RIM/BlackBerry® Device Exploitation: Script

Page	Script
Introduction and Objectives	
01_01_01 Introductory Video	No script.
01_01_02 Introduction and Objectives	This course provides DEA personnel, to include Special Agents, Diversion Investigators, and DEA Task Force Officers, information on how to exploit BlackBerry® devices while conducting an investigation. Upon completion of this course, you will be able to Use the information on BlackBerry® communications records to help further an investigation by being able to: • Identify current capabilities of RIM/BlackBerry®. • Identify the types of BlackBerry® traffic and their routing structures. • List the types of communications records available from RIM and the type of requests legally required to obtain these records. • Identify the information contained on BlackBerry® communications records. For assistance or questions on RIM/BlackBerry Exploitation and other emerging technologies, please contact the ST Operations Support Unit at (703)495-6500 or email ST - Emerging Technologies Support.
Research in Motion (RIM) Overview	
01_02_01 Research in Motion (RIM) Overview	Research in Motion (RIM) was founded in 1984, and is headquartered in Waterloo, Canada, which is in the Ontario province, and has offices throughout North America, Europe, and the Asia-Pacific region. RIM is the company behind the BlackBerry® product line. The BlackBerry product line includes the BlackBerry® PlayBook™ tablet, the award-winning BlackBerry smartphone, software for businesses, and accessories. BlackBerry products and services are used by millions of customers around the world to stay connected to people and content. Based on 2010's 3rd quarter reporting, RIM has over 55 million BlackBerry® Subscribers worldwide and approximately 175,000 BlackBerry® Enterprise Servers (BES). RIM launched their first smartphone in 1999. A smartphone is a device that allows users to make telephone calls but also adds features that might be found on a personal digital assistant or a computer. A

Page	Script
	smartphone also offers the ability to send and receive email and edit documents. A typical Smartphone is a multi-functional computing platform that allows a user to browse the web, engage in web-based email, or have a voice conversation using a VoIP application installed on the phone, all separate from the telephone service offered by the cellular provider. The use of Smartphones in the United States grew by 50 percent from 2008 to 2009, and sales are expected to eclipse traditional cellular phone sales, shifting the balance from traditional cellular phones toward these more powerful and capable devices.
01_02_02 RIM Overview: Global Footprint	Research in Motion has a global footprint. In the U.S., there are over 20 wireless carriers; however, RIM has a presence in over 170 countries through almost 500 wireless carriers such as AT&T, Verizon wireless, Sprint/Nextel, Cricket and T-mobile.
BlackBerry® Overview	
01_03_01 Introduction to BlackBerry® Devices	BlackBerry® devices use cellular and wireless data connections (including WiFi networks) available through a number of providers which offer consumers voice and data communications such as: • PIN to PIN Communications • Blackberry® Messenger Communications • Email (BIS and BES) • Web-browsing (VoIP, Chat, Social, Networking etc.) • Text Messaging (SMS) (provided by cellular provider) • Traditional Voice
01_03_02 PIN to PIN and BlackBerry® Messenger Communications	PIN to PIN and Messenger communications are encrypted peer-to-peer messaging and file transfer between BlackBerry® devices based on their unique PIN. These messages can be sent across networks and international boundaries, via a central relay managed by RIM. PIN to PIN and Messenger communications are popular methods of communication for drug traffickers because of their belief that these methods are secure and untrackable. This method of communication is especially prevalent in Mexico and South America among the drug cartels. Real-time intercept capability of PIN to PIN and Messenger is currently in development. Historical records of the PIN to PIN connections engaged in by a BlackBerry device (which are similar to

Page	Script
	historical call detail records) may be available pursuant to a court order. PIN to PIN logs can be used to identify other devices and members of a DTO. PIN to PIN & Messenger Connection logs require a court order.
01_03_03 BlackBerry® Internet Service (BIS)	BlackBerry® Internet Service (BIS) is RIM's BlackBerry® data service that allows BlackBerry users to access web-based POP3, IMAP, and Outlook Web App email accounts without connecting through a BlackBerry Enterprise Server (BES). The BlackBerry data plan service is usually provisioned through a mobile phone service provider, though all BIS traffic passes through relay servers run by Research In Motion (RIM).
01_03_04 BlackBerry® Enterprise Service (BES)	BlackBerry Enterprise Server (BES) is a business class, email and application delivery system designed for corporate IT environments using Microsoft Exchange, Lotus Domino, and Novell GroupWise. It establishes encrypted, two-way communications between BlackBerry devices among user defined groups such as government agencies. The BES integrates with a user's corporate email account and allows users to access their mail system to receive emails (including personal), appointments, contact information, and even files from the BlackBerry device. All traffic between the enterprise network and the BlackBerry handheld device flows centrally through the BES and is encrypted and secure end-to-end. The BES also allows IT administrators to operate a global network infrastructure securely inside the 'insecure' internet and design and supply the enterprise server system in the business network. Administrators can manage the connected handsets from a central location, allowing full policy control of all users.
Requesting BlackBerry® Communication Records	
01_04_01 Requesting BlackBerry® Communication Records	Making investigative use of BlackBerry® Communications records can provide a goldmine of information for agents and analysts who know how to exploit them. The following are some examples of the types of historical records that may be obtained from RIM. • Basic Subscriber Account Information • PIN to PIN Connection Logs

Page	Script
	• Internet Browsing (I.P.) Logs • Email Logs • BES Server IP address (if targets own their BES) • Stored Content of Email (Preservation Letter (18 USC §2703(f)) followed by a Search Warrant)
01_04_02 Requesting BlackBerry® Communication Records	To request basic subscriber account information from RIM, you will need a DEA 79 (Administrative Subpoena). Typical account information you may receive with a subpoena includes : • Date account established • Email address associated with account (available if RIM provided the email account) • Email address of a 3rd party integrated ISP email account e.g., Yahoo, Hotmail, Gmail, etc. (not available if email is forwarded from a BlackBerry® account) • Phone number, SIM, IMSI, ESN, IMEI, and PIN number associated with SmartPhone SIM card authentication/registration record (analogous to a "connection record" of the device to the network). You can download a sample DEA 79 under the Resources section of this course.
01_04_03 Requesting BlackBerry® Communication Records	To request BES server identifying information from RIM, you will need a DEA 79 (Administrative Subpoena). Typical account information you may receive with a subpoena includes : • BES IP address • Billing information (may be available) You can download a sample DEA 79 under the Resources section of this course.
01_04_04 Requesting BlackBerry® Communication Records	To request transactional records from RIM, you will need a court order. Typical information you may receive with a 2703 (d) order request includes : • PIN to PIN connection logs • Internet Browser logs • SIM Swapping history logs • BIS email logs • Instant Messaging logs—may be available, depending on how the IM is accessed

Page	Script
	You can download a sample court order under the Resources section of this course.
01_04_05 Requesting BlackBerry® Communication Records	To request historical email content, you first need a preservation letter followed by a search warrant. DEA policy requires that a preservation letter MUST be sent to RIM prior to the search warrant to ensure any existing content stored by RIM is maintained by RIM until the search warrant can be issued and executed. Typically, you will be able to obtain approximately 30 days of email content if the target has a RIM-provided email account and the message is over 2 KB. You will sometimes be able to obtain up to 30 days of email content for a 3rd party integrated ISP email account and the message is over 2 KB. You can download a sample preservation letter and search warrant under the Resources section of this course.
01_04_06 Requesting BlackBerry® Communication Records	There is currently no capability to request email content sent via the BES because the RIM does not have access to the BES encryption keys. There is also no capability to request the content of PIN to PIN messages, as RIM does not maintain PIN to PIN content.
Exploiting BlackBerry® Communication Records	
01_05_01 RIM Response to Information Request	A typical response from RIM includes basic subscriber information as requested on the original subpoena. Important things to note on the response include: The reference code, which corresponds to the subpoena for the associated information. It is important to always refer to this code when contacting RIM. You should also note the carrier information, which can be used to subpoena the specific carrier for information on call records.
01_05_02 SIM Swapping Logs	SIM card swapping is a common way for targets to try to cover their tracks. A Subscriber Identity Module or SIM card is a portable chip used in some models of cellular telephones. The SIM card makes it easy to switch phones by simply removing the SIM card from one phone and placing it into another. The SIM holds personal identity information, cellular phone number, phone book, text messages and other data. Transactional records will typically show when SIM cards have been swapped from one device to another. You will need a court order to get the SIM card swapping history logs, which you may be able to use to subpoena the additional device information from the RIM.

Page	Script
01_05_03 PIN to PIN Logs	PIN to PIN Logs are similar to call detail records. They include the date, time sent and received, etc. Notice for each message the source and destination direction will change (for example, depending on whether the party is initiating or receiving the message).
01_05_04 Internet Browsing Logs	When reviewing the internet browsing logs, you can determine websites visited by the user. This log shows, for example, that a website called go.flycell.com was visited, as well as the date and time it was visited. You can use this information to subpoena the ISP and website directly. You can also use the internet browsing logs to look for other social networking sites such as Facebook, MySpace, Yahoo, etc. These sites are potential gateways to information and can open doors to determining who else may be working with your suspect.
01_05_04a Internet Browsing Logs	By following the trail found in the internet browsing logs, you can use the browsing history to subpoena records from the websites visited and potentially find additional information that can aid in your investigation.
01_05_05 Stored Communications Content	Stored communications content may include: • BlackBerry® Messenger communications (global) • BlackBerry® hosted email (xxx@Blackberry.net) • Integrated email accounts (e.g., Hotmail, Yahoo, Gmail, etc.) Typically stored communications data is routinely deleted from RIM's servers, so it is imperative to immediately serve a preservation letter to prevent deletion of data. The preservation letter should be followed by a Search Warrant served to RIM's public safety section.
01_05_06 Real-Time Data Intercept Capabilities	Real-time data intercept capabilities. The capability to conduct U.S. data intercepts of PIN to PIN and BlackBerry® Messenger Communications, as well as BlackBerry® Internet Services is possible pursuant to a court ordered Title III wiretap.
Summary	
01_06_01 Summary	This course has provided basic information about Research in Motion and how to exploit BlackBerry devices during an investigation. For assistance or questions on BlackBerry device exploitation and other emerging technologies, please contact the ST Operations Support Unit at (703)495-6500 or email ST - Emerging Technologies Support.