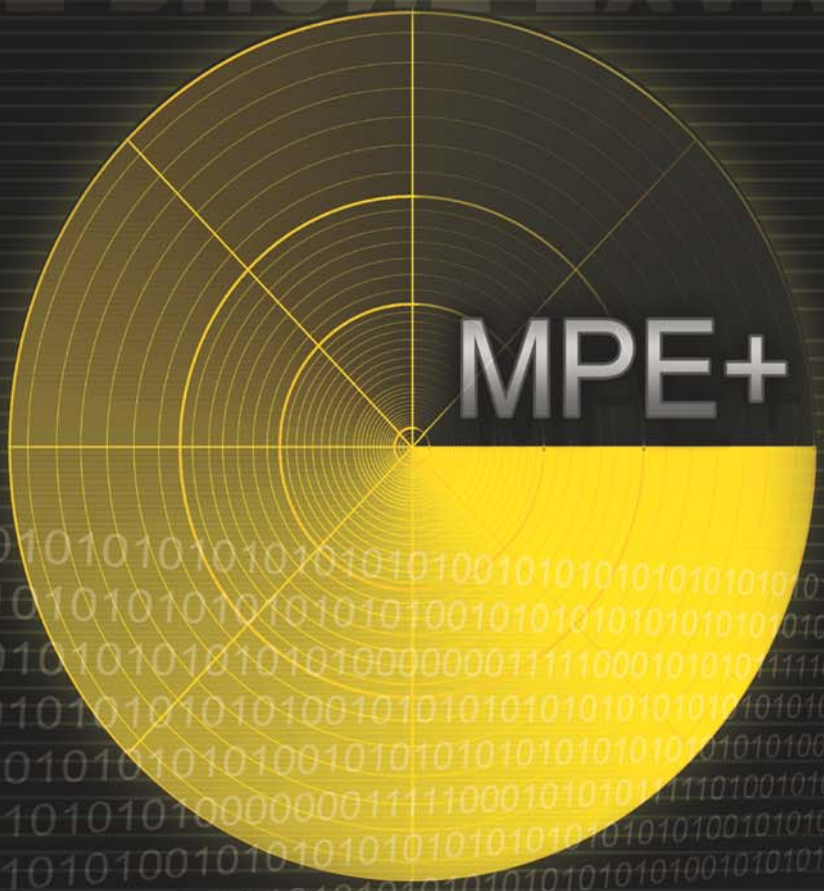
AccessData

MOBILE PHONE EXAMINER PLUS



AccessData®

A Pioneer in Digital Investigations Since 1987

AccessData Legal and Contact Information

Document date: February 2, 2015

Legal Information

AccessData Group, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, Inc.
1100 Alma Street
Menlo Park, California 94025
USA

www.accessdata.com

AccessData Trademarks and Copyright Information

AccessData®	MPE+ Velocitor™
AccessData Certified Examiner® (ACE®)	Password Recovery Toolkit®
AD Summation®	PRTK®
Discovery Cracker®	Registry Viewer®
Distributed Network Attack®	Resolution1™
DNA®	SilentRunner®
Forensic Toolkit® (FTK®)	Summation®
Mobile Phone Examiner Plus®	ThreatBridge™

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project .
- AFF® and AFFLIB® Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

BSD License: Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WordNet License

This license is available as the file LICENSE in any downloaded version of WordNet.

WordNet 3.0 license: (Download)

WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANT- ABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or

Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database. Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format. Steps that require the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use License Manager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site,

www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData website.

AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

AccessData Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, Inc. 1100 Alma Street Menlo Park, California 94025 USAU.S.A. *Voice*: 801.377.5410; *Fax*: 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales:	*Voice*: 800.574.5199, option 1; *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Federal Sales:	*Voice*: 800.574.5199, option 2; *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Corporate Sales:	*Voice*: 801.377.5410, option 3; *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Training:	*Voice*: 801.377.5410, option 6; *Fax*: 801.765.4370 *Email*: Training@AccessData.com
Accounting:	*Voice*: 801.377.5410, option 4

Technical Support

Free technical support is available on all currently licensed AccessData solutions.
You can contact AccessData Customer and Technical Support in the following ways:

AD Customer & Technical Support Contact Information

AD SUMMATION and AD EDISCOVERY	Americas/Asia-Pacific: 800.786.8369 (North America) 801.377.5410, option 5 Email: legalsupport@accessdata.com
AD IBLAZE and ENTERPRISE:	Americas/Asia-Pacific: 800.786.2778 (North America) 801.377.5410, option 5 Email: support@summation.com
All other AD SOLUTIONS	Americas/Asia-Pacific: 800.658.5199 (North America) 801.377.5410, option 5 Email: support@accessdata.com
AD INTERNATIONAL SUPPORT	Europe/Middle East/Africa: +44 (0) 207 010 7817 (United Kingdom) Email: emeasupport@accessdata.com

AD Customer & Technical Support Contact Information (Continued)

Hours of Support:	Americas/Asia-Pacific: Monday through Friday, 6:00 AM– 6:00 PM (PST), except corporate holidays. Europe/Middle East/Africa: Monday through Friday, 8:00 AM– 5:00 PM (UK-London) except corporate holidays.
Web Site:	http://www.accessdata.com/support/technical-customer-support
	The Support website allows access to Discussion Forums, Downloads, Previous Releases, our Knowledge base, a way to submit and track your “trouble tickets”, and in-depth contact information.

Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation: *documentation@accessdata.com*

Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of Summation, FTK, FTK Pro, Enterprise, eDiscovery, Lab and the entire Resolution One platform. They can help you resolve any questions or problems you may have regarding these solutions.

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

AccessData Professional Services Contact Information

Contact Method	Number or Address
Phone	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410, option 7
Email	*services@accessdata.com*

Contents

Chapter 1
Introduction

AccessData (AD) Mobile Phone Examiner Plus (MPE+) is a powerful mobile device data review tool that can be used in the field as part of a mobile field unit or in the lab. Additionally, data extracted from mobile devices using MPE+ can be easily imported into an FTK case, which offers more in-depth drill-down, categorization, full-text index searching, and all of this is right along side other digital evidence collected for a case. MPE+ can extract information such as phone and address book data, media files, call logs, SMS and MMS messages, calendar, and file system data stored in the memory of a mobile device.

Audience

MPE+ and its manual are written for law enforcement and corporate security professionals with the following competencies:

- Basic knowledge of and training in forensic policies and procedures.
- Basic knowledge of and experience with personal computers, mobile phones, enhanced PDAs, and SmartPhones.
- Familiarity with the fundamentals of collecting digital evidence from mobile devices.
- Understanding of forensic data images and how to acquire forensically sound images.
- Experience with case studies and reports.
- Basic competency with FTK.
- Familiarity with the Microsoft Windows environment.

Scope

This manual documents the available tools, functions, and other features built into the Mobile Phone Examiner Plus application. For information on proper mobile device forensics and data analysis practices, you should register for one of AccessData's beginner, intermediate, and / or specialized mobile forensics workshops.

Resources for Other Information

MPE+ Support

The AccessData Support Model is organized around a multi-level tier methodology. The Support Team consists of front-line, tier-one support technicians who provide direct communication with those who initiate the support contact. The team also consists of a second-level, tier-two resources for escalation resources for tier-one personnel, thereby providing an avenue of assistance on any issue that the tier-one technicians may not be able to resolve completely on their own.

Phone/Email Contacts

Americas/Asia-Pacific

800-658-5199 (North America)

801.377.5410 and select Option 5.

Email: support@accessdata.com

Europe/Middle East/Africa

+44 207 836 7397 (United Kingdom)

Email: emeasupport@accessdata.com

Note: Standard Support Hours are Monday through Friday, 7:00 AM - 6:00 PM (MST), except corporate holidays.

Additional Resources

- AccessData MPE+ FAQ:
  https://support.accessdata.com/hc/en-us/articles/204123005-MPE-FAQ
- AccessData User Forum:
  http://forums.accessdata.com
- Supported Phone List:
  http://accessdata.com/devices/
  You can also find supported phones in MPE+ under **Settings** > **Supported Devices**.
- Support videos:
  http://accessdata.com/product-download/digital-forensics/mpe
  You can also find supported phones in MPE+ under **Product Information** > **Training Videos**.

Chapter 2

Getting Started

This chapter contains all the information you need to get started with MPE+, including licensing your software and connecting devices to your computer. Once you have completed the information covered in this chapter, MPE+ will be ready to extract and save data from devices.

Licensing

About Licensing

To launch the application, you must have one of the following.

- A full MPE+ license
- A registered MPE+ Demo license
  See the *MPE+ Quick Install Guide*:

About MPE+ License Options

You may use one the following licensing options:

- USB CodeMeter device: See AccessData Product Licenses (page 85).
- Virtual CodeMeter: See Virtual CodeMeter Activation Guide (page 98).
- Network license: See Network License Server (NLS) Setup Guide (page 104).

See Appendix A — Managing Security Devices and Licenses (page 85) for more information on licensing.

Note: The MPE+ Field Tablet ships with a built in MPE license, and does not require an additional license.

Connecting Devices

Before you connect a device to the system for the purpose of examination, you must ensure the appropriate device drivers are installed and configured properly.

To connect a mobile device for the first time

1. Power up the device (wait until the device is fully powered on before proceeding to the next step).
2. Plug in the device data cable.
3. Check Windows Device Manager to ensure that the device is being detected correctly.
   If the device is not listed in the Windows Device Manager, double check that the appropriate driver is properly installed. For more information, see the MPE+ Quick Install Guide.
4. Once a Windows data connection has been established, you are now ready to select the device in MPE+. See Extracting Data from Mobile Devices (page 20).

Note: If you are unable to connect your device, follow the steps in Resetting a Mobile Device Connection (page 13).

Resetting a Mobile Device Connection

If you're going to process/connect a phone multiple times, power cycle the phone (remove the battery) between each connection.

To connect a mobile device

1. Exit the MPE+ application.
2. Unplug the device data cable.
3. Remove the battery cover on the device.
4. Remove the battery from the device.
5. Remove the SIM card (if applicable).
6. Properly clean all battery and SIM card contacts.
7. Reassemble the device.
8. Power up the device (wait until the device is fully powered on before proceeding to the next step).
9. Plug in the device data cable.
10. Check Windows Device Manager to ensure that the device is being detected correctly.
    If the device is not listed in the Windows Device Manager, double check that the appropriate driver is properly installed. For more information, see the MPE+ Quick Install Guide.
11. Launch MPE+.
12. Once a Windows data connection has been established, you are ready to select the device in MPE+. See Extracting Data from Mobile Devices (page 20).

About the Home Page

The *Home* page appears when you first open MPE+ or when you click the **Home** button on the *Main Ribbon*. The Home page offers you quick links to perform actions in MPE+, product information, and videos and documents that will help you utilize MPE+.

Elements of the Home Page

Element	Element	Description
Quick Links Panel		Contains links to actions in the software.
	Select Device	Click **Select Device** to open the Device Selection dialog. See Extracting Data from Mobile Devices (page 20) for more information.
	Select USIM	Click **Select SIM** to open the SIM/USIM Connection Wizard. See Unlocking a SIM/USIM Smart Card (page 37) for more information.
	Import Image File	Click to import an image of a phone. See Importing an Image (page 38) for details.
	Import IPD	Click to import Blackberry IPD files. See Importing an IPD on page 39.
	Recent Files	Provides links to recently viewed phone data. Click the link to load the data again in MPE+.
Support Panel		Contact information for support including email, phone number, and discussion forum.
Product Information Panel		Contains information about the product, documents for the product, information on other AccessData products, and access to the discussion forum.
	Training	Displays the training page from the AccessData website.
	Training Videos	Contains links to training videos for MPE+. The videos play in the player on the home page.
	What's New	Displays the new features of the current release of the product.
	User's Guide	Displays the user guide for the current release of the product.
	Products	Contains links to the landing pages of other AccessData products.
	Discussion Forum	Displays the discussion forum page from the AccessData website.
	Driver Management	Download and install device drivers.
	Physical Acquisition Support	Download files for physical acquisition of iOS data.

About the Manage Menu

Use the *Manage* menu to manage settings and options of your MPE software.

To access the Manage menu

- Click the **Manage**  button.

The following table displays the options available in the *Manage* menu. Click on the cross reference in each description to see more detailed information about how to use each of these features and options.

Manage Menu Options

Option	Description
Investigator Information	Click to open a form to enter information specific to the investigator. See Entering Investigator Information (page 78) for more information.
Settings	Click **Settings** to change the settings of MPE+. See Managing Settings (page 79).
Supported Devices	Click to see a list of MPE+ Supported Devices and cable numbers. The Supported Mobile Devices List can be exported from the list view. See Viewing Supported Devices on page 84.
User Guide	Click to open the PDF of the MPE+ User Guide. See Opening the User Guide on page 84.
About	Click to view information about your version of the product.
Save Layout	Click to save your current panel layout. See Saving Your Layout on page 83.
Load Saved Layout	Click to load a previously saved panel layout. See Loading a Saved Layout on page 83.
Reset Layout to Default	Click to reset the layout of the panels to the factory default. See Resetting the Layout to the Default on page 83.
Import Drivers	Click to import phone drivers from a file saved on your machine. See About the Home Page on page 14.
Exit	Click to close MPE+.

About the Main Ribbon

The *Main* Ribbon allows you to access the home page, select and extract from device, work with images, and create reports. The following table summarizes your options on the *Main* Ribbon. For more detailed information about each option, click the cross reference in the table description.

Buttons on the Main Ribbon

Button	Description
	Click **Home** to view the *Home* page of MPE+. See About the Home Page on page 14.
	Click **Select Device** to open the Device Selection dialog. See Extracting Data from Mobile Devices on page 20.
	Click **Extract Device Data** when the correct drivers are installed and the device is connected and has been recognized and selected. This action extracts selected data from the phone or other mobile device. See Extracting Data from Mobile Devices on page 20.
	Click **Mass Storage** to collect physical data from mass storage devices, including: SD cards, Flash Drives, Hard Drives, and so forth. See Extracting Data from Mass Storage on page 35.
	Click **Import From Triage Device** to import data from an AD Triage device that has collected information. See Importing from a Triage Device on page 40.
	Click **Extract from SIM** to open the *Device Selection* dialog. See Extracting Data from a SIM/USIM Card on page 36.
	Click **Import Folder** to import a folder that contains phone data files. See Importing Data from a Folder on page 39.
	Click **Export to AD1** to export the extracted data to an AD1 custom content image that can be added to a case in FTK. The AD1 can also be imported back into MPE+ later, without the device connected, to view the extracted data. See Exporting To an AD1 Image (page 74) for more information.
	Click **Import Image** to import an image of the phone data. See Importing an Image on page 38.

Buttons on the Main Ribbon (Continued)

Button	Description
	Click **Mount Image** to mount an image file to a drive letter on the investigation computer. This allows you to review the device image's data as a it appeared on the device.
	Click **Create Report** to open the *Print Report* dialog. This allows you to select the data types to Preview or Export. You can also print the report from the Preview window. See Creating Reports (page 76) for details.

About the Tools Ribbon

The *Tools* Ribbon allows you to parse user data from select devices, create a forensic SIM, carve files, and create/manage/activate Alerts. The following table summarizes your options on the *Tools* Ribbon. For more detailed information about each option, click the cross reference in the table description.

Buttons on the Tools Ribbon

Button	Description
	Click **Android** to parse data for Android phones. See Android Parser on page 44.
	Click **IOS** to parse data for iPhones. See Apple iOS Parser on page 44.
	Click **Deleted** to parse deleted Call History and SMS data. See Parsing Deleted Data on page 47.
	Click **iTunes Backup** to parse data for iTunes backups. See iTunes Backup Parser on page 46.
	Click **IPD/BBB** to parse data for BlackBerry phones, including BBB format. See Blackberry IPD/BBB Parser on page 45.
	Click **App AutoParser** to run pre-defined database queries to parse database data that exists in the current image. See About App AutoParser on page 47.
	Click **Read SIM** to create a forensic copy of a SIM card. See Creating a Forensic SIM Card on page 36.
	Click **Enter SIM** to manually enter the IMSI and ICCID numbers to create a forensic SIM card. See Creating a Forensic SIM Card (page 36)
	Click **Carve Files** to find data that may have been deleted from the phone but that has not been overwritten. The *Data Carve Options* box allows you to select which data types to carve if they are found. See Carving Data (page 41) for more information.

Buttons on the Tools Ribbon (Continued)

Button	Description
	Click **Manager** to create, remove, deactivate, prioritize, import, export, and save Alerts. See Alerts Manager View on page 49.
	Click **Enable/Disable Auto Filtering** to enable/disable Auto Filtering. When Auto Filtering is enabled, MPE will automatically run Alerts when AD1 files are opened in MPE+. See About Alerts on page 49.
	Click **Activate/Deactivate All Alerts** to activate/deactivate all Alerts. See About Alerts on page 49.
	Click **Run Alerts** to run the Alerts listed in Manage Alerts. **Run Alerts** is disabled until you have a supported list of information to run against the Alerts. See About Alerts on page 49.
	Click **Restore Partitions** to return the phone to its previous state. If the phone does not return to its previous state, contact Customer Support. See Connecting an Android Device for Physical Acquisition on page 24.
	Click **Configure dSOLO Mode** to configure dSOLO Mode. dSOLO Mode creates a file that extracts information from an Android device without connecting that device to the computer. See Configuring dSOLO Mode on page 26.
	Click **Read dSOLO Files** to retrieve the files collected in dSOLO Mode. See Reading dSOLO Files on page 26.

Chapter 3

Collecting Data

You can bring phone data into MPE+ in the following ways:

- Extracting Data from a Device: See Extracting Data from Mobile Devices on page 20.
- Extracting Data from Mass Storage: See Extracting Data from Mass Storage on page 35.
- Extracting Data from a SIM: See Extracting Data from a SIM/USIM Card on page 36.
- Importing Data from a File: See Importing an Image on page 38.
- Importing Data from a Folder: See Importing Data from a Folder on page 39.

Extracting Data from Mobile Devices

Once MPE+ has successfully connected to a device, data can then be extracted for review.

Note: If the codemeter is removed at any time during an extraction, the extraction will fail and MPE will close.

To extract data from a device

1. Connect the device to the computer using the appropriate cable.

   To see a list of supported devices and cables, click the **Manage**  button and select **Supported Devices**.

   For more information on connecting devices, see Connecting Devices (page 13)
2. Access the *Device Selection* dialog using one of the following methods:
   - Upon opening MPE+, select **Select Device** from the *Home* page.
   - Click the **Extraction Device Data** button on the ribbon.

   See Device Selection Options on page 21.
3. If the device is already connected, and the drivers are correctly installed, the *Identify* button is active. Click the **Identify** button to populate the *Device Identify* group box. This group box gives you the details that you need to add the Manufacturer and Model drop-down information.
4. Using the information from the *Device Identify* group box, select the correct information for the connected device from the **Manufacturer** and **Model** menus.
5. Click **Connect**.

   Note: If you are unable to connect to the device, see Resetting a Mobile Device Connection (page 13) for more information.

6. In the *Select Data for Extraction* dialog, check the data types that you want to extract from the connected device and click **Extract**. The check boxes available in this dialog are dynamic to the connected device; only the data available for extraction will appear.

   Upon completion of the extraction process, the acquired data is displayed in MPE+. Use the Data Views ribbon to review the data. For more information on how to review the data, see About Data Views (page 53).

Important Things to Note About Extraction

- Not all devices carry the same information, and not all device drivers will allow the extraction of all the data the device holds. The *Select Data for Extraction* dialog only gives you the options appropriate for the device and driver combination you have connected. If a data type is not supported on the device, you will not be able to select it in this dialog and the data will not be extracted.
- You may receive an error message indicating that some information was not able to be extracted. This is due to restraints in the device or driver you selected. Click **Ok** to continue. All extracted data will appear in the MPE+ main window.
- The Apple progress bar on the device on which you are performing a physical extraction is misleading. Although the job may complete, the progress bar will not reflect the complete status, and stops around the 90% mark.
- Certain phones require a device reset in order to extract different types of data during one session of extraction. There are cases where the phone will power down and not power back up. When this occurs, some capabilities will not be extracted. The work around for this is to extract each item individually.
- Once you have selected a device and extracted the data, before selecting another device, you must export the data in order to save the information. Do not attempt to open a second MPE+ window to select another device, this will cause conflicts in the program.
- MPE+ does not extract the current state of some iPhone/iPad devices on subsequent logical extractions. If any of the content changes on the phone and you try to re-extract without restarting MPE+, that new content will not be extracted.
- When extracting from iOS devices, connect the device directly to the machine running MPE+. Do not connect through a USB hub.

Device Selection Options

The Device Selection dialog can be accessed in the following ways:

- Upon opening MPE+, select **Select Device** on the *Home* page.
- Click the **Select Device** button on the ribbon.

Device Selection Options

Objects	Description
Manufacturer	Select the manufacturer of the connected device. You can find the manufacturer underneath the battery of the device or by clicking the **Identify** button.
Model	Select the model of the connected device. You can find the model underneath the battery of the device or by clicking the **Identify** button.
Cable #	Displays the cable number for the selected device after the manufacturer and model are selected. For more information on cables, see the Supported Devices list by clicking on Supported Devices on the Toolbar.
Advanced	Click to open the *Advanced Port Selection* dialog. From here, you can see the ports available for use on the connected device.

Device Selection Options (Continued)

Objects	Description
Identify	Click to populate the *Device Properties* group box.
Device Properties	Displays information about the connected device, including manufacturer, model, and Electronic Serial Number. Populated by clicking the **Identify** button.
Reset	Removes all selected information from the *Device Selection* dialog.
Connect	Connects to the attached device. This button is only active after a manufacturer, model, and port are selected.
Cancel	Closes the *Device Selection* dialog
Status	Displays the status of the device selection process.

Using the Advanced Dialog

Click the **Advanced** button in the *Device Selection* dialog to open the *Advanced Port Selection* dialog. This dialog shows you detailed port information.

Connecting an Android Device to MPE+ using Logical Extraction (Android)

MPE+ 4.1.0 and later requires a specific procedure for acquiring data from Android devices. This section details that procedure.

To extract data from an Android device

1. Install the proper driver for your Android phone. See the MPE+ Quick Install Guide for more information on installing drivers.
2. Ensure the phone has at least a 50% charge.
3. Activate USB Debugging mode on the phone. Activating USB Debugging mode depends on the version of Android from which you are extracting. To activate Debugging mode:
   - On most devices running Android 3.2 or older, select **Settings > Applications > Development**.
   - On Android 4.0 and newer, select **Settings > Developer options**.

   Note: On Android 4.2 and newer, Developer options is hidden by default. To unhide *Developer options*, open **Settings > About phone** and tap *Build number* seven times. Return to the previous screen and *Developer options* is available.
4. Connect the device using the correct cable. To see a list of cables, click **Supported Devices** from the *Manage* ( ) tab.
5. In *MPE+*, click **Select Device** from the *Main* ribbon.
6. Select “Android” as the **Manufacturer** and “dLogical” as the **Model** of the phone.

   Note: You can also select your specific Manufacturer and Model.
7. Click **Connect**.
8. In the *Select Data for Extraction* dialog, check the data type to extract from the connected device and click **Extract**.

Connecting an Android Device for Physical Acquisition

There are two methods for extracting a physical image of an Android device with MPE+. The method you use depends on the state of the device.

Device is Unlocked or Locked with USB Debugging On

USB Debugging is On (Device unlocked/Locked)

To extract data from an Android device

1. Install the proper driver for your Android phone. See the MPE+ Quick Install Guide for more information on installing drivers.
2. Ensure the phone has at least a 50% charge.
3. Activate USB Debugging mode on the phone. Activating USB Debugging mode depends on the version of Android from which you are extracting. To activate Debugging mode:
   - On most devices running Android 3.2 or older, select **Settings > Applications > Development**.
   - On Android 4.0 and newer, select **Settings > Developer options**.

   Note: On Android 4.2 and newer, Developer options is hidden by default. To unhide *Developer options*, open **Settings > About** submenu. In some devices, the **About** submenu is located under the **More/General** submenu. On other devices (namely HTC devices), go to **Settings> About > Software Information> More**. Tap *Build number* seven times. Return to the previous screen and *Developer options* is available.
4. Connect the device using the correct cable. To see a list of cables, click **Supported Devices** from the *Manage* ( ) tab.
5. In *MPE+*, click **Select Device** from the *Main* ribbon.
6. Select “Android” as the **Manufacturer** and “Other (Physical)” as the **Model** of the phone.
7. Click **Connect**.

Important: If MPE+ displays an error code that the device is not rooted, you will need to root the device using a third-party tool. After rooting with a third-party tool, return to MPE+ and begin the extraction process at step 6. If the shell root is successful, the Android partitions for the device return.

8. On Android 4.2 and newer devices, select **Settings > Security > Verify apps**. Deselect this feature.
9. In the *Select Data for Extraction* dialog, select the partitions to extract from the connected device and click **Extract**.

USB Debugging is Off (Device Locked)

This feature is supported for selected Android models only. Supported Android models are noted in MPE+ with "(Physical)" appearing after the model number, for example, **Samsung SGH-T989D (Physical)**. This feature is model specific and you cannot attempt on devices other than the exact model listed.

To extract data from a supported Android device

1. Connect the device using the correct cable. To see a list of cables, click **Supported Devices** from the *Manage* ( ) tab.
2. In *MPE+*, click **Select Device** from the *Main* ribbon.
3. Select "Android" as the **Manufacturer** and "Other (Physical)" as the **Model** of the phone.
4. Click **Connect**.

   Depending on the model of your device, the application displays specific instructions to place the device into recovery mode. Please read all instructions before starting the first phase.
5. At the completion of the process, select the data types to extract from the connected device from the *Select Data for Extraction* dialog and click **Extract**.

Note: If the extraction fails on some Android phones, click **Restore Partitions** on the toolbar to return the phone to its previous state. If the phone does not return to its previous state, contact Customer Support.

Important Android Notes

- After an Android Shell Root, some Android phone's SD cards may become disconnected, and you may receive the error "No device connected, insert blank SD card to continue." To be able to complete Physical extraction in this situation, you need to change the phone settings in *Settings* to:

  (SD Card or Storage) Mount SD Card
- For successful extraction of an Android Device (both logically and physically), the correct ADB driver must be installed. If you are having issues connecting to the Android device, open the *Device Manager* and verify that the ADB driver is listed under **ADB** in the *Device Manager* tree.

  The only exception to this note occurs during a physical extraction when USB Debugging is off. ADB drivers are not installed until MPE+ correctly bypasses the device protection.

dSOLO™

dSOLO™ allows you to provision a MicroSD card to extract pre-configured user data types from any Android device that has an SD card slot. With this mode, you can create an extraction profile containing the items to extract within MPE+ and then compile that profile to a MicroSD card. You can then insert the provisioned card into an Android device independent of any connection to MPE+. The configured application initiates on the Android device and the previously selected extraction capabilities are extracted from the device onto the SDCard in a format that only MPE+ can read.

When extraction completes, you can read the SDCard containing the dSOLO data using the Read dSOLO Files option from the toolbar. Once the data is read, it is immediately available for preview, reporting, and analysis in MPE+.

Once an SD card is provisioned, you can use the same SD card to extract from multiple devices using the same profile without re-configuring the SDCard.

Requirements:

- Android USB debugging must be enabled
- Computer's RSA fingerprint must be authorized (for Android 4.2 and greater)

Configuring dSOLO Mode

You can create a dSOLO configuration file and write it onto an SD card that can be used to collect the data from the target device.

Note: Make sure that the SDCard has a large enough capacity to store the extracted data of the target device or devices.

MPE+ then creates the dSOLO agent (`MPE.apk`) onto the SDCard.

To configure dSOLO Mode

1. Click **Configure dSOLO Mode** from the *Tools* ribbon.
2. Select the configuration options for dSOLO Mode.
3. Select the device from the *Device Selection* menu. This is the device where MPE+ creates the dSOLO Mode file.
4. Click **Create APK**.

Note: When writing to a device that already contains a dSOLO Configuration File, clicking **Create APK** with replace the older configuration file. To retain the older configuration file while adding configuration options, click **Refresh**.

Reading dSOLO Files

When dSOLO acquires information from the target device(s), it saves that information into a dSOLO file. dSOLO files have a `*.dSolo` extension. Before you can review any data collected using dSOLO Mode, MPE+ must import the dSOLO file.

To read dSOLO files

1. Click **Read dSOLO Files** from the *Tools* ribbon.
2. Select the dSOLO file to import.
3. Click **Open**.

> **Note:** dSOLO files are uniquely named using the date and time of extraction. Using this method, multiple collections can be conducted and stored onto one SDCard.

Acquiring Physical Apple Device Images

When acquiring Apple devices physically, you must ensure that your system is configured properly before proceeding. This section describes how to configure your system to acquire physical images of supported Apple devices.

Prerequisites

- Physical extraction files for the device. You can download the files needed from the Physical Acquisition Support tab under the Product Information pane in MPE+. For more information, see **MPE+ Quick Install Guide.**
- You may need up to 3 times the storage capacity of the device available on destination drive (or network storage).

Connecting to an Apple Device for Physical Acquisition

In order to acquire data from Apple devices, you need to complete all the prerequisites (see Prerequisites (page 28)).

Note: After the completion of DFU wizard, do not disconnect, power off, or press any buttons on the device.

To acquire data from an Apple device

1. Power on your Apple device and connect it to the MPE+ system via a USB cable. Your device should now be booted into normal mode.
2. Launch MPE+ and click **Select Device**.
3. In the *Device Selection* dialog, select **Apple** from the Manufacturer drop-down list, **i[DEVICE] (Physical)** as the Model, and click **Connect**.
4. Click **Connect**.
   The DFU wizard launches.
5. Press and hold the sleep button (the button on the top of device).
6. Slide the red button to power off and wait 10 seconds after the device has powered off completely.
7. Click **Connect**.
8. Click **Next**. You have 3 seconds to position your hands over the device's buttons.
9. At that end of the 3 second "Get Ready" count-down, press and hold the *Sleep* and the *Home* buttons simultaneously. Hold both buttons down until the countdown reaches zero.
   This is the first step towards powering on the device into DFU mode.

   Note: Press the *Sleep* button (top) before the *Home* button (bottom) if it is not possible to press both at the same time.
10. As the 10 seconds expire, prepare to release the *Sleep* button (top) while still holding the *Home* button (bottom). Release the button when prompted.
11. The wizard will automatically transition to the next slide and will begin a new countdown.

12. If successful, the wizard will say Complete!

> **Note:** If the device boots into recovery mode, you must unplug the device, and boot the device back into normal mode by holding both buttons until you see the apple logo. Then, click the yellow **Restart** button to start the wizard over again. For help see “Troubleshooting Apple Driver Mode” on page 30.

13. At this point the screen turns white, and then black (on some devices, an AccessData custom splash screen displays). Lastly, an MPE+ logo with an empty progress meter appears.
14. If the device has a passcode, MPE+ prompts you to do one of the following and click **OK**:
    - **Use Brute Force**: Select this if it is a SIMPLE passcode and you do not know the passcode of the phone. SIMPLE passcodes are commonly a 4 digit number. Upon completion, MPE will tell you the SIMPLE passcode of the device.
    - **Use Passcode**: Select this if you know the SIMPLE or COMPLEX passcode. You can then enter the SIMPLE or COMPLEX passcode and bypass the brute force methods.
    - **Get Logical Partition Only**: Select this if you are prompted with a COMPLEX passcode and are unsure of the password. You will still be able to recover data not protected by the Apple API.
15. MPE+ prompts you to choose which partitions you would like to acquire from the device. Check the items you want to extract and click **OK**.
    See Acquiring Apple Device Partitions on page 29.

> **Note:** From this point on, if you make any mistake, no cancel options will be provided. The only recourse will be to unplug the device, boot the device back into normal mode, and start the connect process again from the beginning.

Acquiring Apple Device Partitions

Before you can proceed with these steps, you must be properly connected to the device.

See Connecting to an Apple Device for Physical Acquisition on page 28..

1. When prompted to select which partitions you would like to acquire, choose one of the following:
    - Full Disk (gets user partition, OS Partition, and slack space).
    - OS partition (usually quite small, about 1GB).
    - User partition (Device storage capacity minus OS partition).
    - Decrypted user partition (Same size as user partition. This option will only be available for devices that support encrypted user partitions).
    - Logical OS Partition
    - Logical User Partition

> **Note:** During physical Apple device acquisition, once you have confirmed which partitions you want to extract, you cannot cancel the “Browse for folder” dialog in order to change the selected partitions.

2. When prompted, browse to the desired destination to save the device image.
3. When the acquisition is complete, you will receive a message indicating that the process completed successfully.

Troubleshooting Apple Driver Mode

If you are unable to connect to an Apple device, it may be because the AppleMobileDeviceDriver.exe process is hanging. For help use the steps to confirm driver mode below.

The Apple driver has two modes:

- Apple Mobile Device USB Driver
- Apple Recovery (DFU) USB Driver

> **Note:** You need to put the device into the mode appropriate for the type of extraction you are trying to do (logical vs physical extraction).

To confirm driver mode

1. Open *Device Manager*.
2. Click the **Scan for hardware changes** button.
3. Look under *Universal Serial Bus Controllers*.
4. Right click on **Apple Mobile Device USB Driver**.
5. Click **Properties**.
6. Click on the **Details** tab.
7. Notice the Value being reported.
8. Verify that the Value matches the state of the device.
9. If not, manually end the process in Task Manager.

iLogical™ Enhanced Support

In order to acquire data using iLogical™, you need to complete all the prerequisites (see Prerequisites (page 28)).

To acquire data using iLogical

1. Power on your Apple device and connect it to the MPE+ system via a USB cable.
2. Launch MPE+ and click **Select Device**.
3. In the *Device Selection* dialog, select **Apple** from the Manufacturer menu and **iLogical Device** as the Model
4. Click **Connect**.

> **Note:** When connecting to an iOS 7 Device, accept the **Trust** Dialog on the iDevice before MPE+ makes the connection. The Trust dialog may also display during the connection. If the Trust dialog displays again, select **Trust** on the iOS device to continue. If the connection fails, restart the connection.

5. Enter the iTunes backup password (if known) for the connected device Leave this field blank if backup encryption is turned off or you do not know the password.
6. If the device is locked with a passcode, use the pairing record to extract a logical image. Select a pairing plist and click **OK**. See About Pairing Records on page 31.
7. Select the available data options to extract from the device and click **Extract**. See Selecting Data For Extraction on page 32.

About Pairing Records

A pairing record is a file containing certificates and keys that identify the desktop machine with the mobile device, so that data can be accessed even while the device is locked. When an iOS device is first connected to a desktop machine, it establishes a trusted relationship with the machine, at which point a pairing record is written to disk. Investigators may be able to recover pairing record files from desktop machines that were previously paired with the target device by either extracting them from the file system or using AccessData's Triage product.

Finding Pairing Records on a Local Machine

The folder locations of pairing records varies depending on the operating system of the desktop machine, as follows:

Windows 7

C:\ProgramData\Apple\Lockdown

OSX

/var/db/lockdown/

or

/Users/*/Library/Lockdown/

Windows XP

C:\Documents and Settings*\Local Settings\Application Data\Apple Computer\Lockdown

Windows Vista

C:\Users*\AppData\Roaming\Apple Computer\Lockdown

Selecting Data For Extraction

Depending on the firmware version running on the device, different capabilities display when auto-detected by MPE+. After completing the connect window, MPE+ attempts to connect to the device to determine its capabilities and present the data possibilities in the Select Data for Extraction dialog. These data possibilities include:

Apple Backup Service

The Apple Backup Service capability extracts much of the device's user data by creating a backup of the device, in a similar way that iTunes creates a backup. This data is then parsed and read into MPE+. If the device's owner has enabled backup encryption, the backup password will be required in order to decrypt and read this data. This capability delivers:

- Application Data
- Bookmarks
- Browser History
- Calendar Call
- History
- Contacts, Cookies, Corrected Text, Notes, SMS, User Preferences, and other standard user data
- Filesystem

Application Network Usage and Diagnostics

The Application Network Usage and Diagnostics capability provides a diagnostic dump of applications installed on the device, and a day-by-day breakdown of network bandwidth usage in kilobytes. In addition to network usage, this capability delivers general identifying information about the device, such as:

- the device's assigned name, model, serial number
- disk capacity information
- battery cycle count
- iCloud conflict information.

Note: This data is accessible through the Files artifact section and can be found in the diagnostics folder.

Device Diagnostics

When using the Device Diagnostics capability, device information such as:

- battery cycle information
- WiFi
- HDMI
- and other low level information is acquired.

Note: In addition to this, an IORegistry path is downloaded from the device as well. This data is accessible through the Files artifact section and can be found in the diagnostics folder.

Entire File System (/)

A majority of jailbreak tools install a new service on the device, allowing the entire file system to be accessed. If the target device has had a jailbreak installed, this capability may be available if the jailbreak tool that was used created this service. By selecting this service, the entire file system is acquired from the device and logged into the Files artifact section.

Extended Third Party Application Data

While the Apple Backup Service provides a reasonable amount of third party application data, selecting this capability will cause MPE+ to acquire all of the caches and databases related to each App Store application installed on the device, which can sometimes include:

- downloaded page caches
- user credentials
- databases of friends, accounts, and other such data.

Note: The acquired data from this capability can be found in the Files artifact section inside the file system, within the path /private/var/mobile/Applications. A separate folder will be created for each third party application, and will be named after the application's bundle identifier.

Extended User and System Databases

The Extended User and System Databases capability provides a significant portion of the user file system and is independent of any backup encryption on the device. When used, this capability delivers the following information un-encrypted, even if you do not know the backup password of the device:

- Lockdown and lockdown service logs
- Apple support data and crash logs
- User "Cache" folders
  - Screen captures of suspended applications

    - Cached web data stored by various applications
    - Pasteboard (clipboard) data
    - Icon cache
    - Safari reading list archives, recent searches, and activity thumbnails
    - Video conference history of local IP + date of call
    - Map tile database (of stored / viewed map tiles)
- Apple TV playback logs, if acquiring an Apple TV with normal lockdown
- Storage proxy logs
- Bluetooth diagnostic information
- The application installation log
- Some PPP and VPN data
- A complete dump of all activation and pairing records
- Core Location cache
- Keyboard (typing) caches
- System Configuration information
    - WiFi AP join history / auto-join info)
    - Captive portal configuration (WiFi networks that present a web page)
    - Mobile Gestalt
- A dump of the SMS database, SMS attachments, and SMS drafts (un-sent SMS)
- A dump of various user databases (Address Book, Address Book Images, Envelope Index)
- A dump of the user's voice mail stored on the device (including unread)
- The user's entire photo album, music collection, and media
- System configuration data, such as accounts and WiFi pairing history
- iCloud local cache and control files
    - Lists of artifacts stored in iCloud
    - Lists of other devices (and computer names) synced with same iCloud
- The tmp directory, which often contains useful data
- A directory structure containing information about all files on /var

User Media Folder (/var/mobile/Media)

The User Media Folder capability downloads the entire user’s media folder, which includes:

- iTunes music
- photo reel and album
- iBook downloads
- purchase information
- personal recordings

Note: This information can be found in the Files artifact section, within the file system under /private/var/mobile/Media.

Extracting Data from Mass Storage

MPE+ can extract data from mass storage devices including SD cards, Flash Drives, Hard Drives, and so forth.

To extract data from a mass storage device

1. Click **Mass Storage** on the Main toolbar.
2. Select and enter either a *Physical Image* or *Logical Image*.
3. Click **Next**.
4. Click **Add** to add *Image Destination(s)*. You can also edit or remove existing image destinations.
5. Select the *Destination Image Type*. You can also add notes or a description (optional).
6. Click **Next**.
7. Enter the *Image Destination Folder*, the *Image FileName*, and the *Image Details*.
8. Click **Finish**.

Extracting Data from a SIM/USIM Card

MPE+ can acquire SIM/USIM card data via most “personal computer smart card” (PC/SC) compatible adapters.

To extract data from a SIM card

1. Insert the SIM/USIM card into the card reader device.
2. Connect the card reader device to the computer.
3. Do one of the following:
   - Click **Select USIM** from the *Home* page.
   - Click the **Extract from SIM** button from the application toolbar.

> **Note:** If the SIM/USIM is protected by a PIN then you will be offered a connection dialog indicating the status and options to unlock the SIM/USIM.
> See Unlocking a SIM/USIM Smart Card (page 37) for more information.

4. In the *Select Data for Extraction* dialog, check the data types that you want to extract from the connected device and click **Extract**.

> **Note:** The *File System* option will retrieve all standard SIM card file system data, whereas the *Deep File System* option extracts the file system, plus the file structure above and beyond the standard SIM files and folders (such as service provider files stored on the SIM card).

Upon completion of the extraction process, the acquired data is displayed in the Data Views ribbon. For more information on how to review the data, See About Data Views on page 53..

Creating a Forensic SIM Card

You can create a Forensic (U)SIM card using a PC/SC Reader and the MPE+ Forensic SIM that comes with MPE+. The creation of a Forensic SIM allows you to read the necessary data from the original (U)SIM and transfer this data to the MPE+ Forensic SIM. You can then place the Forensic SIM in the cellular phone and obtain complete network isolation while the device is in the ON position.

Manually entering the IMSI and ICCID numbers is useful when the phone is carrier locked and won’t start/extract without a SIM. You can manually look up a carrier IMSI and then enter it into MPE+ using the **Enter SIM** button on the *Main* ribbon.

To create a Forensic SIM Card

1. Select the **Forensic SIM** button from the ribbon.
2. Insert the original (evidence) (U)SIM into the card reader and click **OK**.
3. Verify that the SIM information is correct and click **Continue**.
4. Insert the MPE+ Forensic SIM Card that came with your MPE+ software into a PC/SC card reader and click **OK**.

   MPE+ writes the captured data from the original (U)SIM to the MPE+ Forensic SIM
5. Immediately following the writing process, you are given a log indicating the success or failure of the write. This information contains the HASH values of the original AND the MPE+ Forensic SIM. This information can be saved to a text file to include in the final report. Click **Save**.

6. Browse to the location where you want to save the log, name the log, and then click **Save**.
7. Click **OK**.

Unlocking a SIM/USIM Smart Card

The Subscriber Identification Module (SIM) standard uses a series of Personal Identification Numbers (PIN) to authenticate those who are attempting to access the data stored on the card. PIN1 is required to unlock the majority of the SIM storage. PIN2 unlocks vendor specific storage.

All SIM cards are designed to protect themselves from unauthorized access. For example, both PIN1 and PIN2 enforce a 3 attempt lock out policy. In the case that all attempts to enter the correct PIN have been exhausted, the PIN Unlock Key (PUK) must be provided. A PUK can be generated by the service provider based on the CCID number of the SIM card. MPE+ supports PINs and PUKs between 4 to 8 numeric characters in length.

Note: DON'T use up all remaining attempts to enter a PIN and / or PUK. If you don't have the PIN, you may need to contact the service provider to get a PIN unlock key (PUK).

To unlock a SIM / USIM smart card

1. Open the *SIM / USIM Connection Wizard* dialog. (When connecting to a protected (U)SIM you will be met with a dialog to enter the (U)SIM security information.)
2. If you have more than one card reader attached to the system, drop down the *SIM/USIM Readers* menu and confirm that you are working with the appropriate card. Otherwise, move on to the next step.

   Note: The unique card identification code (ICCID) can be used to identify which card is currently being read.

3. Enter the current key codes for either PIN1 or PIN2. If you don't know the current PIN number, try resetting the PIN. See Resetting the PIN (page 37).
4. Click **Unlock**.

   If successful, you will be prompted with the *Select Data For Extraction* dialog. For help on completing the extraction, see Extracting Data from a SIM/USIM Card (page 36).

Resetting the PIN

In the case that you do not know the PIN number (required to unlock a SIM card for the purpose of extracting the data it contains), you can reset the PIN to a new value if you have the Pin Unlock Key (PUK). SIM cards grant you 10 attempts to enter the correct PUK before the card is locked permanently.

Note: DON'T use up all remaining attempts to enter a PIN and / or PUK. If you don't have the PIN, you may need to contact the service provider to get a pin unlock key.

To Reset the PIN

1. Open the *SIM / USIM Connection Wizard* dialog. (When connecting to a protected (U)SIM you will be met with a dialog to enter the (U)SIM security information.)
2. If you have more than one card reader attached to the system, drop down the *SIM/USIM Readers* menu and confirm that you are working with the appropriate card. Otherwise move on to the next step.

Note: The unique card identification code (ICCID) can be used to identify which card is currently being read.

3. Click the **Use PUK** button that corresponds to the PIN code you want to reset.
4. Enter the current PUK key codes for either PIN1 or PIN2.

   If you don't know the current PUK code, you will need to contact the service provider. They will need the Card Identification number (ICCID) in order to generate a PUK.
5. Type a 4 to 8 character numeric value (to which you want to reset the PIN number) into the corresponding *New PIN* number field.
6. Click **Reset PIN**.

   If successful, you will be prompted with the *Select Data For Extraction* dialog. For help on completing the extraction, see Extracting Data from a SIM/USIM Card (page 36).

Importing an Image

You can import image files into MPE+. This accommodates the need to revisit an image prior to adding it to an FTK case.

You do not need to have the original source device connected to import an image that was previously exported. The following image formats can be imported:

- AD1
- FAT
- E01
- YAFFS
- YAFFS2
- EXT
- EXT2
- EXT3
- EXT4
- TAR
- RFS
- DD4
- DD8
- DD4.001
- DD8.001

To import an image into MPE+

1. Do one of the following:
   - Select the **Import Image File** from the Home page.
   - Click the **Import Image** button on the *Main* ribbon.
2. Browse to the folder containing the image file.
3. Select the file.
4. Click **Open**.

Importing an IPD

You can import a BlackBerry IPD backup file into MPE+. This allows you to get the phone files without extracting directly from the device.

To import an IPD file

1. Do one of the following:
   - On the *Home* page, select **Import IPD**.
   - Click the **IPD** button on the *Main ribbon*.
2. Browse to the folder containing the image file.
3. Select the file.
4. Click **Open**.

Importing Data from a Folder

You can import a folder that contains phone or iTunes files into MPE+.

Note: You can import multiple folders using multiple imports. When importing another folder, click **YES** when prompted to add the folder to the existing filesystem.

To import a folder

1. On the *Main* ribbon, click the **Import Folder** button.
2. Browse to the folder and click Select Folder.
   The folder contents appear in the Files data view.

Importing and Reviewing from an AD Triage Device

MPE+ allows you to review data captured using AccessData Triage. AD Triage is a tool used for on-scene preview of data and to collect from computers that are live or have been shut down. With the partnership between MPE+ and AD Triage, you can:

- Import AD Triage collected data
- Create reports with the AD Triage data
- View AD Triage data in Data Views
- Use alerts and other MPE+ tools with AD Triage data
- Import phone backup files for Apple and Blackberry devices after the Phone Profile is utilized by AD Triage
- Locate lockdown plist files from desktops and laptops using AD Triage, and then utilize the collected data in MPE+.

Note: Note: Using the lockdown plist files, you can unlock iOS devices that are PIN or Password protected.

Importing from a Triage Device

A Triage device contains information collected from a target computer and is stored on a flash drive. To review the device's information in MPE+, you must first import the data into MPE+.

Note: Triage information may also be saved into an AD1 file and imported as an image. For directions on importing an AD1 file, see Importing an Image (page 38).

To import from a Triage Device

1. Insert the Triage device into the USB port of the MPE+ computer.
2. Click **Import From Triage Device** from the *Main* ribbon.
3. Follow the prompts to complete the import.

Reviewing Data Collected from Triage

Once the Triage data is imported into MPE+, you can review it in *Data Views*.

To review data

1. After importing the Triage data, click the *Data Views* tab.
2. You can now review the information collected by Triage. For more information on Data Views, see About Data Views (page 53).

Chapter 4

Reviewing Data

After you have extracted or imported phone data into MPE+, you can then review that data for relevancy. In order to find relevant data you can use MPE+ to carve out data and parse data. You can then view all the phone data in the MPE+ interface.

- See Carving Data on page 41.
- See Parsing Data on page 44.
- See About Data Views on page 53.

Carving Data

Carved files are the result of scanning through the device's stored data for files that have been deleted or embedded within other files. When the MPE+ carving process encounters a file signature that matches the signature for which you are carving, it will extract that file as a separate file record. For example, by carving for multimedia files, you may be able to recover incriminating 3GP video evidence found in a MMS text message.

Using the data carving feature, you can choose what types of files to carve from the device's data storage media. See the following table for a list data types that can be carved by MPE+.

Data Carve File Types

Images	Documents
• JPEG	• HTML
Video	**Audio**
• 3G2	• MP3
• 3GP	• AMR
• MPEG	• QCP
• MP4	

Carved data is not saved as a separate part of the phone data. It is also not exported to an MPE+ AD1 image. Its only purpose is to provide a preview of what can be found in the phone when the exported MPE+ AD1 image is added and carved in FTK. Saving or exporting carved data to an MPE+ AD1 image would result in duplicate data when that image is added to a case.

After the image is added to FTK, the items identified by carving in MPE+ must be re-carved to be added to the case.

However, items carved in MPE+ can be reported immediately using the Quick Print function, saving a report of the carved items to a PDF file, or printed.

Once data is carved, it is not saved, and cannot be retained and appended with data from subsequent carving operations. Repeating the carving process discards the previously carved data and replaces it with newly carved data. Keep this in mind if you carve one type of data and then want to add to the list by carving other data types. To do so, on subsequent carve operations, you must choose all the file types you want to see results for in a single carve.

Note: If you extracted from a SIM, you must export the data to an AD1 file before you can carve the data.

Running a Data Carve

To run a data carve

1. Click the **Carve Data** button on the *Main* ribbon.

   Note: If you have already done a data carve on the collected phone data, you will be asked if you want to discard the data and do a new carve; click Yes to continue.

2. In the *Data Carve Options* dialog, check the folders in the file system that you want to include in your search, as well as the data types to carve.
3. Click **Continue**.

   The Data Carving progress dialog displays.
4. When carving is complete, the **Cancel** button deactivates and the **Close** button activates. Click **Close**.

   The carved data list is displayed in the *Carved Data*, *Data View*.

Viewing Carved Data

After you have carved out data, you can view the data in the *Data Views* ribbon.

To view Carved Data

- Click the **Data Views** ribbon, then click **Carved Files**.

The Gallery pane displays graphic thumbnails of the files you carved. You can customize the Gallery, Hex, and Natural panes the same way you can customize any of the panels in your layout.

See Customizing Your Layout on page 82.

Selecting a graphic thumbnail will highlight the file in the file list. The file list displays the file name, path, and size of the files. You can also view the file in the Natural or Hex view.

Note: Carved HTML files are best viewed in the Hex Tab.

Filtering by Column in Data Views

You can filter the evidence in the *Data Views* ribbon by the data in the columns. You can apply multiple column filters.

To filter evidence by data in columns

1. Select a Data View.
2. In a pane with columns, click the column filters button  .
3. (Optional) Select the items that you want to continue viewing in the pane.
4. Select a criteria to use for your filter from the drop-down menu, and then enter text associated with the criteria in the text field.
5. To include a second criteria, select a connector from the second drop-down menu. Select a criteria from the third drop-down menu, and then enter text associated with that criteria in the text field.
6. Click **Filter**.

Clearing Column Filters

You can clear column filters that you have applied to a Data View.

To clear column filters

1. Select a Data View.
2. In a pane with columns, click the column filters button  .
3. Click **Clear Filter**.

Parsing Data

After you bring your data into MPE+, you can parse the data for the following devices:

- Android Parser (page 44)
- Apple iOS Parser (page 44)
- Blackberry IPD/BBB Parser (page 45)
- iTunes Backup Parser (page 46)

You can also parse data from the file system data view, as well as parse deleted call history and SMS data.

See Parsing Data from the File System on page 46.

See Parsing Deleted Data on page 47.

Android Parser

MPE+ can parse and collect many data types when the data in the Forensic Files Only option is obtained for the Android file system. This additional capability is obtained if utilizing a logical read on a temporarily rooted or permanently rooted device.

Additionally, physical images imported into MPE+ can now be additionally parsed utilizing the Android Parser OS. Once you mount a physical userdata partition from the Android device, you uncover and collect:

- Application Data
- Book Marks
- Call History
- Email
- IMaccount
- MMS
- Phonebook
- Searches
- SMS

To use the Android parser

1. Load data by either extracting from a device or importing an image.
2. On the *Main* ribbon, click **Android**.
3. Check the data that you want to include and click **Extract**.

Apple iOS Parser

Utilizing the iOS parser allows for the collection of many new data types. You can mount a physical iOS image, either full disk, user partition or TAR file, in MPE and navigate to the iOS parser. You can also import a file system obtained utilizing another tool. With the iOS parser, you can uncover and collect:

- Application Data
- Applications
- Book Marks

- Browser History
- Calendar
- Call History
- Cookies
- Corrected Text
- Email
- Locations
- MMS
- Notes
- Phonebook
- SMS

To use the iOS parser

1. Load data by either extracting from a device or importing an image.
2. On the *Main* ribbon, click **iOS**.
3. Check the data that you want to include and click **Extract**.

Blackberry IPD/BBB Parser

You can parse Blackberry IPD and BBB files. IPD and BBB files recovered on a personal computer can now be imported into MPE+ as well as backups of IPD files collected using Blackberry Desktop Manager 6.0 or earlier. Data types extracted from Blackberry IPD files include:

- Bookmarks
- Calendar
- Call History
- Corrected Text
- Email
- HotList
- Locations
- Memo
- MMS
- Phonebook
- PIN Messages
- Searches
- SMS
- URLs

To use the IPD parser

1. On the Main ribbon, click **IPD**.
2. Select the file or files and click **OK**.

Note: If there is a BBB file, you can right-click the BBB file and click **Extract**.

3. Check the data that you want to include and click **Extract**.

iTunes Backup Parser

You can parse data from an iTunes backup file. Data types extracted from iTunes backup files include:

- Book Marks
- Calendar
- Call History
- Cookies
- Email
- Memo
- MMS
- Phonebook
- SMS
- URLs
- Webkit

To use the iTunes parser

1. Load data by either extracting from a device or importing an image.
2. On the *Main* ribbon, click **iTunes Backup**.
3. Select the file or files and click **OK**.
4. Check the data that you want to include and click **Extract**.

Parsing Data from the File System

You can parse iOS, Android, and backup data from the Files data view.

To parse data from the file system

1. Load data by either extracting from a device or importing an image for an Android, iPhone, or BlackBerry.
2. Click on the **Data Views** tab and click **Files**.
3. Right-click in the *Folder Tree* pane of the *File System* data view and select one of the following:
   - **Parse iOS Folder for User Data**: Select this to parse data for an iPhone.
   - **Parse Android Folder for User Data**: Select this to parse data for an Android phone.
   - **Parse iOS Backup for User Data**: Select this to parse data for an iTunes backup.
   - **Export Folder:** Select this to export the file to a chosen destination.

Parsing Deleted Data

You can parse deleted SMS and call history data from Android and iOS devices.

To parse deleted data

1. Load data by either extracting from a device or importing an image for an Android or iOS device.
2. On the *Main* ribbon, click **Deleted.**
3. Select **Call History, SMS**, or **Select All.**
   - Click **Extract.**

About App AutoParser

App AutoParser allows you to choose from the queries contained in the \AccessData\Sqlite Scripts\ folder to parse databases in the current image. See Reviewing Databases on page 65. This feature allows you to extract any applications in the device filesystem or imported folder with a pre-created query for both Android and iOS.

Using App AutoParser allows the collection of application data from supported queries without the knowledge of where that application is located in the device filesystem. Using App AutoParser, you can select and run all application queries from the displayed list. MPE+ then searches for the application database and runs the associated query when/if the database is located. The results are displayed in the MPE+ interface.

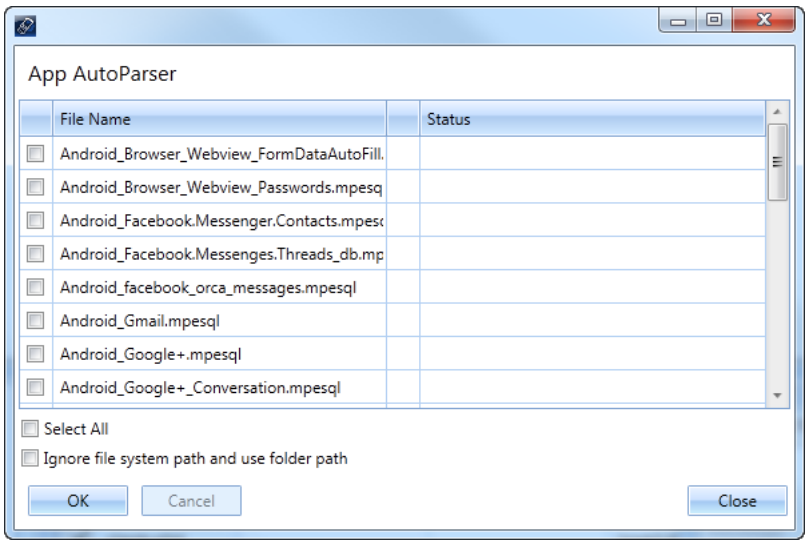
Any query built with the MPE+ SQL Builder auto-populates in the App AutoParser dialog. You can select all, select only iOS, select only Android, or select unidentified OS applications. Once the queries run, MPE+ displays whether the file was located and if the parsing was successful. See Using SQL Builder on page 65.

Note: AccessData provides queries on the user forum to use for many of today's applications. To use these queries, download the queries and copy them to the \AccessData\Sqlite Scripts\ folder. Once the queries are copied, they are immediately available in App AutoParser.

Using App AutoParser

To open App AutoParser

1. Click **App AutoParser** on the *Tools* menu.



2. Select the script(s) to execute. You can select all of the scripts by selecting **Select All**.
3. (Optional) Select **Ignore files system path and use folder path**. Use this option when the target database resides in a separate folder that you may have imported. When selected, App AutoParser ignores the system path provided by the device being imported and uses the folder path where the databases reside. MPE+ then ignores the system path provided in the built query and uses the database name instead. You can use this option:
   - If the path has changed, or
   - The file was not located but you know that the application is in the filesystem.
4. Click **OK**. While the scripts are running, you can cancel them by clicking **Cancel**.
5. After the scripts complete, you can either continue running scripts or you can exit the App AutoParser dialog by clicking **Close**.

> **Note:** After closing the dialog, all query results are located in separate tabs in the MPE+ interface. The tabs are uniquely identified by the name of the database parsed.

About Alerts

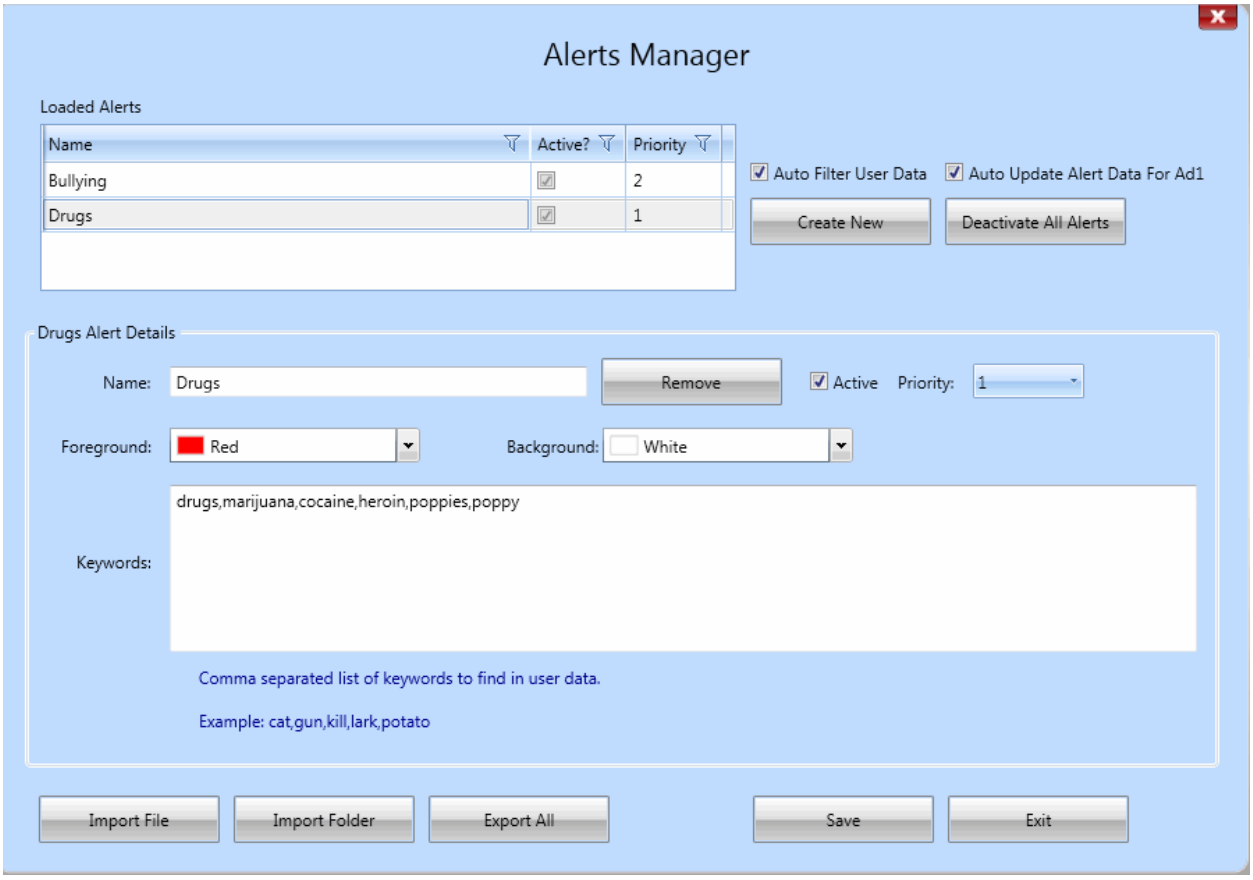
Alerts allow you to create keywords in which MPE+ flags extracted data that is associated with those keywords. You can also manage alerts with the Alerts Manager View located on the Tools menu. With Alerts:

- You can view information found by the Alerts filter. Any alert keywords that are found are tagged in the *Alerts* column by displaying the name of the alert and the color designated for that alert.
- You can view the status of an alerts scan in the MPE+ status bar. When an alert is running, an animated yellow circle indicates the alert filter search is in progress. A blue circle indicates when the alert is not running.
- You also have the option to activate or deactivate alerts.

Alerts Manager View

The Alerts Manager View allows you to create, edit, and delete Alerts, import and export Alert Settings files (*.alertSettings), activate/deactivate Alerts individually or together (All Alerts), prioritize Alerts, and customize how Alerts display when keywords are found.

Alerts Manager View



Alerts Manager Options

Option	Description
Loaded Alerts	Displays a list of all the current Alerts and includes the Alert's name, activity status, and priority. For this pane, you can activate/deactivate Alerts by selecting/deselecting the check box in the *Active?* column.
Create New	Allows you to create a new Alert. After you click **Create New**, you can enter the name and any keywords in the *Alert Details* pane.
Deactivate/Activate All Alerts	Allows you to select or deselect the **Active** option next to all of the alerts listed in the *Loaded Alerts* pane.
Auto Filter User Data	Filters user data automatically when available in MPE+. This feature is selected by default.
Auto Update Alert Data for AD1	Automatically updates and attaches Alert data to the AD1 file associated with the Alert. When this check box is NOT selected, you are prompted each time you close/ save an AD1 to update Alert data for that particular AD1 file. This feature is selected by default.
Alert Details	Displays the Alert's name, activity status, priority, foreground/background colors, and keywords. When creating a new Alert, you enter the name and keywords into the *Alert Details* section and customize the other options as necessary. You also edit Alerts in the *Alerts Detail* pane.
Remove	Deletes the Alert displayed in the *Alert Details* pane.
Foreground/ Background	Allows you to change the foreground and background color that displays in the *Alerts* column of the results table.
Keywords	Allows you to enter and/or view keywords for the Alert. You must separate all keywords with a comma.
Priority	Prioritizes the Alert as to the row being examined in the data table. When the highest priority Alert matches keywords in a row, the Alert tags the row and continues to the next row. For example, if you are running "priority 1," "priority 2," and "priority 3," and the Alert finds a "priority 1" in a row, the Alert continues to the next row, even if that row has "priority 2" and/or "priority 3" keywords.
Export All	Allows you to export the alerts displayed in the *Alerts Manager*. This feature allows you to save groups of alerts. For example, you may have various alerts with keywords associated with bullying. You could export those alerts and name the Alerts Settings file **Bully.alertsSettings**. The next time you are investigating a bullying case, you can import **Bully.alertsSettings** and use the same alerts again. You can also share alerts settings files with other investigators.
Import File	Allows you to import *Alerts Settings* files. *Alert Settings* file have an ***.alertSettings** extension.
Import Folder	Allows you to import a folder containing multiple alerts settings.
Save	Saves the Alert that is currently displayed in the *Alert Details* as well as any changes made to the other options in the *Alerts Manager*.
Exit	Closes the *Alerts Manager* and opens MPE+'s *Home* page. If you have not saved the alerts, MPE+ prompts you to save or discard your changes before continuing.

Creating an Alert

You can create alerts to help investigate and identify evidence using keywords.

To create an Alert

1. Click **Tools > Manage Alerts**.
2. Click **Create New**.
3. Click in the *Name* field and enter a name for the new Alert.
4. Click in the *Keywords* field and enter each keyword, separated by a comma.
5. (Optional) Change the *Activity* status, *Priority*, and/or the *Foreground/Background*.

Note: The only required fields when creating an Alert are the Name and Keywords fields. The other Alert options will remain the default if you do not change them.

6. Click **Save** to save the Alert.
7. If you have more Alerts to create, begin again at step 1. When finished creating Alerts, click **Exit**.

Importing/Exporting Alerts Settings files

You can import and/or export Alerts Settings files. This allows you to create different sets of Alerts, export them, and then import them when needed. For example, you may have a set of alerts that deal with finding drug evidence. You can export those alerts and save them as Drugs.alertsSettings. The next time you are investigating data that deals with a drug investigation, you can import Drugs.alertsSettings and use those alerts again in your investigation. You can also share Alerts Settings files with other investigators.

To export an Alerts Settings file

1. Click **Tools > Manage Alerts**.
2. Click **Export All**.
3. Enter a filename for the export file and click **Save**.

Note: The Alerts Settings file is saved with an ***.alertSettings** extension.

Note: Alerts with the same name are overwritten and only one alert with that name is exported. To keep all your alerts during an export, verify that they each alert has a unique name before exporting.

To import an Alerts Settings file

1. Click **Tools > Manage Alerts**.
2. Click **Import File**.
3. Navigate to the Alerts Settings file to import.

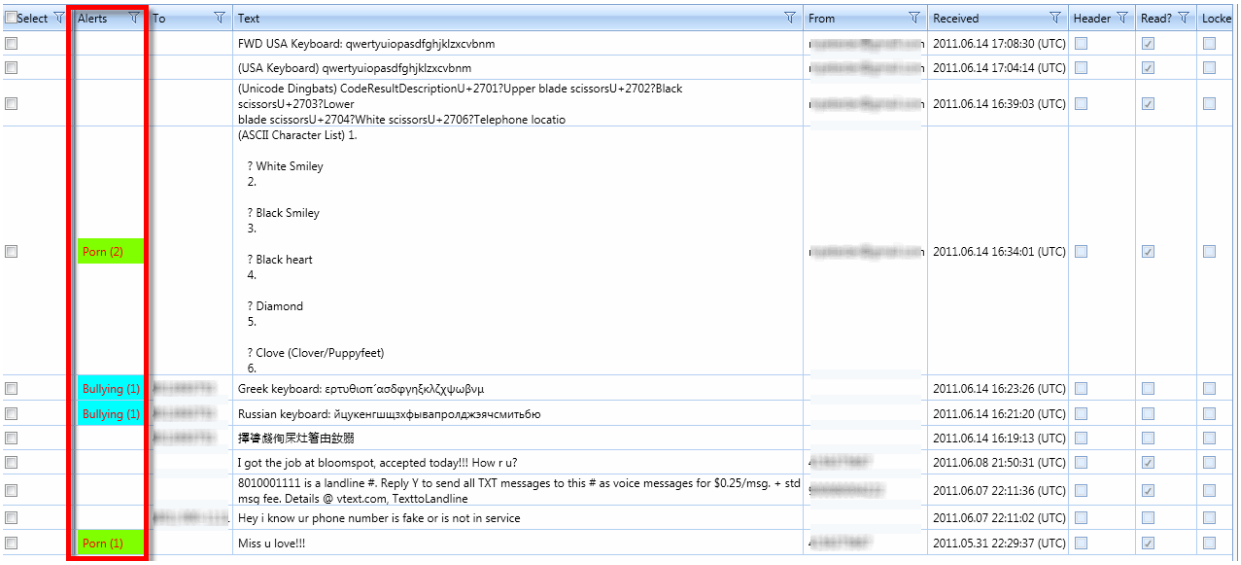
Note: Alerts Settings files have an ***.alertSettings** extent ion.

4. Highlight the file and click **Open**.

Finding Alert Results

After running Alerts on data you are investigating, the *Alerts* column will display the Alert that has matching keywords in the offending row. The Alert status also displays in the color schema configured in the Manage Alerts pane. To display the keyword(s) and the keyword count for that row, hover the mouse pointer over the alert name.

Example of Alerts Column



Select	Alerts	To	Text	From	Received	Header	Read?	Locke
			FWD USA Keyboard: qwertyuiopasdfghjklzxcvbnm		2011.06.14 17:08:30 (UTC)			
			(USA Keyboard) qwertyuiopasdfghjklzxcvbnm		2011.06.14 17:04:14 (UTC)			
			(Unicode Dingbats) CodeResultDescriptionU+2701?Upper blade scissorsU+2702?Black scissorsU+2703?Lower blade scissorsU+2704?White scissorsU+2706?Telephone locatio		2011.06.14 16:39:03 (UTC)			
	Porn (2)		(ASCII Character List) 1. ? White Smiley 2. ? Black Smiley 3. ? Black heart 4. ? Diamond 5. ? Clove (Clover/Puppyfeet) 6.		2011.06.14 16:34:01 (UTC)			
	Bullying (1)		Greek keyboard: ερτυθιοπ΄ασδφγηξκλζχψωβνμ		2011.06.14 16:23:26 (UTC)			
	Bullying (1)		Russian keyboard: йцукенгшщзхфывапролджэячсмитьбю		2011.06.14 16:21:20 (UTC)			
			擇嗜越侮呆灶箸由鈸腸		2011.06.14 16:19:13 (UTC)			
			I got the job at bloomspot, accepted today!!! How r u?		2011.06.08 21:50:31 (UTC)			
			8010001111 is a landline #. Reply Y to send all TXT messages to this # as voice messages for $0.25/msg. + std msg fee. Details @ vtext.com, TexttoLandline		2011.06.07 22:11:36 (UTC)			
			Hey i know ur phone number is fake or is not in service		2011.06.07 22:11:02 (UTC)			
	Porn (1)		Miss u love!!!		2011.05.31 22:29:37 (UTC)			

About Data Views

The Data Views tab allows you to quickly access the type of information in which you are interested by clicking on the corresponding button. Additionally, the Multimedia, File System, MMS, and Carved Data views all feature a HEX viewer and a “Natural” viewer.

The HEX viewer displays the raw data as represented in hexadecimal characters as well as the ASCII representation of those values (shown in the far right column). The far left column provides the hexadecimal offset of the line relative to the beginning of the file. This viewer also features a **Find...** button which allows you to search the file contents for a particular key word (Text) or hex string (Hex).

The Hex viewer contains a Hex Interpreter that automatically converts highlighted hex bytes into various formats.

The Natural viewer automatically displays the selected file using the most appropriate viewer available. If the file selected is a multimedia file, MPE+ will switch to a graphic or video viewer to display the audio and or video content.

Note: MPE+ has no way of knowing if the time stamp associated to an extracted file was recorded by the device using local time or UTC. You as the examiner are responsible to research this attribute for each individual device.

Use the buttons in the Data Views ribbon to browse the available mobile device data.

The buttons in the Data Views ribbon are only activated if the device from which the information was extracted supports that type of data extraction.

Data Views are dynamic to the device from which you have extracted data. Only the columns and grids that contain data are shown in the Data View. MPE shows all data that is returned from the phone. This allows more data to be available to you on some phones.

The following table describes the buttons in the Data Views pane.

Data Views Navigation Ribbon

	Click the *Device Information* button to view the specific details of the phone, including manufacturer and model.
	Click the *Contact List* button to view the phone book data that was extracted or imported. See Contacts Data View on page 56.
	Click the *Call History* button to view the call history that was extracted or imported. See Call History Data View on page 56.
	Click the *Calendar* button to view the calendar extracted or imported. See Calendar Data View on page 56.

Data Views Navigation Ribbon (Continued)

	Click the *Media* button to view all media, including pictures, video, sound, etc. that was extracted or imported. See Media Data View on page 56.
	Click the *Files* button to view the file tree and files that were extracted or imported. See File System Data View on page 56.
	Click the *Bookmarks* button to view the web bookmarks that were extracted or imported. See Bookmarks Data View on page 57.
	Click the *Cookies* button to view the web cookies that were extracted or imported. See Cookies Data View on page 57.
	Click the Searches button to view the web searches that were made on the device. See The Cookies data view shows any cookies that have been saved in the data of certain supported devices. This data view is only activated if the device is web enabled. The cookies data view provides information such as those listed in the following table. on page 57.
	Click the URL's button to view the URL's that were visited using the device. See URL's Data View on page 57.
	Click the *Memos* button to view the memos that were extracted or imported. See Memos Data View on page 58.
	Click the *SMS Messages* button to view texts that were extracted or imported. See SMS Messages Data View on page 58.
	Click the *MMS Messages* button to view multimedia texts that were extracted or imported. See MMS Messages Data View on page 59.
	Click the *Email* button to view email that were extracted or imported. See Email View on page 59.
	Click the PIN Messages button to view messages that were pinned using the device. See PIN Messages Data View on page 59.

Data Views Navigation Ribbon (Continued)

	Click the Auto Text button to view the auto text corrections that were made on the device. See Auto Text Data View on page 59.
	Click the Locations button to see the locations that were saved on the device. See Locations Data View on page 59.
	Click the *Carved Data* button to view files that were carved. See Carving Data on page 41. See Carved Data View on page 59.
	Click the *App Data* button to view data that was collected by the device's applications. See App Data Data View on page 60.
	Click the *Time Analysis* button to view communication data for a selected date range in a graphic representation. See Time Analysis on page 67.
	Click the *Social Analysis* button to view communication data for a selected contact in a graphical representation. See Social Analysis on page 71.

Number of Files

The number of files included in each data view is indicated in the upper right corner of the Data View button. This feature makes it much easier to locate the number of extracted data items.

Note: During a SIM extraction, the number of records are often duplicated because both the SIM and USIM areas are extracted. If the data resides in both locations, then the record is displayed twice, showing an extra record in the count.

Number of Files

Contacts Data View

The Contacts List data view displays the phone book information extracted from the device.

Call History Data View

The Call History data view displays the incoming, outgoing, and missed calls recorded in the device.

Note: With several Android devices, the Number of Times Contacted information on the Call History tab can be unreliable, and you should not use this information to conclusively say that a contact has been contacted as indicated in the Number of Times Contacted column.

Calendar Data View

The Calendar data view displays the calendar entries recorded in the device. Data recorded includes event, notes, time occurred, and time zone.

Media Data View

The media data view will display a list of photos, audio files, and videos found throughout known locations on certain supported devices. Files may be examined in Gallery, Hex, or Natural mode. Natural mode has an embedded media viewer that allows you to examine audio files and videos, as well as photos.

Finding Media Files in the File System

If you have a file system capability, you can right-click on media files on the *Media* tab and select **Find File in File System** to view the file's location on the *File System* tab.

Exporting Media Files

If you have a file system capability, you can now select files in both the media and the carved view to export the file to a desired location in the files' native form. This allows you to do the following:

- Report on carved files using the attach file function in reports
- Save native files to an evidence folder for later analysis
- View files that are not currently viewable in the natural view

You can select a single file or multiple files by clicking the checkbox in the select column, right-clicking in the file list view, and selecting to **Export Item(s)** to a desired location.

File System Data View

The File System data view displays a recreation of the device's file system based on logical file system records extracted from the device. In this pane, the examiner is able to drill-down into the file system and view the extracted data using either the Hex view, or the Natural view.

Note: Selecting many large files to view in the File System View may generate a Disk Full error. To clear the cache, restart MPE+.

While viewing an item in Hex view, you can click the “Find...” button (located at the top of the Hex view tab) to search for either text or hex strings within that item.

Additionally, you can click the “**Find...**” button (or CTRL+F) while viewing an item in Hex view to search for either text or hex strings within that item.

Note: The “Find” function does support the use of an asterisk (*) character as a wildcard to enhance search functionality.

Bookmarks Data View

The Bookmarks data view shows any bookmarks that have been saved in the data of certain supported devices. This data view is only activated if the device extracted from is web enabled.

Cookies Data View

The Cookies data view shows any cookies that have been saved in the data of certain supported devices. This data view is only activated if the device is web enabled. The cookies data view provides information such as those listed in the following table.

Potential Cookie Data

• Web Address	• Name
• Path	• Value
• Date Created	• Date Expires

Searches Data View

The Searches data view shows any searches that have been made on the device. This data view is only activated if the device is web enabled. The Searches data view provides information such as:

- Title
- Short Cut

URL’s Data View

The URL’s data view shows any URL’s that have been visited on the device. This data view is only activated if the device is web enabled. The URL’s data view provides the web address.

Memos Data View

The Memos data view provides both titles and content of extracted memos.

SMS Messages Data View

The SMS messages data view provides information such as those listed in the following table.

Note: Messages with an asterisk next to them may have been corrupted when imported into MPE+. The text of the message may not appear as it did on the phone.

Potential Device Message Data

• Message Type	• Date Received
• Phone Number of Originating Message	• Phone Number of Recipient
• Subject	• Message Text
• Priority	

View Conversation

View Conversation allows you to review a conversation in the context that it was delivered. When SMS items are listed in the SMS Items tab, they are not in any order. Selecting View Conversation will display the selected message and the messages associated with it.

To view a conversation

1. In Data Views, click the SMS Messaging icon.
2. Highlight the row you want to expand.
3. Right-click the row and click **View Conversation**.

The complete conversation displays in the Data Views window. Multiple conversations display with tabs that allow you to move between conversations during the review.

Reporting Information from the Conversation View

You can now report the information from the conversation view. While in the SMS view, you can select a message, and add it to a report.

To add conversation view information to a report

1. Right-click, and select a conversation view or select the conversation in the conversation pane.
2. While the conversation bubbles are visible, right-click the yellow oval at the top of the message and select *Add to report*.

You can elect to remove the report by following the same procedure: selecting the conversation that has been added to the report in the SMS view, right-clicking on the yellow oval, and selecting Remove from report.

Note: NOTE: If the option, Remove from report, is not available, the report has not been added. Also, in order to view the report in Print Preview, another capability (such as SMS, Contacts, Call Logs) must be selected.

MMS Messages Data View

The MMS messages data view provides information about multimedia text files.

Note: If you have a device that contains media text messages, but the MMS option is not available, it is because that device does not allow export of those files. Using the carving feature you can locate the embedded files in the MMS messages.

Email View

The Email data view displays emails that are sent or received on the device; this includes email attachments for some supported devices. Built into MPE+ is an attachment viewer.

PIN Messages Data View

The PIN Messages data view displays messages that were Pinned using the device. This view displays information such as:

- Type
- Date
- To
- Subject
- Body

Auto Text Data View

The Auto Text data view displays text that was corrected by the device. This view displays information such as:

- Text Typed
- Corrected Text

Locations Data View

The Locations data view displays the locations that were saved to the device gps.

Carved Data View

Files recovered or extracted during the carving process can be reviewed using the Carved Data data view.

Finding Carved Files in the File System

You can right-click on media files on the *Media* tab and select **Find File in File System** to view the file's location on the *File System* tab.

Exporting Carved Files

You can now select files in both the media and the carved view to export the file to a desired location in the files' native form. This allows you to do the following:

- Report on carved files using the attach file function in reports
- Save native files to an evidence folder for later analysis
- View files that are not currently viewable in the natural view

You can select a single file or multiple files by clicking the checkbox in the select column, right-clicking in the file list view, and selecting to **Export Item(s)** to a desired location.

App Data Data View

The *App Data* Data View displays data that is collected by applications on the device.This data view is only activated if the device is Android or iOS. Data will display from the following applications:

- QQ
- WeChat

Using pythonScripter™

pythonScripter™ allows you to execute Python scripts on directories and files in MPE+ to increase searching, carving, and parsing abilities. With pythonScripter, you can view the results instantly and then publish the results to MPE+. The published results can then be included in reports and saved to an AD1 file.

The MPE+ pythonScripter utilizes Python 3.3 and its standard shipping modules.

Note: To extend these modules for Python, place these modules into the `Python33 Library` folder located in the `Local AppData` folder where MPE+ (mobilephoneexaminer.exe) resides.

To use pythonScripter

1. Right-click a directory or file and click **Run pythonScripter** ().

   The *pythonScripter* dialog appears.
2. From this dialog, you can select preset scripts or browse to your own personal Python scripts. You can also create, modify, and edit scripts within the *pythonScripter* dialog. See pythonScripter Dialog on page 61.
3. Once the script is entered, click **Execute** to run the script.
4. Click **Publish** to publish the results of the script to a *Python Publish Results* tab in *Data Views*.

   Note: For help with scripting with Python or other Python-related questions, click the Python Help link in the upper, right-hand corner of the Python Scripter dialog.

pythonScripter Dialog

Executing a Script

When you execute a script, the output can display in two areas depending on the code within the script. Some scripts output files, while other scripts output "text". If files are outputted using a script, the script should contain a path to where the data will reside (for example: `tmpDir = "C:/Temp:Test"`). If data is assigned to this temporary area, you can use the **File** tab in the *pythonScripter* dialog. If the script parses a file for text and the output is going to use the print statement, the text displays in the **Console** tab.

Note: If you use the same output path on subsequent extractions and this path is located in the Output Path box, MPE+ displays a message to notify you that data exists and will be deleted from the folder if you continue. To keep the data from a previous script, copy the data to a safe location. You can also change the output path of the script so that it does not interfere with the previous output.

Files Tab

The **Files** tab allows you to browse to the location where the script output the data.

The relative file path for files examined in both the pythonScripter and SQLBuilder are displayed in the interface and subsequent report information.

To browse to the data

1. Click **Browse** next to the Output Path text box.
2. Locate the output path specified in the script and select the folder.
3. The folder now displays in the treeview of the **Files** tab.
4. From the treeview, you can click the folder to see all of the files extracted using the script in the filesview.
5. From the filesview, you can right-click any file and execute another instance of the pythonScripter or the SQL Builder. This could be useful if you ran a file finder for database files and now run the SQL Builder.

Console Tab

The **Console** tab allows you to view the output for scripts that output text returns. If the script delimits the output, you can specify the delimiter after clicking the **Delimited** button.Click inside the box and place your delimiter into the box and click **Delimited** again. The data displays in grid format.

Publishing Results

To publish results after execution, click Publish. The data from the console and the file tab will then be visible in the MPE+ User Interface under the Data View tab and toolbar item Python. Each published result will have its own tab. If you wish to discard a published result you simply have to click the x in the tab. Once the results are published the data can be reported and saved to an AD1 file.

Preset Scripts for pythonScripter

There are several preset Python scripts that can be found and accessed in the **Preset Scripts** selection box. The type of data you are examining determines what scripts appear in the selection box. Scripts for directories will populate if you select a directory and scripts for files will display if you select a file. You can also develop your own Python scripts or use third-party Python scripts that conform to Python 3.3 standards.

To configure the *Preset Script* selection box to display these scripts, copy them to:

C:\Users\<UserName>\Documents\AccessData\Sample Python Scripts

When the scripts are in the folder, they will display in the Preset Script selection box in MPE+.

Note: To display other scripts in the *Preset Script* box, copy them to the “Sample Python Scripts” folder. You can then access those scripts without using the *Browse* menu.

Pre-Loaded Python Scripts

There are two types of pre-loaded Python scripts available to use in MPE+, directory scripts and file scripts.

Directory Scripts

Directory Scripts	Description
BBM_Log_Parser_Directory.py	This script allows you to parse Blackberry Messenger csv files stored on the SD card if logging is enabled. The parsed data will be extracted and converted for easy reporting.
EXIFParser_Directory.py	This script allows you to parse a folder for all the EXIF data from an image file. The parsed data will be extracted and converted for easy reporting.
GPSEXIFParser_Directory.py	This script allows you to parse a folder for all the GPS data from an image file. The parsed data will be extracted and converted for easy reporting.
HashFiles_Directory.py	This script allows you to HASH all the files in a folder and display both the MD5 and SHA256 hash. The parsed data will be extracted and converted for easy reporting.
JPG_Carver_From_Directory.py	This script allows you to carve JPG files using the JPG header from all files in a directory. This will allow you to pull JPG files from un-allocated files under one directory. This script runs much faster than the build in carver. The parsed data will be extracted and converted for easy reporting.
MIMEFinder_Directory.py	This script allows you to locate many file types using the files header. Once located the file is then given an appropriate extension which can then be reviewed in MPE+. The parsed data will be extracted and converted for easy reporting.
GPSTrack_GPX_Directory.py	This script allows you to parse all the track-points from Garmin/Nuvi and Mio devices. The script will convert all the GPX files located in the GPX folder and the GPX/History folder. The parsed data will be extracted and converted for easy reporting.
FileFinderExtension_Directory.py	This script allows you to enter any file extension(s) to search for within a directory. This can be used to quickly locate database files, user files and more and perform additional analysis.

File Scripts

File Scripts	Description
Android_Cell_Wifi_cache_Parser.py	This script allows you to parse the wifi.cache and the cell.cache files located at com.android.location on an Android device. This will parse the location data of both files and display it. The parsed data will be extracted and converted for easy reporting.
BBM_Log_Parser.py	This script allows you to parse Blackberry Messenger csv files stored on the SD card if logging is enabled. The parsed data will be extracted and converted for easy reporting
BLOB_File_Extractor.py	This script allows you to specify a table and a row containing BLOB data. Once specified and executed the BLOB data is extracted and converted to a readable format for easy reporting.

File Scripts

File Scripts	Description
JPG_Carver_From_File.py	This script allows you to carve JPG files using the JPG header from any file. This will allow you to pull JPG files from un-allocated files. This script runs much faster than the build in carver. The parsed data will be extracted and converted for easy reporting.
XML_Parser.py	This script converts the XML data into a readable format that can be extracted for easy reporting.
GPSTrack_GPX.py	This script allows you to parse all the track-points from Garmin/Nuvi and Mio devices. The script will convert the GPX files located in the GPX folder and the GPX/History folder. The parsed data will be extracted and converted for easy reporting.
GPSWaypoint_GPX.py	This script allows you to parse all the way-points from Garmin/Nuvi and Mio devices. The script will convert the GPX files located in the GPX folder and the GPX/History folder. The parsed data will be extracted and converted for easy reporting.

Reviewing Databases

There are two ways to gather database information in *Data Views*, SQLite Explorer and SQL Builder.

Using SQLite Explorer

SQLite Explorer allows you to quickly expand a SQLite database and view that database's columns and rows in *Data Views*.

To use SQLite Explorer

1. Right-click the database file in the filesystem view and click **SQLite Explorer**.
   The database is expanded and displayed as a table grid in a tab in Data Views. The name of the tab is the name of the database file that you selected.
2. Click the tables or rows from the left column to isolate them in the *Natural* pane.

> **Note:** If there is no left column displayed, hover the mouse over the left border of the Natural pane and expand the pane by clicking and dragging the border to the right.

Using SQL Builder

SQL Builder allows you to extract data from any SQLite from within MPE+. You can now extract application data that was not attainable in a common format or without using a third-party tool. Multiple table selection, foreign keys and data type assignment are all supported within SQL Builder. Once your SQL script is executed you can publish the extracted data to MPE+. The published data can be saved to an AD1 file and the data can be included into any MPE+ report.

The relative file path for files examined in the SQLBuilder are displayed in the interface and subsequent report information.

To use SQL Builder

1. Right-click the database file in the filesystem view and click **SQL Builder**.
   The SQL Builder dialog appears. Each table within the SQL Database is located in the first column.
2. Select a table
   The columns contained within the table appear in the second column. The columns contain the user data. Using the SQL Builder in conjunction with the SQL Browser allows you to see the data within the database using the SQL Browser and then extract the data using the SQL Builder.
3. Click the double-right arrow button () to move the column to the *Selected Columns* pane.
   The selected column name appears in the Selected Columns field.

4. Specify the type of data in the column. The types of data available are:
   - String (used for numbers, text)
   - UNIX Date (used for iOS and Android devices)
   - Milliseconds (used for Android Devices)
   - MicroSeconds (used for Android Devices)
   - MAC Date (used for iOS Devices)
   - Duration (used to convert seconds to minutes)
   - Foreign Key (used to show the relations between two different tables to “tie” the data to each table and show data from two relational tables)
5. Repeat steps 2-4 as needed to add the database information for your script.
6. Click **Execute**.
   The results appear in the *Results* tab at the bottom of the SQL Builder.

   Note: If any of the data displays incorrectly (for example, UNIX data should have a MAC date), you can change the type and click **Execute** again. You can also remove a previously Selected Column by clicking the << button and clicking **Execute** again.

7. Click **Publish** to display the results in *Data Views*.
   These results appear in a tab titled *SQLite Query Results* and a child tab displays the name of the database parsed. Closing the tab in *Data Views* clears your query results. To view the query results again, execute SQL Builder and run the same query or a saved query.

Saving Queries in SQL Builder

You can save any script files you create for future use on the same database type.

To save a script

1. Enter a name in the Query Name field and click **Save**.
   The saved scripts are saved to:
   C:\Users\<UserName>\Documents\AccessData\Sqlite Scripts.

   Note: These scripts are encrypted and can only be used within MPE+. Once stored in the preset area, select the box under *Saved Queries* and click **Open**.

Time Analysis

The Time Analysis data view provides a graphical interface to enhance understanding and analysis of email, SMS, MMS, and call history data on a phone. You view data based on file and email dates and can filter that data by contact.

Time analysis can only display data that has an associated date. If a file or an email does not contain a valid Created, Modified, Last Accessed, Sent or Received date, it is not displayed. For example, carved files do not have an associated date so they are not displayed in Visualization.

Opening Time Analysis

To open the time analysis viewer

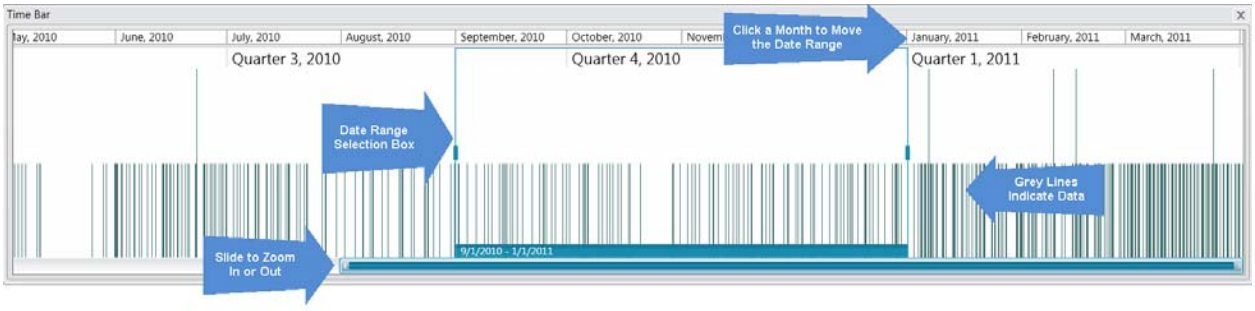
1. Bring phone data into MPE+ via import, or extraction.
2. Click on the **Data Views** tab.
3. Click the **Time Analysis** tab.

Setting the Date Range

The information that is displayed in Time Bar panel is organized using a time line from the oldest date on the left to the most current date on the right.

The time line is configured based on the dates of the data that you specified. For example, if the data that you specified had creation dates that ranged from 8/15/2003 to 9/11/2003, it will build a time line with those dates as the start and end.

Time Bar Panel



The vertical gray bars represent where the data files are on the time line. You must specify a date range for the base time line that you want to view. Only the data that exists in the base time line will be displayed in the charts and list.

When you first open Time Analysis, a limited default base time line is specified. The default base time line starts with the oldest data that is in the set. The base time line is designated by a blue box called the date range selection box.

For example, if you are viewing files, the default base time line is the first month starting with the creation date of the oldest file. The time line is displayed in weeks, with vertical gray bars representing the data.

You adjust the range and the location of the date range by adjusting the date range selection box. The information in the bar and pie charts change when you adjust the date range selection box.

To adjust the date range

1. You can change the date range of the data set by adjusting the blue selection box.
2. You can do one of the following options:
   - Select a time period that is on the top of the time line, for example, a month, or a quarter.
   - Drag the sliders of the blue date range selection box to make it bigger or smaller.
   - Drag the selection box to a different position.
   - Use the mouse scroll wheel to move the selection box left or right.

Zooming In and Out in the Time Line

You can zoom in and out on the time line in the Time Bar panel to view a smaller or larger time line.

To zoom in or out on the time line

- From the Time Analysis data view, in the Time Bar panel do one of the following:
  - Slide the slider bar at the bottom to the right to zoom in.
  - Slide the slider bar at the bottom to the left to zoom out.
  - Use the mouse wheel to zoom in or out.

Filtering by Contact

You can filter the data in the time line by contacts in the phone. When you select a contact in the Contacts panel, all other contacts are filtered out of the time line.

To filter by contact

- In the *Contacts* panel, select a contact from the list.

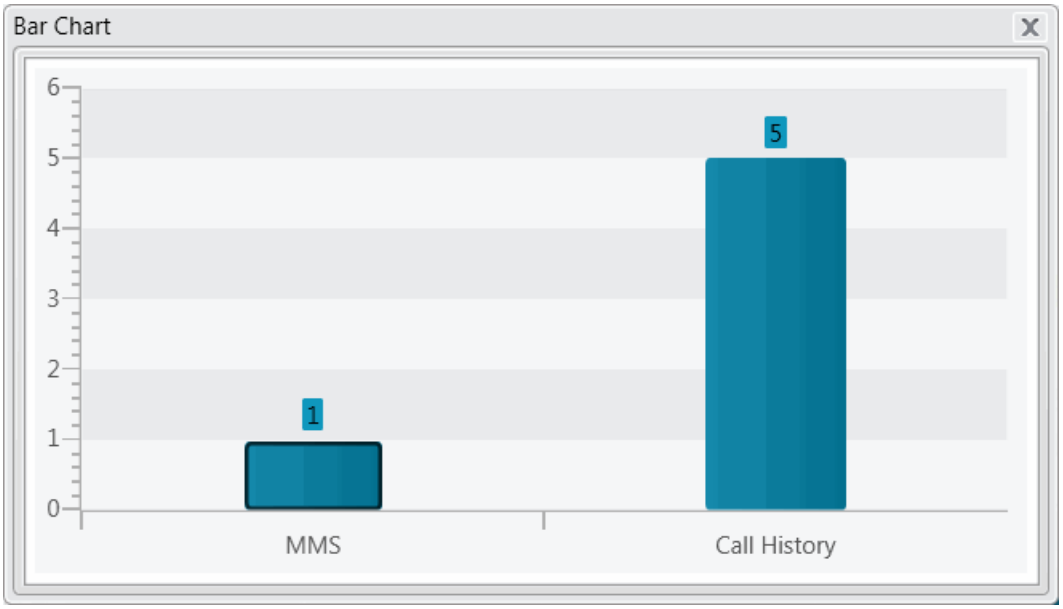
To remove filters

- In the *Contacts* panel, click the **Deselect All** button.

Visualizing Data Views by Bar Chart

The bar chart lets you view the data for the selected date range in a bar chart. You can select a bar in the chart to view the data files for the selected data view. The files appear in the Communication Data panel when you click the bar.

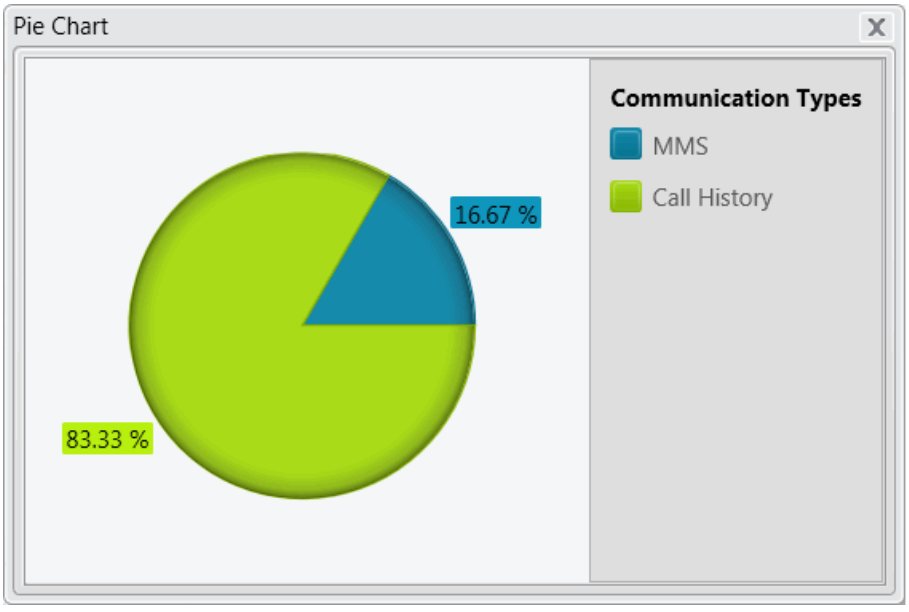
Bar Chart Panel



Visualizing Data Views by Pie Chart

The pie chart displays the percentages of each data view in the selected date range. You can select a portion of the pie chart or click on an item in the legend to view the data files for the data view. The files appear in the Communication Data panel when you click the chart.

Pie Chart Panel



Viewing Data Files in the Communication Data Panel

The Communication Data panel displays details about the files in the date range. The information that is displayed in the Communication Data panel is generated based on the data view that you selected in the bar chart, pie chart, or pie chart legend.

Within the Communication Data panel you can sort, group, and sub-group, items according to columns. To sort, drag and drop the desired column heading onto the blue bar. Any column heading that includes a filter icon can be used to sort the file list data set.

To sort by column

- In the *Communication Data* panel, click the column header to sort by the column.

To group columns

- In the *Communication Data* panel, click and drag the column header and drop it in the space above the columns.

Taking a Snapshot

You can take a snapshot of the Time Analysis data view and save it as a PNG file in a designated location for future reference.

To take a snapshot

1. In the *Contacts* panel, click the **Take Snapshot** button.
2. Browse the location where you want to save the file.
3. Click **Save**.

Social Analysis

The Social Analysis data view displays the SMS, MMS, email, and call history data for selected contacts in a graphical representation. This allows you to see which contacts had a greater volume of communication data.

Opening Social Analysis

To open the social analysis viewer

1. Bring phone data into MPE+ via import, or extraction.
2. Click on the **Data Views** tab.
3. Click the **Social Analysis** tab.

Selecting a Contact

To view the communication data of a contact, you must first select the contact in the Contacts panel and the data will be reflected in the bar chart.

To select a contact

- From the Social Analysis tab, in the Contacts panel, do one of the following:
  - Click the **Select All** button to view the communication data for all the contacts.
  - Check contacts individually to view data for specific contacts.

Viewing Contact Data in the Communication Data Panel

The Communication Data panel displays details about the selected contact. The information that is displayed in the Communication Data panel is generated based on the contact that you select in the bar chart of the Social Analysis data view.

Within the Communication Data panel you can sort, group, and sub-group, items according to columns. To sort, drag and drop the desired column heading onto the blue bar. Any column heading that includes a filter icon can be used to sort the file list data set.

To sort by column

- In the *Communication Data* panel, click the column header to sort by the column.

To group columns

- In the *Communication Data* panel, click and drag the column header and drop it in the space above the columns.

Taking a Snapshot

You can take a snapshot of the Time Analysis data view and save it as a PNG file in a designated location for future reference.

To take a snapshot

1. In the *Contacts* panel, click the **Take Snapshot** button.
2. Browse the location where you want to save the file.
3. Click **Save**.

Viewing the Social Analyzer Chart

The social analysis chart provides a contextual view of an individual's social network, based on the social data volume contained in the data set.

To view the social analyzer chart

1. Bring phone data into MPE+ via import, or extraction.
2. Click on the **Data Views** tab.
3. Click the **Social Analysis** tab.
4. Do one of the following:
   - Click the **Select All** button to view the communication data for all the contacts.
   - Check contacts individually to view data for specific contacts.
5. Click the **Social Analyzer Chart** button to view the chart.

Selecting Data for Export

You can check data files in the data views that can then be included in a report for export.

To select data for export

1. Bring phone data into MPE+ by import or extraction.
2. Click on a Data View.
   See About Data Views on page 53.
3. In a list of data files, check the files that you want to include in the report.
4. Then, when running a report, select to include checked files.

Chapter 5

Exporting Data

After you have collected and reviewed the phone data, you can export the phone data in multiple ways.

- Exporting phone data to an AD1 file that can be read by FTK or MPE+: See Exporting To an AD1 Image on page 74.
- Exporting phone data to a report: See Creating Reports on page 76.

Exporting To an AD1 Image

All extracted data is exported to an MPE+ AD1 Image. If you want to include only certain types of data, select only those types to extract from the device.

When you have completed your FULL examination of the device, then you can create an AD1 of the extracted data.

The resulting image can be read by MPE+, Imager, or any FTK-based product.

To export the currently extracted mobile device data to an AD1 image

1. Click the **Export to AD1** button on the *Main* ribbon.
2. When prompted, enter a filename and select a destination folder for the image that will be created.
3. Click **Save**.
4. In the confirmation message box, click **OK**.

Note: In addition to the AD1 file, a text file is saved in the same location that you designated that contains a date and time stamp for the export. This information is for your records.

Adding an MPE+ AD1 Image to a Case in FTK

An MPE+ AD1 image is added as evidence in FTK the same way any other AD1 image is added. Simply select **Acquired Image(s)** as the Evidence Type. For more information, see the AccessData FTK User Guide.

Exporting Data from the File System

You can export files or folders directly from the File System Data View to the location of your choice.

Exporting a Folder

You can export a folder from the File System data view.

To export a folder

1. Bring data into MPE+ by extraction or import.
   See Collecting Data on page 20.
2. Click on the **Data Views** ribbon and click the **Files** button.
3. Expand the folders in the Folder Tree pane and right-click the folder to export.
4. Click **Export Folder**.
5. Click **OK**.

Exporting a File

You can export a specific file from the File System data view.

To export a file

1. Bring data into MPE+ by extraction or import.
   See Collecting Data on page 20.
1. Click on the **Data Views** ribbon and click the **Files** button.
2. Expand the folders in the Folder Tree pane and select the folder that contains the file you want to export.
3. In the *Files in Selected Folder* pane, right-click the file you want to export and click **Export File**.
4. Click **OK**.

Creating Reports

You can create reports in the *Print Report* dialog to Preview or Export a report that contains the data type(s) you select. Reports only pull data that is stored in the cache, and thus does not include File System data. In addition, this option will be active only if cache data is available from device extraction or image import.

The data types that appear in the *Data to Report* dialog are dynamic to the phone data that has been extracted or imported.

This feature provides the following benefits:

- Easy review of the data by external persons not involved in the extraction, who may be interviewing subjects involved in the investigation.
- Previewing of data for court purposes where the full report has not been completed.
- Any other purpose that requires the immediate review of the extracted data.

If you plan to print the Phonebook data, it is important to generate a Preview or an Export first. Phonebooks often have a schema that allows for hundreds of entries and all the entries will print, including the blank ones.

The Preview and Export features allow you to see which pages actually have meaningful data of any data type before you print a hard copy.

The Attachments option allows you to attach any supporting files the your report, including PDF, JPG, BMP, PNG, and GIF. This allows you to add the visualization screen captures, parsed images, and additional report items saved to PDF to the completed report.

If you need to include all pages to maintain continuity for distribution, use the Export feature and distribute the PDF.

Note: Video and Audio files will not appear in a report.

Previewing a Report

The Print Report Preview option allows you to review, save, print, export, and/or email your report.

To preview a report

1. Click **Create Report** on the *Main* ribbon.
2. In the *Print Report* dialog box, select one of the following:
   - **Include All Data**: Select to include all the phone data and select from all the available data types.
   - **Include Only Selected Data**: Select to include only the data columns that were selected during review. This will limit the data types to only those available for the selected columns.
3. Select the *Data to Report* to be included in the export.
4. Select the format(s) in the *Export To* pane.

Note: The data that you can select for the Quick Print report is dynamic to the data that was extracted or imported. Only the data types that were extracted or imported will appear in the Quick Print Report dialog.

5. (Optional) Click **Investigator Info** to enter information about the investigator. See Entering Investigator Information (page 78) for more information on investigator information.

6. Click **Preview**.
   From the Preview, you can review, save, print, and export the report using the Preview Toolbar.

Exporting a Report

There are two ways to export a report, in the Print Report dialog and in the Preview window.

To export a report in the Print Report dialog

1. Click **Create Report** on the *Main* ribbon.
2. In the *Print Report* dialog box, select one of the following:
   - **Include All Data**: Select to include all the phone data and select from all the available data types.
   - **Include Only Selected Data**: Select to include only the data columns that were selected during review. This will limit the data types to only those available for the selected columns.
3. Select the Data to Report to be included in the export.
4. Select the format(s) in the *Export To* pane.
5. (Optional) Click **Investigator Info** to enter information about the investigator. See Entering Investigator Information (page 78) for more information on investigator information.
6. Click **Export**.
   The Quick Print Report file is generated and saved in the specified location.

To export a report in Preview window

1. Open the *Print Report* dialog and click **Preview**.
   See Previewing a Report on page 76.
2. Click the *Export to* icon drop-down menu  .
3. Click the format to which you are exporting.
4. Each format displays a dialog specific to that file format. Enter the export options and click **OK**.
5. Enter a file name and navigate to where you will save the file.
6. Click **Save**.

Attaching Files to a Report

You can attach supporting files to any report.

To attach files to a report

1. In the *Print Report* dialog, click **Attachments**.
2. In the *Select Attachments* dialog, click **Browse**.
3. Select the files to attach to the report.

   Note: You can use standard Windows select commands (for example, Ctrl+click and Shift+click) to select multiple files.

4. Click **Open**.
5. You can remove any attached files by clicking **Remove** next to the attachment to remove.
6. Add comments to each attachment and click **Done**.

Reporting Information from the Conversation View

You can now report the information from the conversation view. While in the SMS view, you can select a message, and add it to a report.

See Reporting Information from the Conversation View on page 78.

Printing a Report

You can print from either the *Print Report* dialog or the *Preview* window.

To print a report from the Preview window

1. Open the *Print Report Preview* window.
   See Previewing a Report on page 76.
2. Click either the *Print* or *Quick Print* icon.
   - *Print* opens the *Print* dialog where you can make changes to your printer, number of copies to print, page ranges, and so forth. Click **Print** to print the report.
   - *Quick Print* sends the report directly to the default printer without opening the Print dialog.

Entering Investigator Information

You can include information about the investigator who is collecting the data to appear on the report. Besides the default information provided in the dialog, you can also enter custom information about the investigator.

To enter investigator information

1. Do one of the following:
   - Click **Create Report** on the *Main* ribbon and click **Investigator Info**.
   - Click the **Manage** button and click **Investigator Information...**.
2. Enter the investigator information. There are no required fields, therefore, you can enter only the information you want.
3. Click **Select Logo** to change the image or logo that appears on the report.
4. You can also create additional values by entering items in the *Additional Information* group box. Click **Add Item** to add an item to the Investigator Information.
   - For example, if you want to include an email address for the investigator, enter “Email Address” in the *Name* field and the email address in the *Value* field.
5. Click **Save**.
6. Navigate back to the *Print Report* dialog to complete the report.

Chapter 6

Managing Settings

MPE+ Settings

MPE+ Settings can be altered from the Manage menu. The following things can be set:

- See Setting the License Host and Port on page 79.
- See Setting the Temporary Folder Path on page 79.
- See Setting Data Carving Max Concurrent Carvers on page 80.
- See Setting the MPE+ Theme on page 80.

Setting the License Host and Port

You can set the License Host (this can be either localhost, or the computer name or IP Address of a remote network computer), and the License Port (the port number being used for transmitting activation information) from the Settings options. The default port is 6921, but if this is in use, you can change it.

To set the License Host and Port

1. Click the **Manage**  button.
2. Click **Settings**.
3. Enter the **License Host** and **Port**.
4. Click **Save**.

Setting the Temporary Folder Path

You can set the location where your temporary data is stored. MPE+ uses a temporary folder while extracting data from a device and you can specify the location where you would like this data to reside. The location you select may need to contain large amounts of data, so it must be able to hold at least 100GB.

To select the location of temporary data storage

1. Click the **Manage**  button.
2. Click **Settings**.
3. Click the **Browse** button and select the location where you want temporary data stored.
4. Click **Save**.

Setting Data Carving Max Concurrent Carvers

You can set the maximum number of concurrent carvers that you want to run. By default, this is set to 20, which works for most machines. Only increase this number if you have a higher processing machine. Otherwise, increasing the number will cause your machine to run slowly.

To set data carving max concurrent carvers

1. Click the **Manage**  button.
2. Click **Settings**.
3. Set the number of carvers that you want to be able to run concurrently.
4. Click **Save**.

Setting the MPE+ Theme

You can customize the color theme of MPE+. You changes to the theme will be reflected in the application when you restart it.

To set the MPE+ Theme

1. Click the **Manage**  button.
2. Click **Settings**.
3. Expand the **Available Themes** drop-down and select the theme of your choice.

Setting Internet Connectivity for MPE+

You can manually enable and disable MPE+'s access to the internet.

To allow MPE+ to connect to the internet

1. Click the **Manage**  button.
2. Click **Settings**.
3. Select the check box to enable internet access or deselect to disable.

Managing Drivers

Importing Drivers Manually

You can import drivers from a file on your system in addition to having MPE+ automatically search for and install new drivers.

To import drivers from a folder

1. Click the **Manage**  button.
2. Select **Import Drivers**.
3. Browse to the file and click **OK**.

Managing Layouts

You can perform the following tasks with layouts:

- See Customizing Your Layout on page 82.
- See Saving Your Layout on page 83.
- See Loading a Saved Layout on page 83.
- See Resetting the Layout to the Default on page 83.

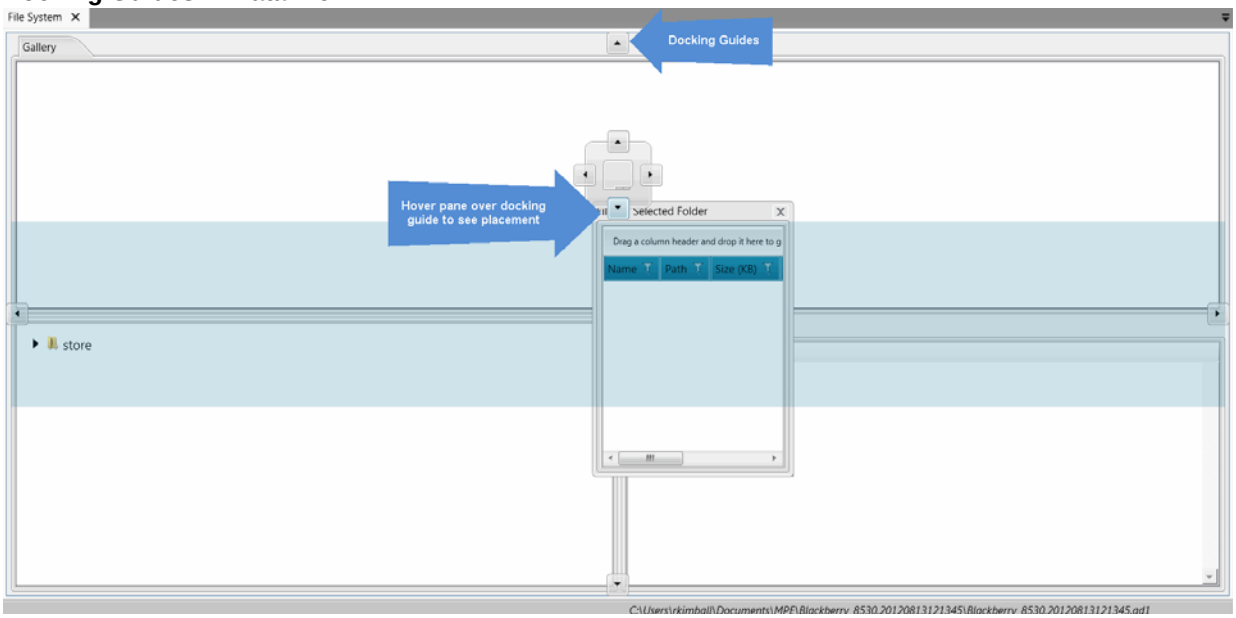
Customizing Your Layout

You can customize the layout of MPE+ by clicking and dragging the panels in the Data Views. You can then save your layout for continued use.

To customize your layout

1. Extract or import phone data.
2. Click on the **Data Views** tab.
3. Select the *Data View* that you want to view.
4. Click and drag the panels to the location that best works for your workflow. Use the docking guides if you want the panel to dock within the window, or you can let the panel float.

Docking Guides in Data View



Saving Your Layout

You can save your custom layout so that you don't have to customize the panels every time you use MPE+. You can only have one layout saved at a time.

To save your custom layout

1. Click the **Manage**  button.
2. Click **Save Layout**.
3. Click **OK**.

Loading a Saved Layout

If you have altered your layout to be different than the layout that you have saved, you can return to your saved layout by loading it.

To load a saved layout

1. Click the **Manage**  button.
2. Click **Load Saved Layout**.
   The saved layout loads in the Data View.

Resetting the Layout to the Default

If you have changed you layout and you want to return the default layout, you can reset the layout to the default.

To reset the layout to the default

1. Click the **Manage**  button.
2. Click **Reset Layout to Default**.
   The layout resets to the default in the Data View.

Opening the User Guide

You can open the MPE+ User Guide from the application if you need more information on the application.

To open the MPE+ User Guide

1. Click the **Manage**  button.
2. Click **User Guide**.
   The PDF of the guide opens.

Viewing Supported Devices

To view a list of supported devices

1. Click the **Manage**  button.
2. Click **Supported Devices**.

Chapter 7

Appendix A — Managing Security Devices and Licenses

This chapter expands on the licensing information needed to run AccessData products, including AccessData product licenses, Virtual CodeMeter activation, and Network License Server configurations.

AccessData Product Licenses

This section acquaints you with the managing AccessData product licenses. Here you will find details regarding the LicenseManager interface and how to manage licenses and update products using LicenseManager.

Installing and Managing Security Devices

Before you can manage licenses with LicenseManager, you must install the proper security device software and/or drivers. This section explains installing and using the Wibu CodeMeter Runtime software and USB CmStick, as well as the Keylok USB dongle drivers and dongle device.

Installing the Security Device

As discussed previously, AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device can be the older Keylok dongle, or the newer WIBU-SYSTEMS (Wibu) CodeMeter (CmStick). Both are USB devices, and both require specific software to be installed prior to connecting the devices and running your AccessData products. You will need:

- The WIBU-SYSTEMS CodeMeter Runtime software with a WIBU-SYSTEMS CodeMeter (CmStick), either the physical USB device, or the Virtual device. See
- The WIBU-SYSTEMS CodeMeter Runtime software, and the AccessData Dongle Drivers with a Keylok dongle

> **Note:** Without a license security device and its related software, you can run PRTK or DNA in Demo mode only.

The CmStick or dongle should be stored in a secure location when not in use.

You can install your AccessData product and the CodeMeter software from the shipping CD or from downloadable files available on the AccessData website at www.accessdata.com.

Click **Support > Downloads**, and browse to the product to download. Click the download link and save the file locally prior to running the installation files.

Installing the CodeMeter Runtime Software

When you purchase the full PRTK package, AccessData provides a USB CmStick with the product package. The green Keylok dongles are no longer provided, but can be purchased separately through your AccessData Sales Representative.

To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping CD, or from the setup file downloaded from the AccessData website.

Locating the Setup File

To install the CodeMeter Runtime software from the CD, you can browse to the setup file, or select it from the Autorun menu.

To download the CodeMeter Runtime software

1. Go to www.accessdata.com and do the following:
2. Click **Support** > **Downloads**.
3. Find one of the following, according to your system:
   - CodeMeter Runtime 4.20b (32 bit)
     MD5: 2e658fd67dff9da589430920624099b3
     (MD5 hash applies only to this version)
   - CodeMeter Runtime 4.20b (64 bit)
     MD5: b54031002a1ac18ada3cb91de7c2ee84
     (MD5 hash applies only to this version)
4. Click the **Download** link.
5. Save the file to your PC and run after the download is complete.

When the download is complete, double-click on the **downloaded file.**

To run the CodeMeter Runtime Setup

1. Double-click the **CodeMeterRuntime**[*32 or 64*]**_4.20b.exe**.
2. In the *Welcome* dialog, click **Next**.
3. Read and accept the License Agreement.
4. Click **Next**.
5. Enter User Information.
6. Specify whether this application should be available only when you log in, or for anyone who uses this computer.
7. Click **Next**.
8. Select the features you want to install.
9. Click **Disk Cost** to see how much space the installation of CodeMeter software takes, and drive space available. This helps you determine the destination drive.
10. Click **OK**.
11. Click **Next**.

12. When you are satisfied with the options you have selected, click **Next**.
13. Installation will run its course. When complete, you will see the “CodeMeter Runtime Kit v4.20b has been successfully installed” screen. Click **Finish** to exit the installation.

The CodeMeter Control Center

When the CodeMeter Runtime installation is complete, the CodeMeter Control Center pops up. This is a great time to connect the CmStick and verify that the device is recognized and is Enabled. Once verified, you can close the control center and run your AccessData product(s).

When the software is installed, but the CmStick is not connected, you will see a system tray icon that looks like this:

When the software is installed, and the CmStick is connected and recognized, you will see a system tray icon that looks like this:

For the most part there is nothing you need to do with this control center, and you need make no changes using this tool with very few exceptions. If you have problems with your CmStick, contact AccessData Support and an agent will walk you through any troubleshooting steps that may need to be performed.

Installing Keylok Dongle Drivers

To install the Keylok USB dongle drivers

1. Choose one of the following methods:
   - If installing from CD, insert the CD into the CD-ROM drive and click **Install the Dongle Drivers.**
     If auto-run is not enabled, select **Start** > **Run**. Browse to the CD-ROM drive and select `Autorun.exe`.
   - If installing from a file downloaded from the AccessData website, locate the `Dongle_driver_1.6.exe` setup file, and double-click it.
2. Click **Next.**
3. Select the type of dongle to install the drivers for.
4. Click **Next**.
5. If you have a USB dongle, verify that it is not connected.
6. Click **OK**.
   A message box appears telling you that the installation is progressing.
7. When you see the Dongle Driver Setup window that says, “Finished Dongle Installation,” click **Finish**.
8. Connect the USB dongle. Wait for the Windows Found New Hardware wizard, and follow the prompts.

Important: If the Windows Found New Hardware wizard appears, complete the wizard. Do not close without completing, or the dongle driver will not be installed.

Windows Found New Hardware Wizard

When you connect the dongle after installing the dongle drivers, you should wait for the Windows Found New Hardware Wizard to open. It is not uncommon for users to disregard this wizard, and then find that the dongle is not recognized and their AccessData software will not run.

To configure the dongle using the Found New Hardware Wizard

1. When prompted whether to connect to Windows Update to search for software, select, “No, not this time.”
2. Click **Next**.
3. When prompted whether to install the software automatically or to install from a list of specific locations, choose, “Install the software automatically (Recommended).”
4. Click **Next**.
5. Click **Finish** to close the wizard.

Once you have installed the dongle drivers and connected the dongle and verified that Windows recognizes it, you can use LicenseManager to manage product licenses.

Installing LicenseManager

LicenseManager lets you manage product and license subscriptions using a security device or device packet file.

To download the LicenseManager installer from the AccessData web site

1. Go to the AccessData download page at: http://www.accessdata.com/downloads.htm.
2. On the download page, click the **LicenseManager Download** link.
3. Save the installation file to your download directory or other temporary directory on your drive.

   3a. The current version information is as follows:
   - License Manager version 3.1.1 (`LicenseManager_3.1.1.exe`)
   - Release Date: March 25, 2010
   - MD5: 2e645ca8b0ca57aafbc156213be2147f (for this version only)

To install LicenseManager

1. Navigate to, and double-click the installation file.
2. Wait for the *Preparing to Install* processes to complete.
3. Click **Next** on the *Welcome* screen
4. Read and accept the License Agreement
5. Click **Next**.
6. Accept the default destination folder, or select a different one.
7. Click **Next**.
8. In the Ready to Install the Program dialog, click **Back** to review or change any of the installation settings. When you are ready to continue, click **Install**.
9. Wait while the installation completes.
10. If you want to launch LicenseManager after completing the installation, mark the **Launch AccessData LicenseManager** check box.
11. Select the **Launch AccessData LicenseManager** check box to run the program upon finishing the setup.
12. Click **Finish** to finalize the installation and close the wizard.

Starting LicenseManager

To launch LicenseManager

1. Launch LicenseManager in any of the following ways:
   - Execute `LicenseManager.exe` from `C:\Program Files\AccessData\Common Files\AccessData LicenseManager\`.
   - Click **Start > All Programs > AccessData > LicenseManager > LicenseManager.**
   - Click or double-click (depending on your Windows settings) the **LicenseManager** icon on your desktop  .
   - From some AccessData programs, you can run LicenseManager from the **Tools > Other Applications** menu. This option is not available in PRTK or DNA.

When starting, LicenseManager reads licensing and subscription information from the installed and connected WIBU-SYSTEMS CodeMeter Stick, or Keylok dongle.

If using a Keylok dongle, and LicenseManager either does not open or displays the message, "Device Not Found"

1. Make sure the correct dongle driver is installed on your computer.
2. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
3. Remove the dongle after the device has been uninstalled.
4. Reboot your computer.
5. After the reboot is complete, and all startup processes have finished running, connect the dongle.
6. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, "No, not this time."
7. Click **Next** to continue.
8. On the next options screen, choose, "Install the software automatically (Recommended)
9. Click **Next** to continue.
10. When the installation of the dongle device is complete, click Finish to close the wizard.
11. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, "Device Not Found"

1. Make sure the CodeMeter Runtime 4.20b software is installed. It is available at **www.accessdata.com/support**. Click Downloads and browse to the product. Click on the download link. You can **Run** the product from the Website, or **Save** the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray:  .
2. Make sure the CodeMeter Stick is connected to the USB port. When the CmStick is then connected, you will see the icon change to look like this:  .

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open LicenseManager without a CodeMeter Stick installed

1. Click **Tools** > **LicenseManager**.
   LicenseManager displays the message, "Device not Found".
2. Click **OK**, then browse for a security device packet file to open.

Note: Although you can run LicenseManager using a packet file, AccessData products will not run with a packet file alone. You must have the CmStick or dongle connected to the computer to run AccessData products that require a license.

Using LicenseManager

LicenseManager provides the tools necessary for managing AccessData product licenses on a WIBU-SYSTEMS CodeMeter Stick security device, a Keylok dongle, a Virtual Dongle, or in a security device packet file.

LicenseManager displays license information, allows you to add licenses to or remove existing licenses from a dongle or CmStick. LicenseManager, and can also be used to export a security device packet file. Packet files can be saved and reloaded into LicenseManager, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and in some cases download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

The LicenseManager Interface

The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab and the Licenses tab.

The Installed Components Tab

The Installed Components tab lists the AccessData programs installed on the machine. The following information is displayed on the Installed Components tab:

LicenseManager Installed Components Tab Features

Item	Description
Program	Lists all AccessData products installed on the host.
Installed Version	Displays the version of each AccessData product installed on the host.
Newest Version	Displays the latest version available of each AccessData product installed on the host. Click **Newest** to refresh this list.
Product Notes	Displays notes and information about the product selected in the program list.
AccessData Link	Links to the AccessData product page where you can learn more about AccessData products.

The following buttons provide additional functionality from the Installed Components tab:

LicenseManager Installed Components Buttons

Button	Function
Help	Opens the LicenseManager Help web page.
Install Newest	Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.
Newest	Updates the latest version information for your installed products.

LicenseManager Installed Components Buttons (Continued)

Button	Function
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.

The Licenses Tab

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick. The Licenses tab provides the following information:

LicenseManager Licenses Tab Features

Column	Description
Program	Shows the owned licenses for AccessData products.
Expiration Date	Shows the date on which your current license expires.
Status	Shows these status of that product's license: • **None**: the product license is not currently owned • **Days Left**: displays when less than 31 days remain on the license. • **Never**: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.
Name	Shows the name of additional parameters or information a product requires for its license.
Value	Shows the values of additional parameters or information a product contained in or required for its license.
Show Unlicensed	When checked, the License window displays all products, whether licensed or not.

The following license management actions can be performed using buttons found on the License tab:

License Management Options

Button	Function
Remove License	Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the AccessData License Server web page to confirm success.
Refresh Device	Connects to the AccessData License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server.
Reload from Device	Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle.
Release Device	Click to stop the program reading the dongle attached to your machine, much like Windows' Safely Remove Hardware feature. Click this button before removing a dongle. This option is disabled for the CodeMeter Stick.

License Management Options (Continued)

Button	Function
Open Packet File	Opens Windows Explorer, allowing you to navigate to a .PKT file containing your license information.
Save to File	Opens Windows Explorer, allowing you to save a .PKT file containing your license information. The default location is My Documents.
Finalize Removal	Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect.
View Registration Info	Displays an HTML page with your CodeMeter Stick number and other license information.
Add Existing License	Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the AccessData License Server.
Purchase License	Brings up the AccessData product page from which you can learn more about AccessData products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Opening and Saving Dongle Packet Files

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To save a security device packet file

1. Click the **Licenses** tab, then under License Packets, click **Save to File**.
2. Browse to the desired folder and accept the default name of the .PKT file; then click **Save**.

> **Note:** In general, the best place to save the .PKT files is in the AccessData LicenseManager folder. The default path is **C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.**

To open a security device packet file

1. Select the **Licenses** tab.
2. Under *License Packets*, click **Open Packet File**.
3. Browse for a dongle packet file to open. Select the file and click **Open**.

Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

Removing a License

To remove (un-associate or unbind) a product license

1. From the Licenses tab, mark the program license to remove.

   This action activates the Remove License button below the Program list box.
2. Click **Remove License** to connect your machine to the AccessData License Server through the internet.
3. When you are prompted to confirm the removal of the selected license(s) from the device, click **Yes** to continue, or click **No** to cancel.
4. Several screens appear indicating the connection and activity on the License Server, and when the license removal is complete, the following screen appears.
5. Click **OK** to close the message box.

   Another internet browser screen appears from LicenseManager with a message that says, “The removal of your license(s) from Security Device was successful!” You may close this box at any time.

Adding a License

To add a new or released license

1. From the Licenses tab, under Browser Options, click **Add Existing License.**

   The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click **Submit**.
2. An AccessData LicenseManager Web page will open, displaying the following message, “The AccessData product(s) that you selected has been bound to the record for Security Device *nnnnnnn* within the Security Device Database.

   “Please run LicenseManager’s “Refresh Device” feature in order to complete the process of binding these product license(s) to this Security Device.” You may close this window at any time.
3. Click **Yes** if LicenseManager prompts, “Were you able to associate a new product with this device?”
4. Click **Refresh Device** in the Licenses tab of LicenseManager. Click **Yes** when prompted.

The newly added license displays in the License Options list.

Adding and Removing Product Licenses Remotely

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

Adding a License Remotely

To remotely add (associate or bind) a product license

1. On the computer where the security device resides:
   1a. Run LicenseManager.
   1b. From the **Licenses** tab, click **Reload from Device** to read the dongle license information.
   1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the dongle packet file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   3a. Remove any attached security device.
   3b. Launch LicenseManager. You will see a notification, “No security device found”.
   3c. Click **OK**.
   3d. An “Open” dialog box will display. Highlight the .PKT file, and click **Open**.
   3e. Click on the **Licenses** tab.
   3f. Click **Add Existing License.**
   3g. Complete the process to add a product license on the website page.
   3h. Click **Yes** when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”
   3i. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, **[serial#].wibuCmRaU.**
   3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides:
5. On the computer where the dongle resides:
   5a. Run the update file by double-clicking it. (**[serial#].wibuCmRaU** is an executable file.)
   5b. After an update file downloads and installs, click **OK**.
   5c. Run LicenseManager.
   5d. From the Licenses tab, click **Reload from Device** to verify the product license has been added to the dongle.

Removing a License Remotely

To remotely remove (un-associate or unbind) a product license

1. On the computer where the dongle resides:
   1a. Run LicenseManager.
   1b. From the Licenses tab, click **Reload from Device** to read the dongle license information.
   1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   3a. Launch LicenseManager. You will see a notification, “No security device found”.
   3b. Click **OK**.
   3c. An “Open” dialog box will display. Highlight the **.**PKT file, and click **Open**.
   3d. Click on the **Licenses** tab.
   3e. Mark the box for the product license you want to un-associate; then click **Remove License.**
   3f. When prompted to confirm the removal of the selected license from the dongle, click **Yes**.
   3g. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.
   3h. Click **Yes** to save the update file to the local computer.
   3i. The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.
   3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides.
5. On the computer where the dongle resides:
   5a. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.
   5b. Run LicenseManager
   5c. On the Licenses tab, click **Reload from Device** in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.
   5d. Click **Save to File** to save the updated dongle packet file to the local machine.
6. Copy the file to a computer with an Internet connection.

Updating Products

You can use LicenseManager to check for product updates and download the latest product versions.

Checking for Product Updates

To check for product updates, on the Installed Components tab, click **Newest**. This refreshes the list to display what version you have installed, and the newest version available.

Downloading Product Updates

To install the newest version, mark the box next to the product to install, then click **Install Newest**.

Note: Some products, such as FTK 2.x, Enterprise, and others, are too large to download, and are not available. A notification displays if this is the case.

To download a product update

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click **Newest** to refresh the list showing the latest releases, then compare your installed version to the latest release.

   If the latest release is newer than your installed version, you may be able to install the latest release from our Website.
2. Ensure that the program you want to install is not running.
3. Mark the box next to the program you want to download; then click **Install Newest**.
4. When prompted, click **Yes** to download the latest install version of the product.

   4a. If installing the update on a remote computer, copy the product update file to another computer.
5. Install the product update. You may need to restart your computer after the update is installed.

Purchasing Product Licenses

Use LicenseManager to link to the AccessData Web site to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to sales@accessdata.com.

Note: Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking **Refresh Device**.

Sending a Dongle Packet File to Support

Send a security device packet file **only** when specifically directed to do so by AccessData support.

To create a dongle packet file

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click **Load from Device**.
4. Click **Refresh Device** if you need to get the latest info from AD's license server.
5. Click **Save to File**, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to:

   support@accessdata.com.

Virtual CodeMeter Activation Guide

Introduction

A Virtual CodeMeter (VCM) allows the user to run licensed AccessData products without a physical CodeMeter device. A VCM can be created using AccessData License Manager, but requires the user to enter a Confirmation Code during the creation process.

The latest revision of this guide can be found at:

http://accessdata.com/downloads/media/VCM_Activation_Guide.pdf

Preparation

- Contact your AccessData sales rep to order a VCM confirmation code.
- Install CodeMeter Runtime 4.10b or newer (available on the AccessData download page).
- Install the latest release of License Manager (available on the AccessData download page).
- The following steps are to be run on the system where you want to permanently attach the VCM.

> **Note:** Once created, the VCM cannot be moved to any other system.

- AD LAB WebUI and eDiscovery administrators, please also follow steps outlined under in Additional Instructions for AD LAB WebUI and eDiscovery (page 101) in order to enable VCM licensing on the AccessData License Service.

Setup for Online Systems

To setup a Virtual CodeMeter

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

> **Note:** When creating a VCM on Windows Server 2003 or 2008, please refer to the special set of steps written for those platforms. See Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions (page 100).

3. Select **Create A Local Virtual CMStick**
4. Click **OK.**
   The Confirmation Code Required dialog displays.
5. Enter your confirmation code.
6. Click **OK**, AccessData License Manager will automatically synchronize with the License Server over the Internet.
7. Click **OK** when the update completes. License Manager will then create the VCM on your system.
8. At this point, AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Setting up VCM for Offline Systems

You can setup a Virtual CodeMeter on a system that is not connected to the internet (offline). You must also have one machine that connects to the internet to perform certain steps. This section details what to do on which machine.

Perform these steps on the Online system

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

> **Note:** When creating a VCM on Windows Server 2003 or 2008 Enterprise Edition, please refer to the special set of steps written for those platforms. See Creating a Virtual CM-Stick with Server 2003/ 2008 Enterprise Editions (page 100).

3. Select **Create Empty Virtual CMStick (offline)**.
4. Click **OK.**
5. The resulting dialog prompts you to save the ***.wibucmrau** file. Enter a name and path for the file, then click **Save**.
6. Transfer the ***.wibucmrau** to the Online system.

Perform these steps on the Online system

7. Unplug any AccessData dongles you currently have connected.
8. Launch License Manager.
9. Select **Create Activation File (online)**.
10. Click **OK**.
    The Confirmation Code Required dialog appears.
11. Enter your confirmation code and click **OK**.
12. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the ***.wibucmrau** file. Click **OK** when the update completes.
13. Transfer ***.wibucmrau** back to the offline system.

Perform these steps on the Offline system

14. Unplug any AccessData dongles you currently have connected.
15. Launch License Manager.
16. Select **Create Activate Virtual CMStick (offline)**.
17. Click **OK**.
18. The resulting dialog prompts you to browse to the location of the newly updated *.wibucmrau file. Locate the file, then click **Open**. License Manager creates the VCM on your system.
19. At this point, AccessData License Manager should now display a serial number for the VCM on the “Licenses” tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions

This section contains special instructions for using a VCM with Windows Server 2003 or 2008 Enterprise Editions. Complete each section in order.

To Create an Empty CodeMeter License Container

1. On the Server 2003/2008 machine, unplug any CodeMeter devices.
2. Open the CodeMeter Control Center. Make sure the window on the License tab is, empty indicating that no licenses are currently loaded.
3. Select **File > Import License.**
4. Browse to the License Manager program files directory.
   - 32 bit systems: **C:\Program Files\AccessData\LicenseManager**
   - 64 bit systems: **C:\Program Files (x86)\ AccessData\LicenseManager**
5. Highlight the **TemplateDisc5010.wbb** file, then click **Import**.
6. Click the **Activate License** button.
7. When the *CmFAS Assistant* opens, click **Next**.
8. Select **Create license request**, and click **Next**.
9. Confirm the desired directory and filename to save **.WibuCmRaC**. (Example: **Test1.WibuCmRaC**)
10. Click **Commit**.
11. Click **Finish**.

To Copy to another machine

1. Copy the new **.WibuCmRaC** to another machine that is not running Windows Server 2003/2008 Enterprise.

   Note: The destination system must have an active internet connection.

2. Unplug any AccessData dongles you currently have connected.
3. Launch *License Manager*.
4. Select **Create Activation File (online)**.
5. Click **OK**.
6. In the Confirmation Code Required dialog enter your confirmation code and click **OK**.
7. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the ***.wibucmrau** file. Click **OK** when the update completes.

To Finish the activation on the Windows Server 2003/2008 Enterprise system

1. Copy the activated .WibuCmRaC file to the Server 2003/2008 machine.
2. On the Server 2003/2008 machine, unplug any CodeMeter devices.
3. Open the CodeMeter Control Center. Make sure the window on the License tab empty indicating that no licenses are currently loaded.
4. Select **File > Import License.**
5. Browse to the location where the activated **.WibuCmRaC** is stored. Click **Import**.
6. AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

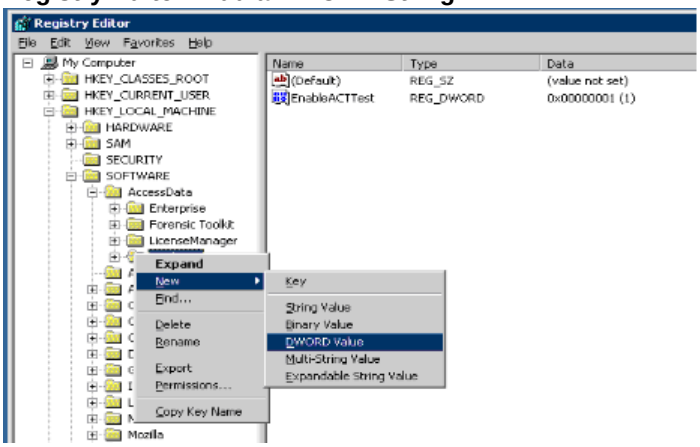
Additional Instructions for AD LAB WebUI and eDiscovery

This section provides additional information for enabling the Web User Interface to recognize a VCM.

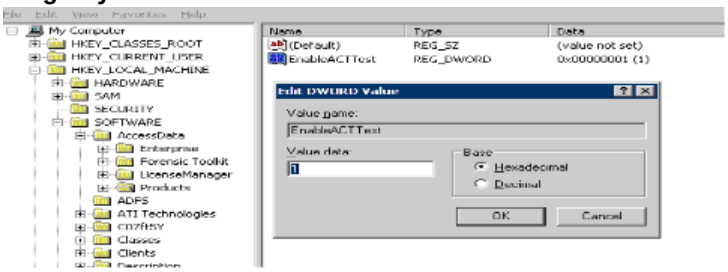
To enable AD Lab WebUI and eDiscovery to use VCM

1. Open Registry Editor.
2. Navigate to the following key:
   HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products
3. Add the following DWORD registry string to the key and set the value to 1:
   HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products | EnableACTTest

Registry Editor: Add a DWORD String



Registry Editor: Add a DWORD Value



The *AccessData License Service* will know to expect a VCM when *EnableACTTest* is set to "1."

Virtual CodeMeter FAQs

Q: How do I get a Virtual CodeMeter (VCM)?

A: Contact your AccessData product sales representative. They will provide you with a VCM confirmation code.

Q: How do VCMs work?

A: A VCM operates in almost exactly the same way as a hardware CodeMeter device, except that they exist as a file stored on the hard disk. During activation, the VCM file (named with a WBB extension) is tied to the hardware of the system using unique hardware identifiers. Those unique identifiers make VCMs non-portable. When AccessData License Manager is launched, it will automatically load the VCM and display its license

information. From there, you can refresh, remove, add existing licenses, etc just the same you would with a hardware security device.

Q: Are VCMs supported on virtual machines (VM)?

A: No. Due to the fact that virtual machines are portable and VCMs are not, VCMs are not supported on virtual machines. Currently it is recommended to use AccessData Network License Service (NLS) to license systems running as virtual machines. CLICK HERE for more information.

Q: Does the AccessData Network License Service (NLS) support VCMs?

A: The current release of NLS does not support using VCM as a network dongle. AccessData is considering this support for a future release.

Q: How can I “unplug” a VCM?

A: If you want to prevent License Manager from automatically loading the VCM you can "unplug" it by stopping the CodeMeter Runtime Service server and then moving (cut and paste) the WBB file to a new location (renaming the file does not suffice). By default the WBB file is located at:

32 bit systems:
C:\Program Files\CodeMeter\CmAct
64 bit systems:
C:\Program Files (x86)\CodeMeter\CmAct

Q: I have activated a VCM on my system, but now I need to activate it on a different system. What should I do?

A: Since a VCM is uniquely tied to the system on which it is activated, it cannot be moved to any other system. If you need to activate a VCM on a different system, you need to contact your AccessData Sales Representative.

Q: What if I need to reinstall Windows, format my drive, change my system's hardware, or back up my VCM in case of a disaster? Will the VCM still work?

A: The VCM can be backed up by simply copying the WBB file to a safe location. It can be restored by copying the WBB file to the CmAct folder. The VCM cannot be restored without a WBB file. If you do not have a back up of your WBB file, you will need to get a new confirmation code from your AccessData Sales Representative.

Q: My AccessData product does not seem to recognize the license stored on a VCM. What am I doing wrong?

A: VCMs are supported by the following versions of AccessData products:

- FTK 1.81.6 and newer
- FTK 3.1.0 and newer
- PRTK 6.5.0 and newer
- DNA 3.5.0 and newer
- RV 1.6.0 and newer
- eDiscovery 3.1.2 and newer
- AD Lab 3.1.2 and newer
- AD Enterprise 3.1.0 and newer
- MPE+ 4.0.0.1 and newer

Ensure that the version of the product you are running support VCMs. If the version you are running is listed as supported, verify that according to License Manager, the release date of the version you are running falls before the expiration date of the license.

Network License Server (NLS) Setup Guide

Introduction

This section discusses the installation steps and configuration notes needed to successfully setup an AccessData Network License Server (NLS).

Note: Click on this link to access the latest version of this guide:

Network License Server (NLS) Setup Guide.

Preparation Notes

- CodeMeter Runtime 3.30a or newer must be installed on all Client and Server systems
- AccessData License Manager must be used to prepare the network dongle. The system running License Manager must have internet access and have CodeMeter Runtime installed.
- The current release of NLS supports the following versions of Windows:
  - Windows XP 32/64 bit
  - Windows Server 2003 32/64 bit
  - Windows Vista 32/64 bit
  - Windows Server 2008 R1 32/64 bit
  - Windows 7 32/64 bit
  - Windows Server 2008 R2 64 bit
  - Windows 8 32/64 bit

Setup Overview

To setup NLS

1. Download the latest release of NLS located in the utilities section of the AccessData download page.
2. Extract contents of ZIP to a folder of your choice.
3. On the NLS server system, run through the NLS Installation MSI and accept all defaults.
4. Prepare network dongle:
   4a. Provide the serial number to AD Support and request to have the “Network Dongle Flag” applied.
   4b. Migrate any additional licenses to the network dongle
   4c. Refresh the network dongle device using AccessData License Manager.
5. Launch the AccessData product on the NLS client system.
6. Enter the NLS server configuration information:
   - IP address or hostname of NLS server system
   - Port 6921
7. Click, **OK**.

If you encounter any problems, please read the notes below for troubleshooting information.

Network Dongle Notes

- AccessData License Manager 2.2.6 or newer should be installed in order to manage licenses on the network dongle.
- Network dongles can hold up to 120 physical licenses. Each License has a capacity to hold thousands of sub licenses (i.e. Client count or worker count).
- Contact AccessData Technical Support to have your CodeMeter device flagged as a Network Dongle (required for NLS).

NLS Server System Notes

- Make sure the CodeMeter device is flagged as Network Dongle (i.e. License Manager will show the serial as "1181234N". To have this flag set on your CodeMeter device, please contact AccessData Technical Support).
- Server system must be configured to allow incoming and outgoing traffic on TCP port 6921.
- A web interface to view and revoke licenses all licenses is accessible at

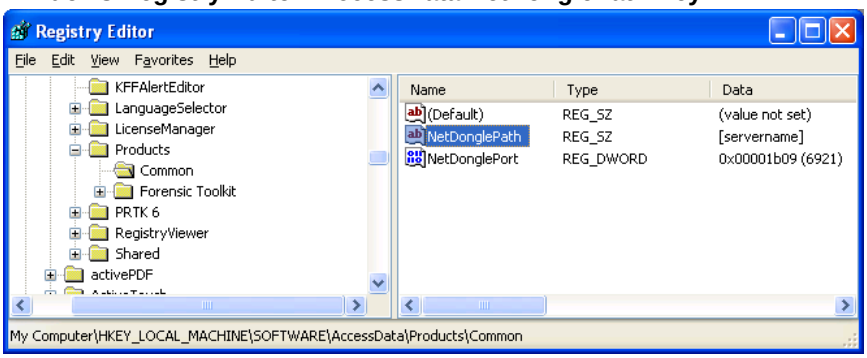
  `http://localhost:5555`

  This page can be reached only from a web browser running locally on the NLS server system.
- A Network Dongle cannot be used to run AccessData products locally unless the NLS server is running locally.
- Some versions of Windows may not find a local NLS server when the DNS hostname of the server is provided. In those cases, it is recommended to use a static IP address.
- When using the NLS across domains, users must have permissions to access resources on both domains (either by dual-domain membership or cross-domain trust).
- When running NLS on Windows Server 2008, Terminal Services must be installed and accepting connections. If Terminal Services is not configured it will not open the port and share out the licenses correctly.
- The name of the service according to Windows is “AccessData Network License Service.”

NLS Client System Notes

- When launched, any NLS client application that needs to lease a license from the NLS server will automatically check for the following values within the Windows Registry.

Windows Registry Editor: AccessData NetDonglePath Key



- **NetDonglePath**: The IP address or DNS hostname of the system hosting the Network License Server service which is found in the following registry key on the client system: `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common`

- **NetDonglePort**: The TCP port number through which the client and server systems have been configured to use. This value is located in the same key as NetDonglePath.
- **uniqueId**: In order to lease a license from the server, the client system must first posses a unique identification value. This value is automatically generated by applications such as FTK 3, PRTK, or DNA. (Registry Viewer and FTK 1.x cannot be used setup initial client NLS configuration at this time.)

  You can find the each client system's uniqueId by inspecting the following registry key:
  HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared

- The Client system must be configured to allow all incoming and outgoing traffic on TCP port 6921.
- The following products support the ability to lease a license from a NLS server:
  - FTK 2.2.1 and newer
  - FTK 1.81.2 and newer
  - FTK Pro 3.2 and newer
  - PRTK 6.4.2 and newer
  - DNA 3.4.2 and newer
  - Registry Viewer 1.5.4 and newer
  - AD Enterprise 3.0.3 and newer
  - AD Lab 3.0.4 and newer
  - AD Lab Lite 3.1.2 and previous
  - Mobile Phone Examiner 3.0 and newer
  - Explicit Image Detection (EID) Add-on
  - Glyph Add-on
- Use AccessData License Manager (ver. 2.2.4 or newer) to migrate licenses off other devices and onto a network device.
- When running AccessData products on Windows Vista, 7, or Server 2008 you must choose **Run as administrator** at least once in order to lease a license from a NLS server.
- If the NLS client application is having trouble leasing a license either from the NLS server, AccessData recommends that you reset the licensing configuration to default.
- To reset the licensing configuration, delete and recreate the NLS registry key located at:

  HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common