Tablet: From the Tools menu, click the "Driver Support" button, and select what packages to install

DVD or ISO:

1. Uninstall any versions of MPE+ prior to version 4.6
2. Ensure CodeMeter Runtime is installed
3. Ensure your CodeMeter dongle is connected and has a current MPE+ license
4. If needed, download the MPE+ ISO from http://accessdata.com/MPE-clickonce
5. If you need an offline copy of the Apple physical support files, contact Support at 800-658-5199 or support@accessdata.com to obtain them
6. Insert the MPE+ DVD or mount the ISO
7. If setup does not start automatically, run the included "setup.bat" from the DVD/ISO
8. Let the installer run all the way through, installing all prerequisites
9. If prompted, download and install the newest version of iTunes from http://www.itunes.com
10. Open iTunes and confirm automatic syncing is disabled (under Edit > Preferences > Devices)
11. Launch MPE+ and set the TEMP folder path appropriately
12. Install additional drivers by importing the folder on the DVD/ISO containing the driver packs you want to install (eg. to install the Android drivers for Windows 7 x64, you'd browse to [DVD]:\Setup\Drivers\Wind7amd64\Android)
    MPE+: From the Options menu, click "Import Driver" and select the folder to import
    MPE+ Tablet: From the Tools menu, click the "Import Drivers Manually" button and select the folder to import

Notes:

- Full installation can take quite a while as there is a lot of data for it to download and install, including prerequisites, driver files, firmware, Apple physical support files, and MPE+ itself.
- 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.

Q. What is the importance of the MPE+ TEMP folder and where should I put it?

A. 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.

Q. 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+ Tablet:

1. Click the lower-right button in Tablet MPE+
2. Click "Settings"
3. Click the button next to the "Temporary Data Path" field to select a new location
4. Click "OK"

Q. Do I really need the Apple physical support files?

A. These files are necessary only if you want to be able to extract physical images of Apple devices.

Q. The MPE+ installers left several shortcuts on my desktop and Start menu. Do I need these?

A. No. These shortcuts are safe to delete. Some of the shortcuts won't even work as unnecessary files have been removed from their accompanying programs.

MPE+ Tablet

Q. What is the MPE+ Tablet?

A. With the release of MPE+ 4.6, we are introducing a new, slimmer tablet preloaded with a touch-friendly version of MPE+. The new MPE+ Tablet interface is also available here if you'd like to install it on the old MPE+ Tablet.

Q. How do I install the MPE+ Tablet interface?

A. The procedure for installing either MPE+ or MPE+ Tablet is outlined in this post.

Q. What are the specifications for the new MPE+ Tablet?

Operating System: Windows 7 Embedded Standard x64
Display: 10.1" Capacitive Screen
CPU: Dual-Core 1.66 GHz Intel Atom N570
RAM: 2 GB DDR2
Drive: 16 GB SSD
Expandable Storage: microSDHC Slot
Ports: USB 2.0 x 2, USB 3.0 x 1, Multi-Use Port for Ethernet & VGA adapter, A/C Port

Q. The Tablet's internal drive does not have much space. Where should I store my data?

A. The new MPE+ Tablet is meant to be a pass-through device. Images should not be stored on the Tablet's internal drive, but on external media. Your MPE+ TEMP folder should also be stored on external media to ensure you do not run out of space.

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

A. The procedure for changing the TEMP folder location in either version of MPE+ is outlined in this post.

Q. How can I expand my available storage space?

A. You can add storage space by connecting a USB thumb drive or inserting a microSDHC card. External USB HDDs can also be used if desired.

Q. Does the new MPE+ Tablet have WiFi connectivity?

A. No. Although the Tablet hardware includes a WiFi card, we have left it disabled intentionally to protect the device. Internet connectivity can be achieved via Ethernet with the included adapter.

Q. Can I use the Tablet's built-in SIM card slot?

A. No. Although the Tablet hardware includes a slot for a SIM card, we have left it disabled intentionally to protect the device. The SIM card reader in the MPE+ Cable Pack can still be used to analyze SIM cards.

Q. How do I use the USB 3 port on the new tablet?

A. The USB 3 port on the new tablet requires an adapter, which is shipped with the tablet. If your tablet is lacking the driver for the adapter to work, you can find it on the driver CD included with the tablet or download it from here.

Drivers

Q. What drivers are included on the MPE+ disc or on AccessData's site?

A. iTunes and a basic driver package are installed as prerequisites with MPE+. Other drivers can be downloaded and installed from within MPE+ itself.

Q. How do I modify what drivers are installed if I did not install them all during the initial installation?

A. You can modify what drivers are installed from within MPE+ itself, or uninstall drivers through the Control Panel.

Q. What do I do if I am unable to download the driver via MPE+?

A. Manually import them from the MPE+ DVD/ISO.

Q. What do I do if I am unable to download the Apple Device Physical Files via MPE+?

A. Contact Support at 800-658-5199 to obtain the Apple Device Physical Files another way.

Q. Does AccessData provide drivers for every supported phone?

A. 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

Q. Why does MPE+ prompt me for different cables than the ones included in my cable pack?

A. We have gone through three 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 the that pack than the newer packs. Please see the attached MPE Cable Numbers.zip for a table comparing the contents and numbering of the different cable packs.

Q. Can I use OEM cables with MPE+?

A. Yes. It is actually encouraged to obtain any cables, chargers, and accessories when seizing a phone.

Q. Does AccessData provide cables for every supported device?

A. We provide cables for many supported phones, but are unable to provide cables for all supported devices.

Phones

Q. What phone/devices are supported by MPE+?

A. You can view a list of supported devices in MPE+ itself, or online. 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 most unsupported smartphones, MPE+ includes generic extractions that work with most of these devices.

Q. Why aren't all phones supported by MPE+?/Why can't MPE+ collect all the data from every phone?

A. 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. We are constantly working to add more supported devices to our product and improve device support.

Q. What is the general process for acquiring data from a phone?

1. Ensure the proper drivers have been installed.
2. For GSM 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 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

Q. What are the two black cards I received in the MPE+ bundle?

A. The MPE+ bundle includes a blank SIM card that can be used as a forensic SIM (it says “MPE+ Forensic SIM” in the back), 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.

Q. What is a forensic SIM?

A. 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.

Q. 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.

Q. How do I create a forensic SIM?

Automatically:

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 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.
5. Select "Forensic SIM" from the Main toolbar.
6. Once it has read the IMSI and ICCID, click “Continue”.
7. Insert a blank/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.

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 Main 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

Q. How can I collect logical data from an Android device with MPE+?

Devices: Most Android devices
Type of Capture: Logical

Procedure:

1. Install the ADB (Android Debug Bridge) driver for your phone. Some are included in the Driver Pack or on the MPE+ CD, but ADB drivers are specific to device model and carrier so we cannot provide them all. These should be obtained through the device carrier (not the device manufacturer).
2. Remove any memory cards that came with the device and insert an empty "forensic" SD card (this is where MPE+'s agent will be temporarily stored).
3. On the device itself, set the device to connect in Debugging/Development mode (this setting can be in different locations on different devices, so check with the device's user manual).
4. On the device itself, set the device to allow applications from Unknown Sources (this setting can be in different locations on different devices, so check with the device's user manual).
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 device's Manufacturer and Model in the drop-downs.
9. Click "Connect" and proceed to acquire the data you want.

Q. How can I collect Protected User Data (Forensic Files) from Android devices with MPE+?

Devices: Most Android devices
Type of Capture: Logical

Procedure:

1. Install the ADB (Android Debug Bridge) driver for your phone. Some are included in the Driver Pack or on the MPE+ CD, but ADB drivers are specific to device model and carrier so we cannot provide them all. These should be obtained through the device carrier (not the device manufacturer).
2. Remove any memory cards that came with the device and insert an empty "forensic" SD card (this is where MPE+'s agent will be temporarily stored).
3. On the device itself, set the device to connect in Debugging/Development mode (this setting can be in different locations on different devices, so check with the device's user manual).
4. On the device itself, set the device to allow applications from Unknown Sources (this setting can be in different locations on different devices, so check with the device's user manual).
5. Connect the device with the proper cable.
6. Unlock the device.
7. Gain Shell Root (*not* full root) with a tool like SuperOneClick.
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" and proceed to acquire the "Forensic Files".

Q. 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. Some are included in the Driver Pack or on the MPE+ CD, but ADB drivers are specific to device model and carrier so we cannot provide them all. These should be obtained through the device carrier (not the device manufacturer).
2. Remove any memory cards that came with the device and insert an empty "forensic" SD card (this is where MPE+'s agent will be temporarily stored).
3. On the device itself, set the device to connect in Debugging/Development mode (this setting can be in different locations on different devices, so check with the device's user manual).
4. On the device itself, set the device to allow applications from Unknown Sources (this setting can be in different locations on different devices, so check with the device's user manual).
5. Connect the device with the proper cable.
6. Unlock the device.
7. Gain Shell Root (*not* full root) with a tool like SuperOneClick.
8. Click the "Select Device" button on the Main toolbar in MPE+.
9. In the Manufacturer drop-down, select "Android".
10. In the Model drop-down, select "Android (Physical).
11. Click "Connect" and proceed to acquire the data you want.

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

Devices: Most Android devices
Source Image: Physical DD "userdata" image or Logical AD1 image containing "Forensic Files"
Included Parsers: Bookmarks, Call History, Email, IM Accounts, MMS, Phonebook/Contacts, Search History, SMS

Procedure:

1. Import either a physical DD image of an Android "userdata" partition or a logical AD1 image of an Android containing "Forensic Files" by either clicking the "Import Image" button on the Main toolbar.
2. Select the parser for "Android" in the Main toolbar.
3. Navigate to and select the appropriate folder, then click "OK":
   Physical DD: root > [root]
   Logical AD1: File System > data
4. Select the data types you wish to parse out and click "Extract".

Notes:

- 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 "Generic Android" in the Model drop-down.
- Android physical images will be saved in DD format and cannot be viewed in MPE+. They must be processed in FTK.
- 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.
- The Android Parser may not be able to automatically parse out all data types on all images.

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

A. 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.

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

A. Many ADB drivers can either be download via the Driver Management console or imported from the MPE+ DVD/ISO. 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.

Q. How can I make sure my ADB driver is working?

A. 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 by running the command "adb devices" from the directory containing adb.exe. This will list any devices that are communicating over ADB.

Q. I get the error "No flash card in device", but I know there is an SD card in it.

A. The phone may be automatically mounting the SD card to the PC as a Mass Storage Device. You'll know if it's mounted to your PC because you'll be able to browse the phone's SD Card in Windows Explorer. If it is mounted, you should find the option to unmount it and set the phone to Charge Only mode in the phone's Notifications (pull down the Notification Bar at the top of the screen).

Q. What is contained in the Protected User Data (Forensic Files)?

A. "Forensic Files" refers to the full contents of an Android device's “/data” folder. This folder contains a wealth of user data, including SQLITE databases full of "deleted" data (contacts, SMS, app cache,

downloads, etc.) that is normally hidden from the user. To acquire this data, either select to extract "Forensic Files Only" to extract *only* the "/data" folder, or select "File System" to extract the *entire File System* including the "/data" folder.

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

A. 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.

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

A. MPE+ can currently bypass locks and get physical images from devices in the *Samsung Galaxy S II family* running *Android 2.3.4 or 2.3.5*, regardless of whether USB Debugging is enabled or if the device is in a rooted state. This includes the following device models:
GT-I9100
GT-I9100G
GT-I9100M
GT-I9100P
GT-I9108
GT-I920T
GT-I9210
GT-I9210T
SCH-R760
SGH-I727
SGH-I727R
SGH-I757M
SGH-I777
SGH-I9100T
SGH-I927
SGH-T989
SGH-T989D
SHV-E110S
SHV-E120S
SHW-M250K
SHW-M250L
SHW-M250S
SPH-D710

Procedure:

1. Ensure Samsung Kies is installed (usually installed automatically as part of MPE+ firmware).
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 "Samsung" in the Manufacturer drop-down.
6. Select the correct device model with the "(Physical)" label in the Model drop-down.
7. Click "Connect".
8. If prompted, disconnect and reconnect the device from the PC and click "Connect" again.
9. Wait while MPE+ prepares the devices (this may take several minutes).
10. When prompted, proceed to acquire the data you want.

Apple Devices

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

Devices: iPhone (all models through iPhone 4S), iPod Touch (all models through iPod Touch 4G), iPad (all models through "The New" iPad)
iOS: iOS 2.x - 6.0.1
Type of Capture: Logical

Procedure:

1. Connect the device with the normal Apple USB cable and allow Windows to install any needed drivers.
2. Click the "Select Device" button on the the Main toolbar in MPE+.
3. Unlock the device.
4. Select "Apple" in the Manufacturer drop-down.
5. Select the correct device in the Model drop-down.
6. Click "Connect".
7. When prompted, enter the device's iTunes backup password if one exists.
8. Proceed to acquire the data you want.

Q. How can I collect physical (or deep, unencrypted logical) images from an iPhone/iPad/iPod Touch with MPE+?

Devices: iPhone (all models through iPhone 4), iPod Touch (3G & 4G), iPad 1
iOS: iOS 2.x - 5.1.1
Type of Capture: Physical

Procedure:

1. Connect the device with the normal Apple USB cable.
2. Click the "Select Device" button on the the Main toolbar in MPE+.
3. Select "Apple" in the Manufacturer drop-down.
4. Select the correct device with the "(Physical)" label in the Model drop-down.
5. Click "Connect" and follow the on-screen prompts to put the device in DFU mode. Note that holding the buttons down for longer than prompted will result in the device not going into DFU mode and you will need to restart the process.
6. 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.
7. When prompted, select which partitions to acquire and proceed to acquire the data.

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

Devices: Most Apple devices
Source Image: Physical DD "userpartition" images or Logical TAR "logicaluserpartition" image
Included Parsers: Bookmarks, Calendar, Call History, Cookies, Email, Memos, MMS, Phonebook/Contacts, SMS, URL History, Webkit, Application List, Auto/Corrected Text, User Dictionary, Location Logs

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 Main toolbar.
3. Navigate to and select the appropriate folder, then click "OK":
   Physical DD: root > Data > mobile > Library
   Logical TAR: root > mobile > Library
4. Select the data types you wish to parse out and click "Extract".

Q. How can I parse out data from an iTunes backup?

Devices: iPhone (all models through iPhone 5), iPod Touch (all models through iPod Touch 5G), iPad (all models through iPad Mini)
iOS: iOS 2.x - 6.0.1
Source Data: iTunes Backup
Included Parsers: Bookmarks, Calendar, Call History, Cookies, Memos, MMS, Phonebook/Contacts, SMS, URL History, Webkit, Application List, Auto/Corrected Text, User Dictionary, Location Logs

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 Main 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".

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 and cannot be viewed in MPE+.
- 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.

Q. Apple Software Update asked me to upgrade iTunes. Should I allow this?

A. Sure, but please make sure that the option to disable automatic syncing is checked (under Edit >

Preferences > Devices) to prevent it from potentially contaminating evidence.

Q. How do I get my device out of DFU mode?

A. If your device does not reboot itself after extraction, hold down the Home button and Power button together for 15 seconds to get out of DFU mode.

Q. Can MPE extract data from my iOS device if it has a PIN/password?

A. Standard logical extractions require you to know the PIN/password to unlock the device. If your device uses a simple password (4 digits), MPE+ will allow you to brute force the password, enter the password, or just extract the deep logical TAR files. If your device uses a complex password, MPE+ will allow you to enter the password or just extract the deep logical TAR files.

Q. Logical imaging of my Apple device fails part-way through extraction. What can cause this?

A. The main thing I've seen cause this is using a faulty data cable.

Q. What does error 1013 mean when acquiring a physical image from an Apple device?

A. This means that you are using an unsupported device.

Q. What are the .IOS_KEYS files created during physical extractions?

A. These contain the key bundles that MPE+ and FTK will use to decrypt the physical image(s).

Q. Why can't FTK display some files in a physical DD image from an Apple device?

A. 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 your 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.

Q. Why can't FTK display some PNG graphics in a physical image even after decryption?

A. Many of the PNG graphics built in to 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.

Q. Can I carve for deleted data on an iOS device?

A. 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 have logical TAR or physical DD 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.

Deleted files (old file versions from factory resets, photos taken with the camera, etc.): As of iPhone 3GS and iOS 4, iOS employs file-level encryption for many 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

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

Devices: Most BlackBerry Phones
Type of Capture: Logical

Procedure:

1. Install BlackBerry Desktop via the MPE+ Driver Pack.
2. Power on the phone.
3. Connect the device with the proper cable.
4. Click the "Select Device" button on the the Main toolbar in MPE+.
5. Select "BlackBerry" in the Manufacturer drop-down.
6. Select the correct device in the Model 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. (**Important:** A BlackBerry keyboard contains numbers and letters on the same keys. 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' is actually 'wers'.)
9. Proceed to acquire the data you want.

Q. How can I automatically parse out data from a BlackBerry IPD backup?

Devices: Most BlackBerry devices
Source Image: BlackBerry IPD backup file
Included Parsers: Bookmarks, Calendar, Call History, Corrected Text, Email, HotList, Locations, Memos, MMS, Phonebook/Contacts, PIN Messages, Search History, SMS, URL History

Procedure:

1. Select the parser for "IPD" from the Main toolbar.
2. Select a BlackBerry IPD backup file to import.
3. When prompted, enter the phone's/backup's password/PIN. If the device/backup has no password/PIN, leave this field blank.
4. Select the data types you wish to parse out and click "Extract".

Notes:

- If a BlackBerry device isn't explicitly listed as supported, you can often still perform the extraction by selecting "BlackBerry" in the Manufacturer drop-down and "Other BlackBerry Phone" in the Model drop-down.
- Prior to MPE+ 4.5, extraction from a password/PIN locked BlackBerry is not supported and you must disable the password/PIN lock in the phone's settings.

Q. Why does MPE+ deselect "Email" when extracting from newer BlackBerry phones?

A. MPE+ currently does not support email extraction from BlackBerry 8000 or newer. However, you can usually still get the email by creating an IPD backup of the phone and parsing it with MPE+.

Q. Can MPE+ parse BBB backup files created with BlackBerry Desktop 7?

A. No. MPE+ can currently only parse IPD backup files. You can download BlackBerry Desktop 6.1 here, which will create IPD backups.

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

A. 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.

Q. How do I extract files from an encrypted SD card?

A. 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

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

Devices: Supported iDEN devices
Type of Capture: Logical

Procedure:

1. Install the MPE+ Driver Pack, selecting to install the iDEN drivers (they should be installed to C:\Program Files (x86)\AccessData\Mobile Phone Drivers\iDENAD)
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 installations 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 iDEN_USB_Device.inf in the iDENAD\iDEN folder and click "OK" and "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".
11. Open MPE+ and click the "Select Device" button on the the Main toolbar.
12. Select the proper manufacturer in the Manufacturer drop-down.
13. Select the proper device in the Model drop-down.
14. Click "Connect" and proceed to acquire the data you want.
15. 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 installations fails or not, we need to change the driver.
16. Open the Device Manager and find the iDEN Device entry.
17. Right-click the iDEN Device entry and select "Update Driver Software".
18. Tell Windows to browse your computer for driver software.
19. Tell Windows to let you pick from a list of drivers.
20. Click "Have Disk" and browse to Flash_P2K_Patriot.inf in the iDENAD\FlashPatriot folder and click "OK" and "Next".
21. 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

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

Devices: Supported Windows Mobile devices (Not Windows Phone 7)
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 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.

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

A. 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 and unzip Windows Mobile Exploit.zip
2. Connect the phone to the PC
3. Browse to the phone's storage using Windows Explorer
4. If the phone has a touchscreen, copy "ClearSecurity(Touchsreen).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

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

A. There could be many causes for this:

- Ensure the device is on and unlocked.
- For GSM 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.

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

A. 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. It may also be due to a file system change in a specific firmware version that MPE+ cannot read/parse yet. This may also be due to the fact that the phones are full dynamic systems and can essentially choose not to allow a user to collect data. 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.

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

A. 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.

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

A. 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 (or go to Tasks>Extract Data) to extract the remaining data.

Known Issues

MPE+ cannot be installed or run from multiple user accounts on the same PC.

Resolution: Choose one user account (with Administrator privileges) under which to install and run MPE+.

During the installation, you may be prompted to reboot the PC, stopping the installation prematurely.

Resolution: If possible, select to reboot the PC later, and wait until MPE+ runs for the first time and finishes driver installation before rebooting. If you are forced to reboot the PC, you may need to manually resume/restart your installation so everything installs completely.

The MPE+ splash screen or window may cover up some of the driver installers or prompts.

Resolution: Move the MPE+ window or pay attention for installers showing up in the Task Bar.

You may be warned that a driver is unsigned or a publisher is unknown.)

Resolution: Unfortunately, not all driver manufacturers have signed their drivers. Pleas make sure to allow all of these drivers to install, anyway. Sometimes, it may be possible to check "Always trust software from..." to reduce the number of warnings/prompts.

MPE+ may fail to download the Apple physical support files if your PC is behind a proxy or firewall.

Resolution: Please contact AccessData Support at 800-658-5199 and we will find another way to get the needed files to you.

On Windows XP, the AccessData phone drivers for older Sanyo, LG, Motorola, and Samsung phones may not install automatically.

Resolution: Please contact AccessData Support at 800-658-5199 to get these drivers, which you can then manually install as needed.

You will only be prompted to update MPE+ once on start up. If you decide not to update, you will not be prompted again.

Resolution: Update manually via the MPE+ installer web page.

MPE+ will only recognize the SIM Card reader if it is plugged in before starting MPE+.

Resolution: Make sure the SIM Card reader is connected and empty before starting MPE+.

On some CDMA phones, MPE+ appears not extract media files.

Resolution: Some CDMA phones do not save their media files with proper extensions. You should still be able to find the media files if you extract the File System and carve for media files.

When using a Nokia Symbian phone, the agent may say its certificate has expired.

Resolution: Change the phone's date to the year 2011. This will not affect existing data on the phone.

Certain CDMA phones require a device reset in order to extract different types of data during one session of extraction and the phone will power down and not power back up. When this occurs, some capabilities will not be extracted.

Resolution: If your phone seems to be resetting itself during extraction, you may need to extract each data type individually.

Multiple subsequent extractions using some devices (Windows Mobile, Apple and Android) may fail.

Resolution: Restart MPE+ and try extracting data again.

If the user inputs the incorrect model number when extracting, that incorrect number will appear in the Quick Print Report.

Resolution: Select the correct device from the MPE+ menus when extracting data.

On a rooted Android phone, if you select the "Forensic Files Only" option, all other extraction options are ignored and only the forensic files are pulled.

Resolution: Perform the extraction for Forensic Files, then perform a new extraction to get the remaining data.

MPE+ cannot read/parse physical DD "fulldisk" images from iOS 5+ devices.

Resolution: Import the physical DD "userpartition" or logical TAR "logicaluserpartition" images for use with the iOS parsers, instead.

On some CDMA phones, the File System fails to extract during a "Select All" extraction.

Resolution: Perform one extraction selecting only the File System, then another extraction selecting everything else.

The SQLite viewer Natural View pane covers part of the DB Structure view.

Resolution: Use the slider to resize the Natural View pane.

Visualization may take a while to populate if many contacts are selected at once.

Resolution: This is currently unavoidable as MPE+ populates these views on-the-fly.

"System.OutofMemoryException" when generating a large PDF report in MPE+.

Resolution: Please try the following solutions/work-arounds

- Set your Virtual Memory (in your Windows System Properties) to the highest recommended amount
- Install "CutePDF" and click "Print PDF" to "print" the report to a PDF
- Generate an RTF or CSV report instead