Attention: Check **http://www.edecdigitalforensics.com/support/support-documentation** to ensure you have the latest user manual

TARANTULA

Chinese Cell Phone Analysis Tool

Software Version 1.1 | User Manual Version 1.14.2012

User Manual

eDEC Digital Forensics

Sales Inquiries
sales@edecdigitalforensics.com
www.edecdigitalforensics.com
Tel: +1 (805) 962-3080
Fax: +1 (805) 962-3086

Support Inquiries
support@edecdigitalforensics.com
http://support.edecdigitalforensics.com
Tel: +1 (805) 962-3080

Table of Contents

1. License and Support

1.1 License Period and Updates

License Period

Tarantula typically ships with a 1 year license that includes the following:

- Software updates available on our website at least every quarter
- New cables shipped to customer upon release
- Bug fix updates available on our website on a regular basis
- Customer support via email or phone (see section 1.2 below)

Updates

Tarantula software and hardware will continue to function after the license period ends, but updates will be discontinued until a license update is purchased. License updates are typically sold anually. If you require a different license period, please contact sales@edecdigitalforensics.com.

Updates generally include:

- Extraction support updates for new devices
- Decoding support updates
- Added features

1.2 Support Resources

For the most effective support, please initiate a support ticket online via our support site or by sending an email to support@edecdigitalforensics.com (sending an email to this address will automatically generate a support ticket). We try to respond to all support inquiries within 24 hours or less.

Online Support Ticket System	http://support.edecdigitalforensics.com
Email Support	support@edecdigitalforensics.com
Phone Support	+1 (805) 962-3080

2. Introduction

2.1 Tarantula Overview

Tarantula is the first forensic tool that supports extraction and analysis of cell phones based on Chinese chipsets. It employs low-level data extraction for acquisition of cell phone flash memory, providing the user with a complete binary dump file that is automatically decoded into human-readable format. It also employs logical acquisition of certain types of devices. Tarantula is a combination of hardware and software, which together support examination of the majority of Chinese phones on the market.

Tarantula supports a wide range of devices based on Chinese chipsets, but it is most useful for examination of "white-box" phones, or "clone phones". These phones are designed and manufactured in China and have numerous features for 1/3 to 1/5 the price of top international brand phones. Although white-box phones represent roughly 30% of the worldwide cell phone market, they are difficult to examine due to their lack of hardware and software consistency. Tarantula excels in supporting these devices.

The Tarantula Kit Includes:	▪ Tarantula Hardware Box ▪ AC power adaptor for hardware box ▪ USB data cable ▪ [29] Data cables ▪ Phone power cable - RJ45 ▪ Phone power cable – Serial ▪ Software security dongle ▪ Cell phone battery charger (with AC power adaptor) ▪ 3 eDEC Black Hole Faraday Bags, Standard size, window ▪ Quickstart guide ▪ Carrying case

3. Requirements

System Requirements:	▪ 1 Ghz 32-bit (x86) processor ▪ 512 MB of system memory ▪ [1] USB interface ▪ [1] USB interface (preferably on board)
Operating System Support:	▪ Windows XP Service Pack 3 ▪ Windows 7 32bit ▪ Windows 7 64bit must run VMware with Windows XP installed
Software Requirements:	▪ Microsoft .net framework 3.5 ▪ Microsoft SQL Server CE ▪ Tarantula hardware driver ▪ USB to Serial (Spreadtrum) driver
Power Requirements:	▪ Input: 100-240V 50/60Hz ▪ Output: DC 9V, 2000mA
Environment Requirements:	▪ Ambeint temperature: 32°F - 110°F ▪ Storage temperature: 0°F - 120°F ▪ Do not subject Tarantula hardware to excessive shock or vibration

4. Software Setup

4.1 Software Download

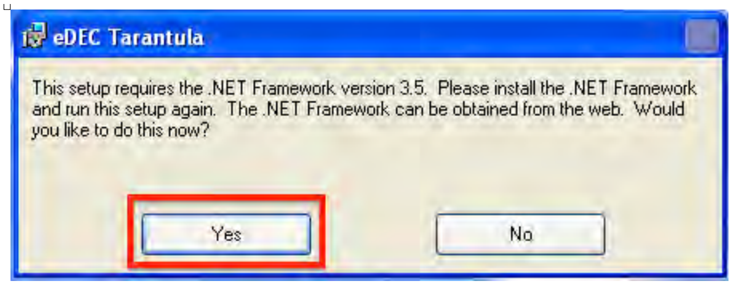
Visit www.edecdigitalforensics.com/support to download the latest version of Tarantula software.

To login to the eDEC Tarantula Downloads page, use your hardware serial number for both the username and password. The hardware serial number can be found by peeling back the bottom part of the rubber on the Tarantula hardware unit and viewing the yellow sticker.

4.2 Software Installation

Tarantula Software Installation

1. Run the file *setup.exe*
2. The software will check if .NET Framework is installed. If it does not install in properly, it will go to the Microsoft website to download. After successful download, restart installation



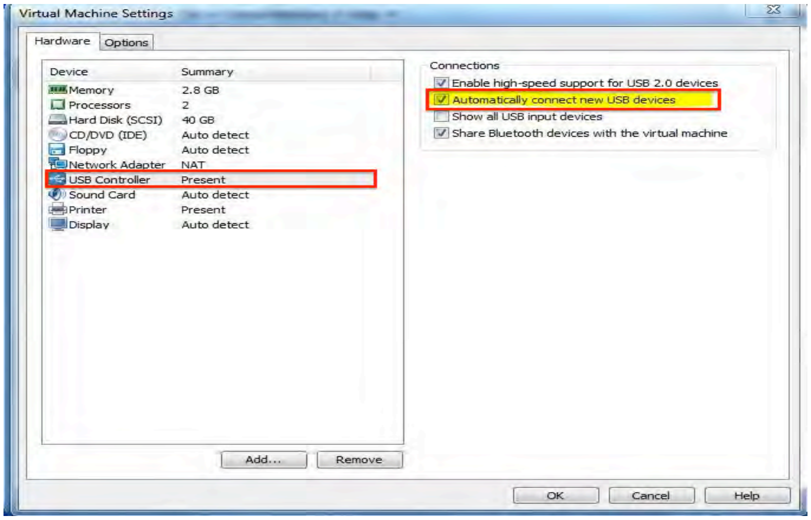
This setup requires the .NET Framework version 3.5. Please install the .NET Framework and run this setup again. The .NET Framework can be obtained from the web. Would you like to do this now?

3. Keep the default installation folder, click Next
4. Confirm the installation and click Next
5. Make sure the installation completes

To see the changes, close all of your programs, and then restart Windows.

Please Note:

- When running a Virtual Machine, make sure that the required USB's for Tarantula are defaulted to the Virtual Machine. Make sure to add the Prolific USB- Serial COMM- Port and the HID Dongle at the top/ bottom of the Virtual Machine's window. Once added, try running Tarantula again.



Device	Summary
Memory	2.8 GB
Processors	2
Hard Disk (SCSI)	40 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Connections
☑ Enable high-speed support for USB 2.0 devices
☑ Automatically connect new USB devices
□ Show all USB input devices
☑ Share Bluetooth devices with the virtual machine

- If Tarantula's window is cut off, you need to resize the text on your screen.

4.3 Tarantula Hardware Driver Installation

Tarantula Hardware Driver Installation

- Plug the Tarantula USB cable into a USB port on your computer
- Push the power button on the front of the Tarantula hardware unit
- When Windows detects the hardware and asks for the driver location, point it to the following folder

C:\Program Files\eDEC Tarantula\driver\Tarantula\

4.4 Spreadtrum Driver Installation

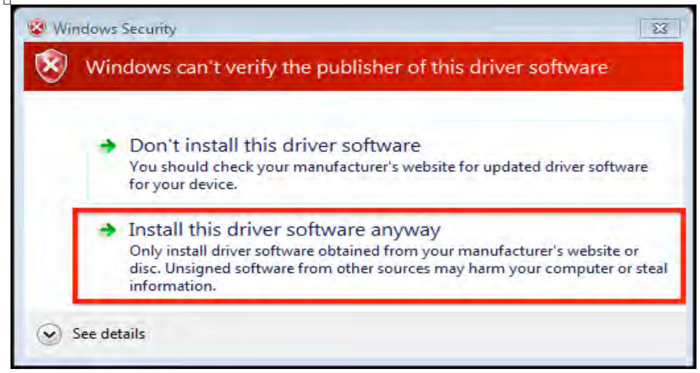
USB to Serial Driver (Spreadtrum Driver) Installation

Install the USB to Serial driver by running this file

C:\Program Files\eDEC Tarantula\driver\Spreadtrum\Install.bat

Please Note:

For Windows 7 Users, a Windows Security window may pop-up twice during the installation of the Spreadtrum Driver. Select *Install this driver software anyway*



Windows Security

Windows can't verify the publisher of this driver software

Don't install this driver software
You should check your manufacturer's website for updated driver software for your device.

Install this driver software anyway
Only install driver software obtained from your manufacturer's website or disc. Unsigned software from other sources may harm your computer or steal information.

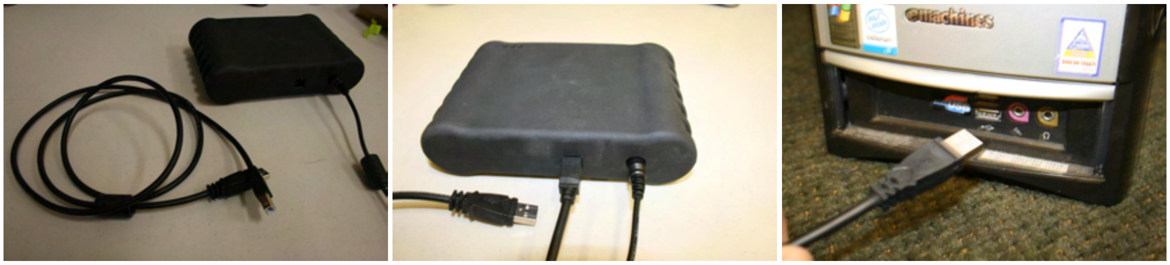
See details

5. Hardware Setup

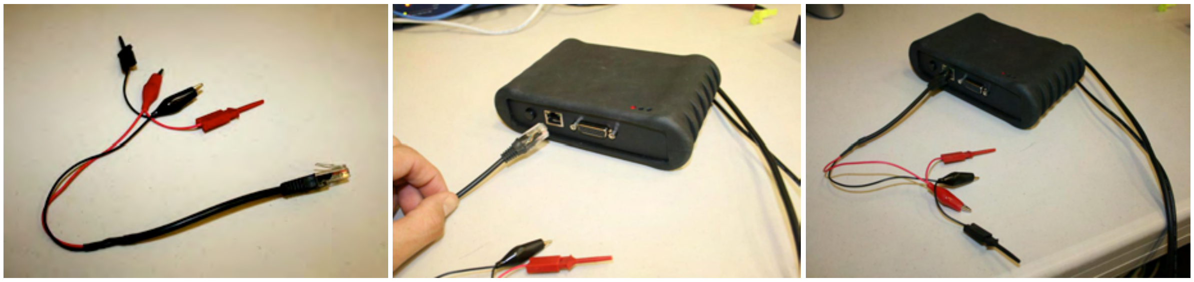
5.1 Tarantula Hardware Setup

1 Connect the AC power adaptor to the back of the Tarantula box and plug into outlet

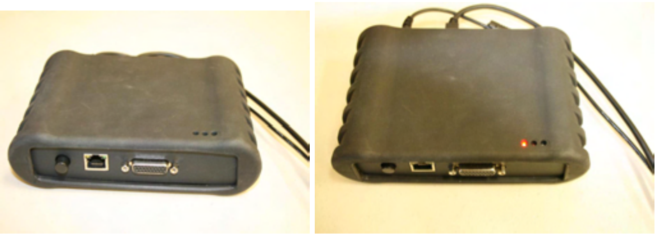
2 Insert the USB cable into the Tarantula box. Insert the other end into the USB port in your computer.



3 Insert the RJ45 power cable into the RJ45 port on the front of the device.



4 Press the power button on the front of the hardware box and make sure the power LED indicator on the top of the box is lit.



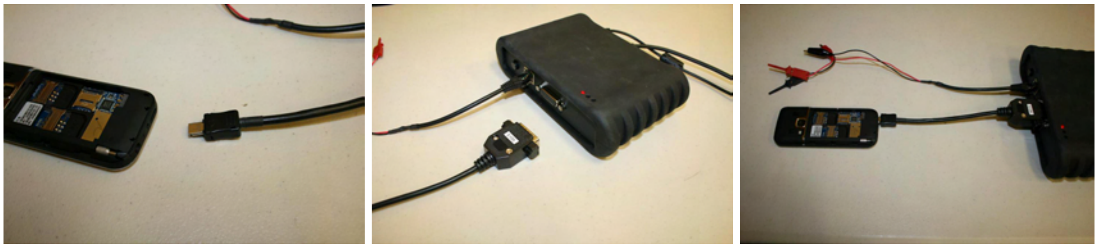
5.2 Connection to Suspect Cell Phone

1 **Allow Access to Suspect Phone Power Terminals**

Remove the back cover and battery from the suspect cell phone

2 Select Correct Data Cable and Connect

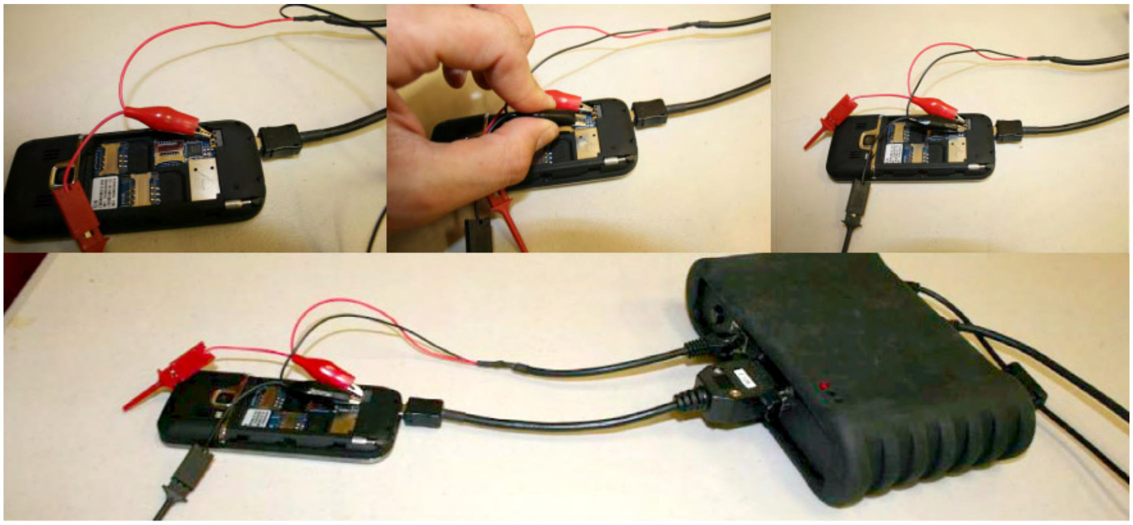
Find the data cable that matches the data port of the suspect phone and connect to the phone. Connect the serial side of the cable to the Tarantula hardware.



3 Connect Power Cable to Suspect Phone

Suspect cell phones may not be powered by a battery during examination with Tarantula. The supplied power cable must be used.

- Observe the phone battery to determine which battery terminals are used to supply power to the phone.
- Connect the RJ45 phone power cable clamps to the + and - power terminals of the phone. If the battery is not available to help determine which terminals are used for power, different combinations must be attempted. The most common terminals used are the outer terminals (1 and 3), so try those first. Tarantula automatically selects + and – power so the user does not need to match the red clamp with the positive terminal or the black clamp with the negative terminal.
- If the Tarantula hardware is not already powered on, press the On button on the front of the unit.



Please Note:

- Because of the nearly infinite amount of hardware combinations found on the types of phones that Tarantula supports, it may be difficult to match the correct data cable with the suspect phone data port. Some cables may fit the same data port, so observing the pin configuration in the phone port as well as the cable can help with selection of the right cable.

6. Performing and Examination

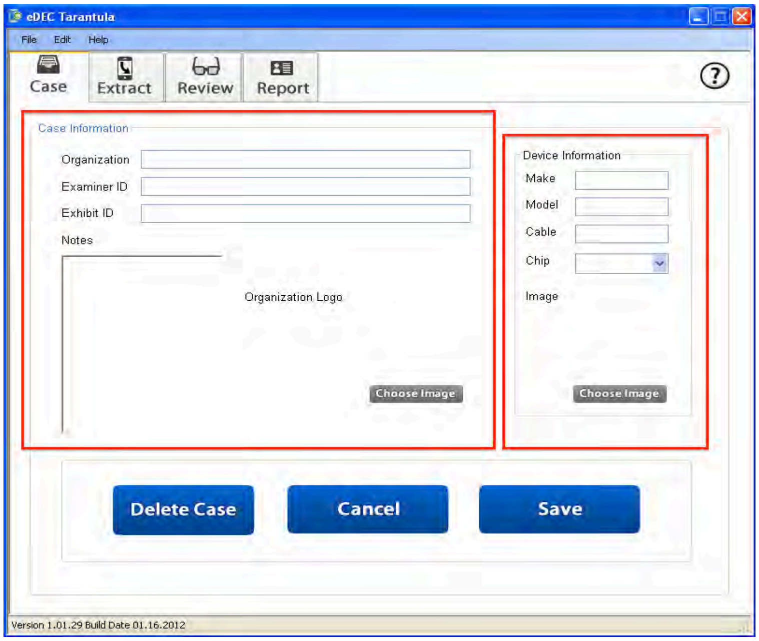
At this time, please connect the Software Security Dongle to open eDEC Tarantula

6.1 Case Admin

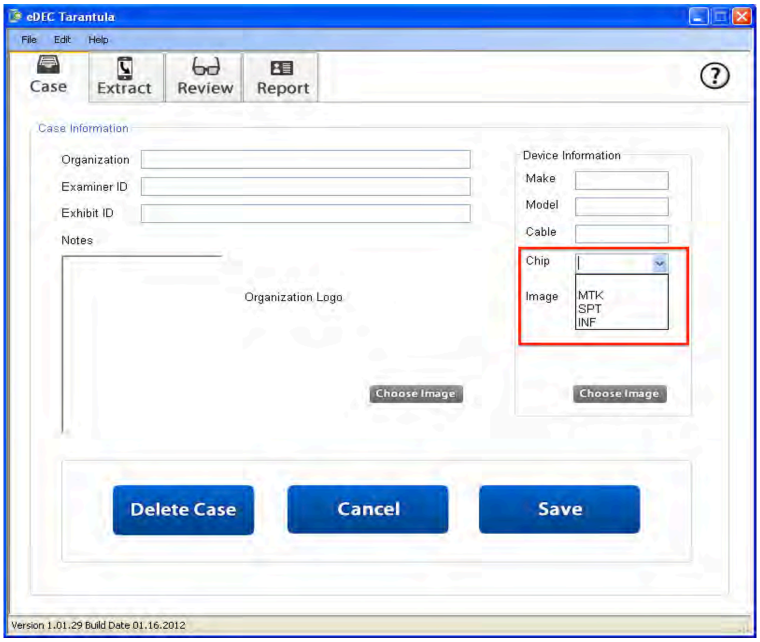
Click the **New Case** button to open a new case

You will see 2 categories:

1. Case Information – Information that relates to the examiner and the case
2. Device Information – Information that relates to the phone being examined. Please note that this section may be referred to as “Device Information (User-added)” elsewhere in the software. This is because Tarantula extracts device information during the examination that is referred to as “Phone Information (Extracted)”



- The **Chip Type** dropdown is used when importing external .bin files and using Tarantula decoding. If the chip type is unknown, leave this field blank.



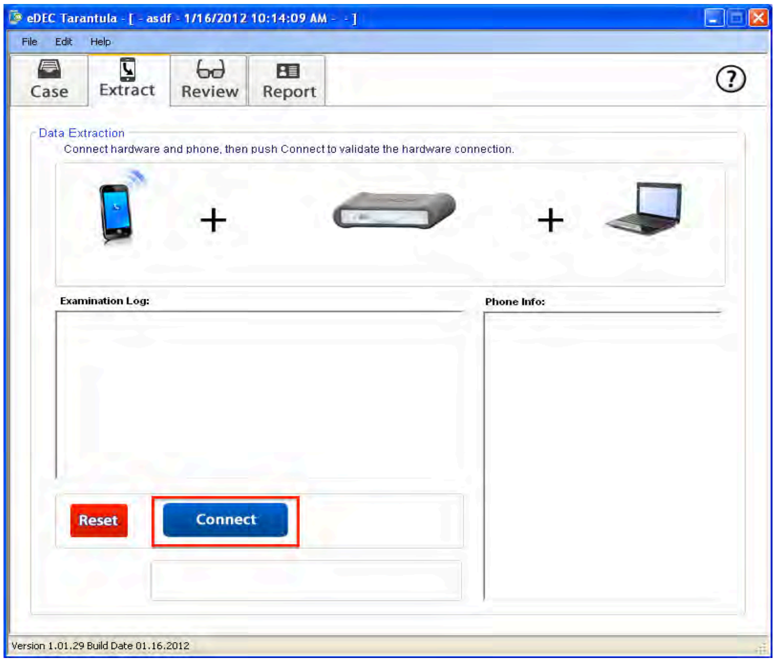
After saving the new case, select Open Case to begin the Extraction process

6.2 Extract Tab

At this time, make sure data and power cables are connected properly to the phone and to the Tarantula hardware (See **section 5.2**)

6.2.1 Initiate Connection with the Tarantula Hardware

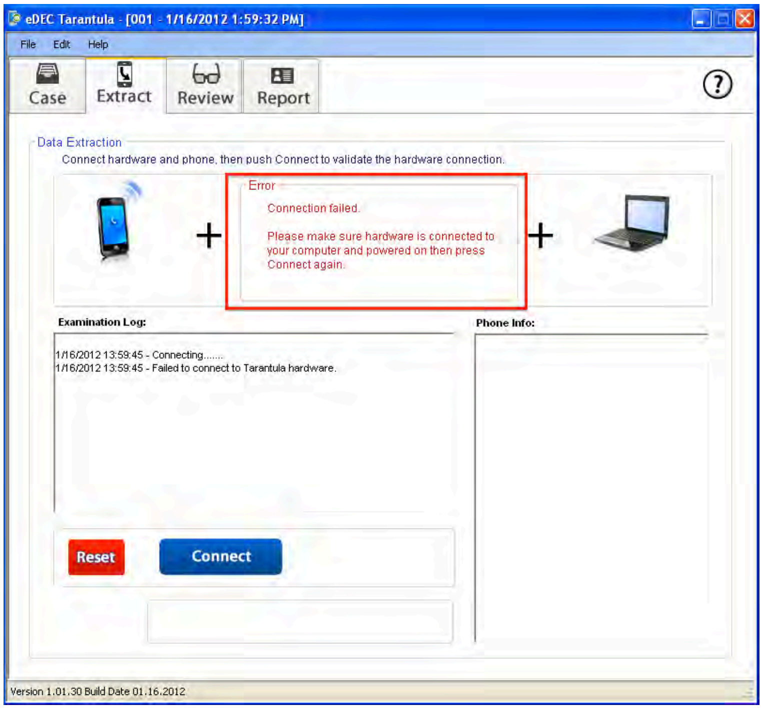
- Press *Connect* to initiate a connection with the Tarantula hardware (If the connection is successful, please go to **step 6.2.2)**



Connect hardware and phone, then push Connect to validate the hardware connection.

Version 1.01.29 Build Date 01.16.2012

- If the connection is unsuccessful like the screenshot below, please try the following:



Connect hardware and phone, then push Connect to validate the hardware connection.

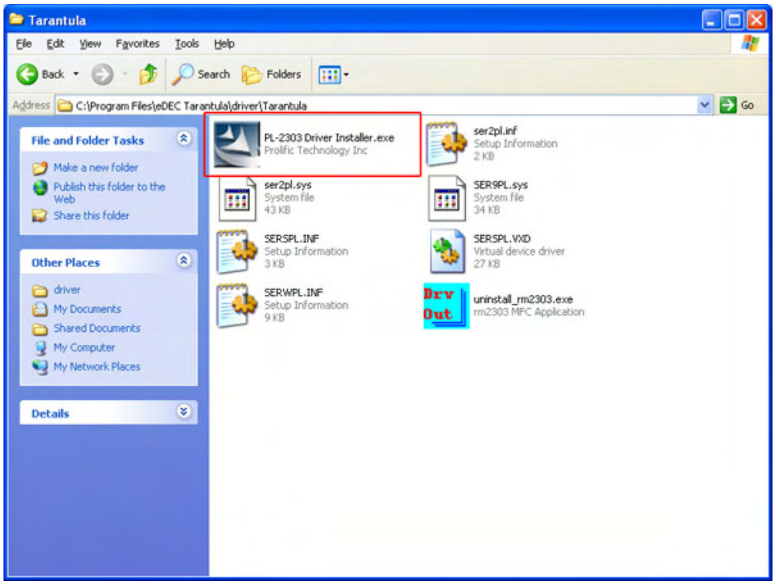
Connection failed.

Please make sure hardware is connected to your computer and powered on then press Connect again.

```
1/16/2012 13:59:45 - Connecting.......
1/16/2012 13:59:45 - Failed to connect to Tarantula hardware.
```

Version 1.01.30 Build Date 01.16.2012

1. Make sure Tarantula is connected correctly and turned on and push **Connect** again
2. If the connection is still unsuccessful, try reinstalling the Tarantula hardware driver by clicking the file in, *C:\Program Files\eDEC Tarantula\driver\Tarantula\* and shown in the picture below



C:\Program Files\eDEC Tarantula\driver\Tarantula

PL-2303 Driver Installer.exe
Prolific Technology Inc

ser2pl.inf
Setup Information
2 KB

ser2pl.sys
System file
43 KB

SER9PL.sys
System file
34 KB

SERSPL.INF
Setup Information
3 KB

SERSPL.VXD
Virtual device driver
27 KB

SERWPL.INF
Setup Information
9 KB

uninstall_rm2303.exe
rm2303 MFC Application

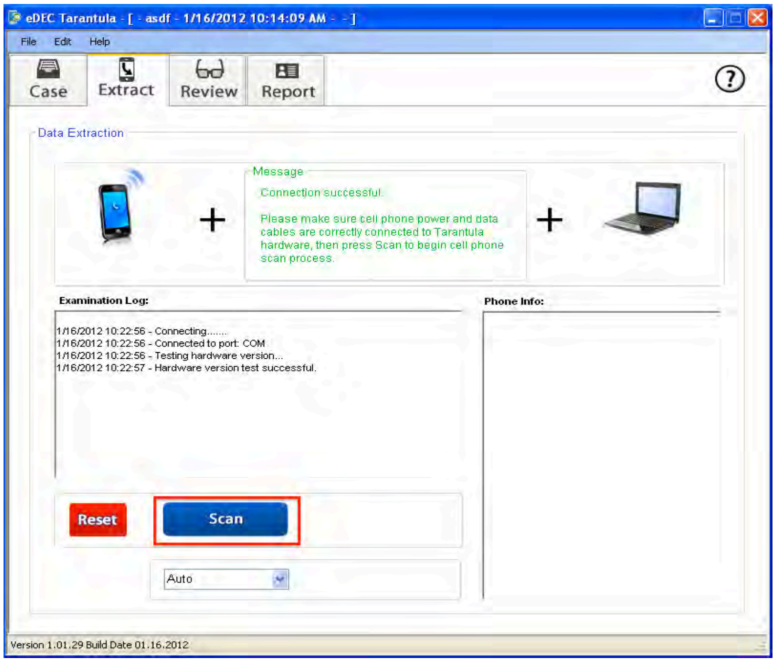
After successful installation, your system may need to be restarted.

Please Note:

Depending on the software version you have, Tarantula may require a hardware firmware upgrade, which will happen automatically during this connection process. Please do not power off the unit during the firmware upgrade

6.2.2 Scan the Phone

Press *Scan* to initiate a scan of the phone.



Message

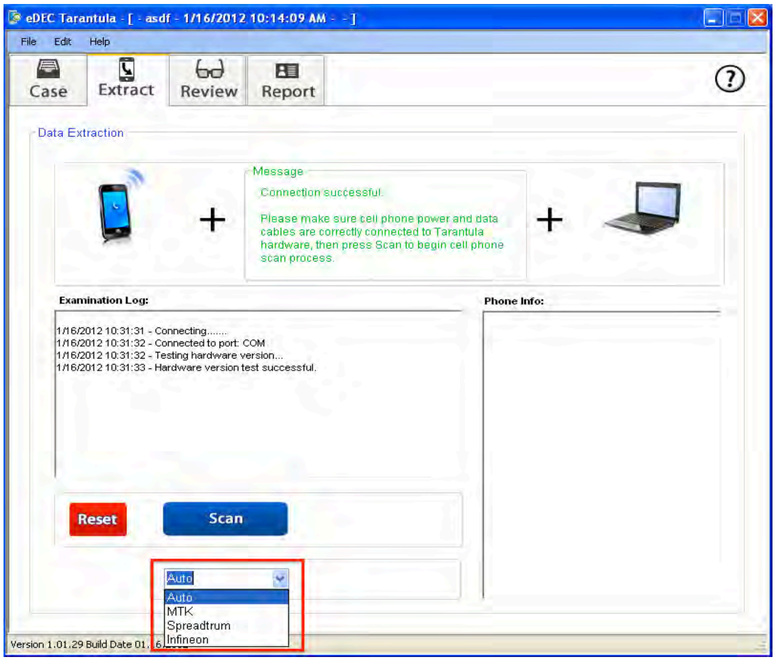
Connection successful.

Please make sure cell phone power and data cables are correctly connected to Tarantula hardware, then press Scan to begin cell phone scan process.

```
1/16/2012 10:22:56 - Connecting.......
1/16/2012 10:22:56 - Connected to port: COM
1/16/2012 10:22:56 - Testing hardware version...
1/16/2012 10:22:57 - Hardware version test successful.
```

Version 1.01.29 Build Date 01.16.2012

- If you know the chip type of the phone, you can click on the drop down, shown below, and select the matching chip. If not, select Auto.



Message

Connection successful.

Please make sure cell phone power and data cables are correctly connected to Tarantula hardware, then press Scan to begin cell phone scan process.

```
1/16/2012 10:31:31 - Connecting.......
1/16/2012 10:31:32 - Connected to port: COM
1/16/2012 10:31:32 - Testing hardware version...
1/16/2012 10:31:33 - Hardware version test successful.
```

Version 1.01.29 Build Date 01.16.2012

- The scan and extraction processes require user interaction with the phone at specific times. Press the power button on the phone at the right times by carefully following the on-screen prompts.

- During the scan process, Tarantula attempts to determine the chip type in the phone. The phone power button will need to be held until Tarantula scans successfully.
  If a successful scan cannot be achieved, perform the following operations:
  1. Make sure the correct power button is being pushed on the phone
  2. Make sure the battery clamps are on the correct power contacts. See “Connect Power Cable to Suspect Phone” section above.
  3. Try the scan again

  If still unsuccessful:
  1. Remove the serial data cable from the phone and the Tarantula hardware and connect it back in to both
  2. Remove the RJ-45 power from the phone and the Tarantula unit and connect it back in to both or switch to the Serial power cable.
  3. Turn the Tarantula unit off and back on
  4. Restart the software
  5. Try the scan again

- Once a successful scan is achieved, you will be alerted to move to the next step to perform an extraction

6.2.3 Extract Data

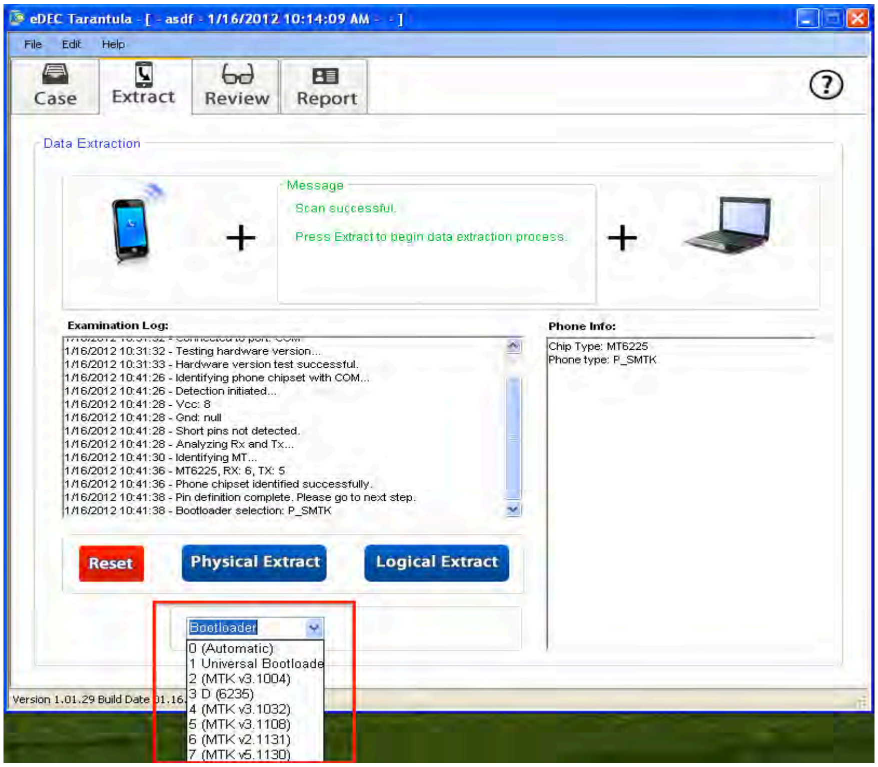
Choose *Physical Extract* or *Logical Extract* to begin the extraction

- The scan and extraction processes require user interaction with the phone at specific times. Press the power button on the phone at the right times by carefully following the on-screen prompts.

  Tip: If the phone’s chip type is a Spreadtrum, you do not need to hold the power button during the scan and extraction process. If it is a Mediatek chip, you must hold the power button down in the beginning of the extraction until the bootloader is download is complete, then you may let go of the power button.

- Information extracted physically and logically will be displayed in the **Phone Info** box on the right side of the Extract tab
- If a successful extraction cannot initiate, please try the following:
  1. Make sure to follow the on-screen prompts to understand when to push the power button. Pushing the power button early or late can cause unsuccessful extractions
  2. Retry the extraction

- When extraction initiates, a bootloader will be downloaded to the phone and extraction of the .bin (binary) file will begin. If the bootloader is known, you may select a specific one



Scan successful.

Press Extract to begin data extraction process.

```
1/16/2012 10:31:32 - Connected to port: COM
1/16/2012 10:31:32 - Testing hardware version...
1/16/2012 10:31:33 - Hardware version test successful.
1/16/2012 10:41:26 - Identifying phone chipset with COM...
1/16/2012 10:41:26 - Detection initiated...
1/16/2012 10:41:28 - Vcc: 8
1/16/2012 10:41:28 - Gnd: null
1/16/2012 10:41:28 - Short pins not detected.
1/16/2012 10:41:28 - Analyzing Rx and Tx...
1/16/2012 10:41:30 - Identifying MT...
1/16/2012 10:41:36 - MT6225, RX: 6, TX: 5
1/16/2012 10:41:36 - Phone chipset identified successfully.
1/16/2012 10:41:38 - Pin definition complete. Please go to next step.
1/16/2012 10:41:38 - Bootloader selection: P_SMTK
```

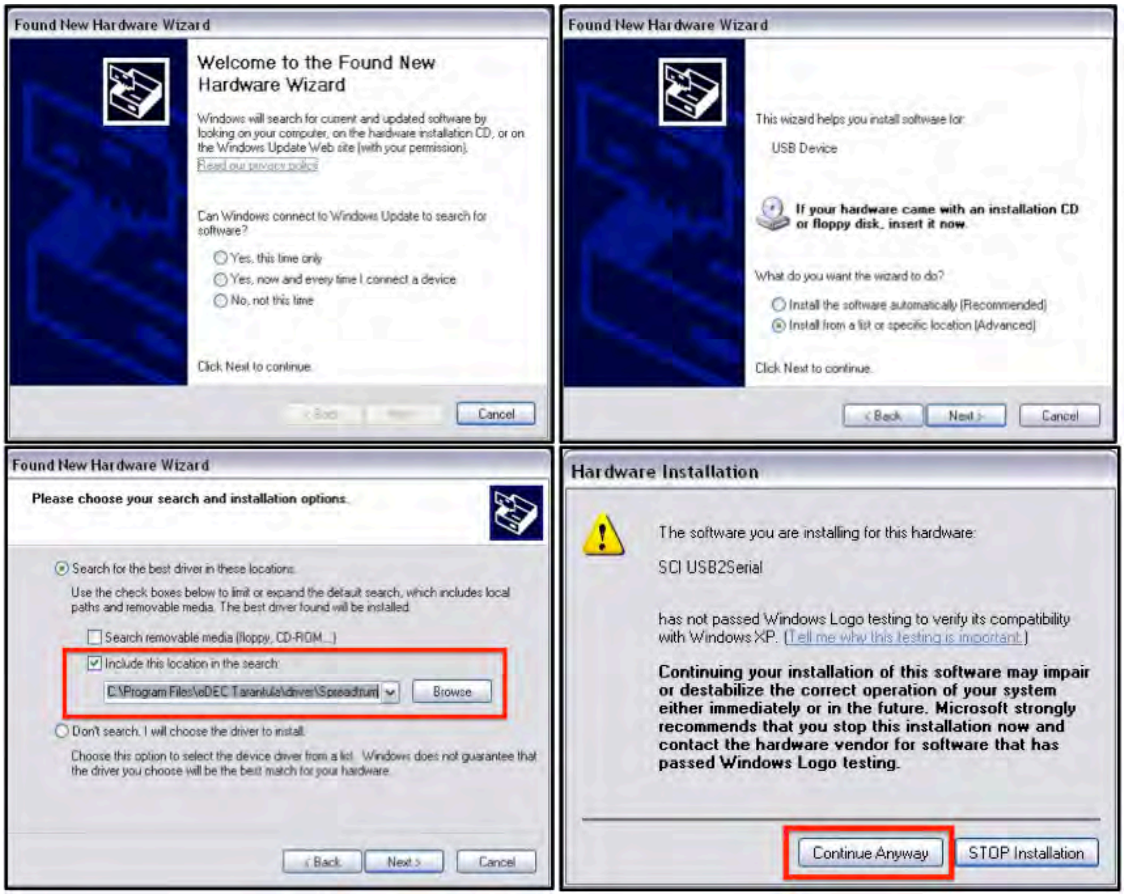
Chip Type: MT6225
Phone type: P_SMTK

Version 1.01.29 Build Date 01.16.

- If extraction stops during the .bin file extraction, please try the following:
  1. Remove the RJ-45 power cable from the phone and Tarantula hardware. Find the serial power cable and connect it between the Tarantula hardware and the data cable. Connect the power clamps on this cable to the power terminals on the phone.
  2. If the phone was identified as a Spreadtrum phone, try reinstalling the Spreadtrum driver (see below)
  3. Retry the extraction

- If a phone with a **Spreadtrum** chip is detected, Windows may ask to install a driver during the Extraction process. Follow these steps:

  1. Select *Yes, this time only,* then click Next
  2. Select *Install from a list or specific location,* then click Next
  3. Select *Search for the best driver in these locations,* then search for *C:\Program Files\eDEC Tarantula\driver\Spreadtrum\Install.bat,* then click Next
  4. A *Hardware Installation* window will pop-up, select *Continue Anyway*
  5. Select Finish in the *Found New Hardware Wizard,* then restart Tarantula/ restart Windows



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy

Can Windows connect to Windows Update to search for software?

○ Yes, this time only
○ Yes, now and every time I connect a device
○ No, not this time

Click Next to continue.

Found New Hardware Wizard

This wizard helps you install software for:

USB Device

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

○ Install the software automatically (Recommended)
● Install from a list or specific location (Advanced)

Click Next to continue.

Found New Hardware Wizard

Please choose your search and installation options.

● Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

□ Search removable media (floppy, CD-ROM...)
☑ Include this location in the search:
C:\Program Files\eDEC Tarantula\driver\Spreadtrum

○ Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

Hardware Installation

The software you are installing for this hardware:

SCI USB2Serial

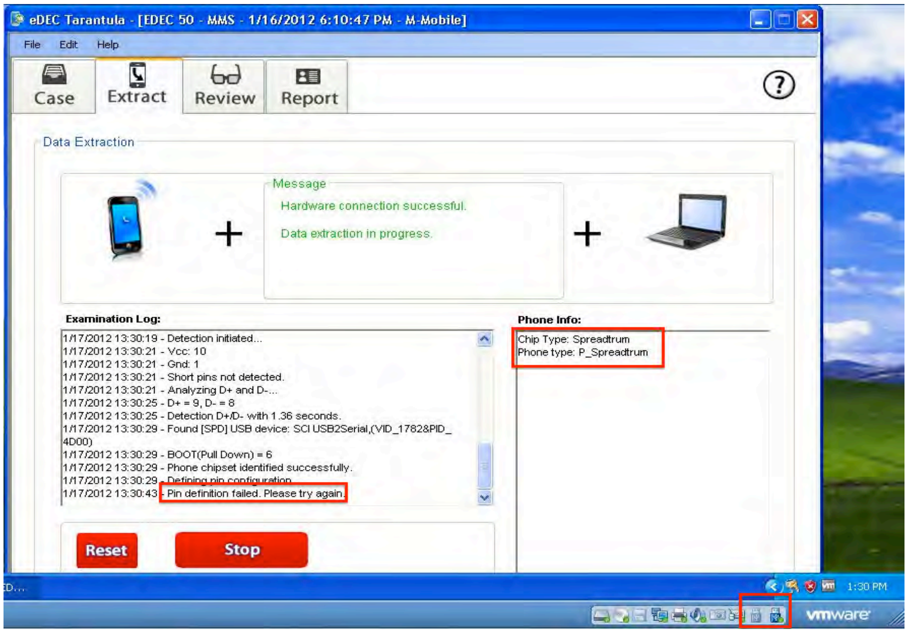
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

After successful extraction, move on to the Review tab

Please Note:

- When extracting a Spreadtrum phone on VMware for the first time, the extraction may fail as shown below. Make sure that all USB devices are defaulted to VMware and that the Spreadtrum driver is installed. Restart Tarantula. The Spreadtrum USB device name is SCI USB2Serial.



Hardware connection successful.

Data extraction in progress.

Examination Log:

```
1/17/2012 13:30:19 - Detection initiated...
1/17/2012 13:30:21 - Vcc: 10
1/17/2012 13:30:21 - Gnd: 1
1/17/2012 13:30:21 - Short pins not detected.
1/17/2012 13:30:21 - Analyzing D+ and D-...
1/17/2012 13:30:25 - D+ = 9, D- = 8
1/17/2012 13:30:25 - Detection D+/D- with 1.36 seconds.
1/17/2012 13:30:29 - Found [SPD] USB device: SCI USB2Serial,(VID_1782&PID_
4D00)
1/17/2012 13:30:29 - BOOT(Pull Down) = 6
1/17/2012 13:30:29 - Phone chipset identified successfully.
1/17/2012 13:30:29 - Defining pin configuration
1/17/2012 13:30:43 - Pin definition failed. Please try again.
```

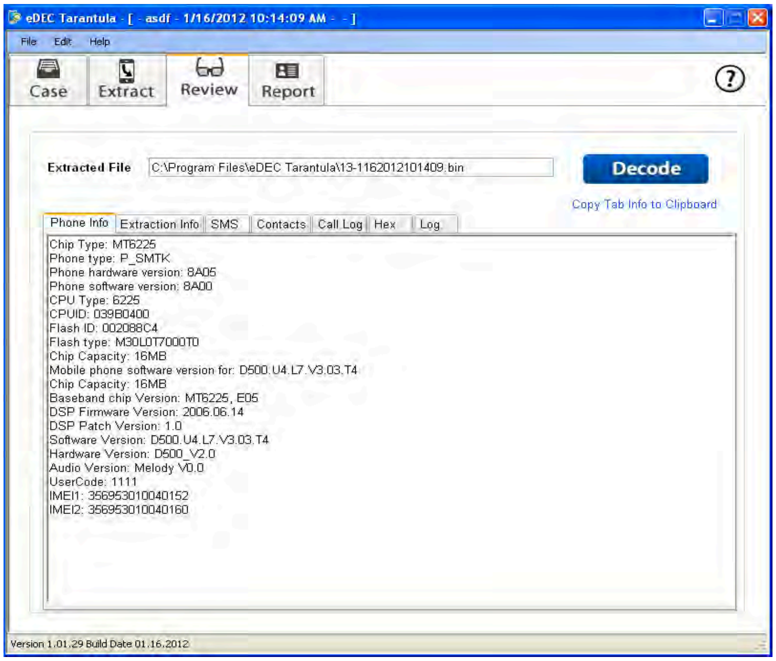
Phone Info:

```
Chip Type: Spreadtrum
Phone type: P_Spreadtrum
```

- If an Infineon phone is identified and fails during the extraction proccess, you may need to press the power button several times and/or undo one of the power cable clamps and reclamp it during the extraction.

6.3 Review Tab

Click the **Review** tab to view and decode extracted information



Extracted File: C:\Program Files\eDEC Tarantula\13-1162012101409.bin

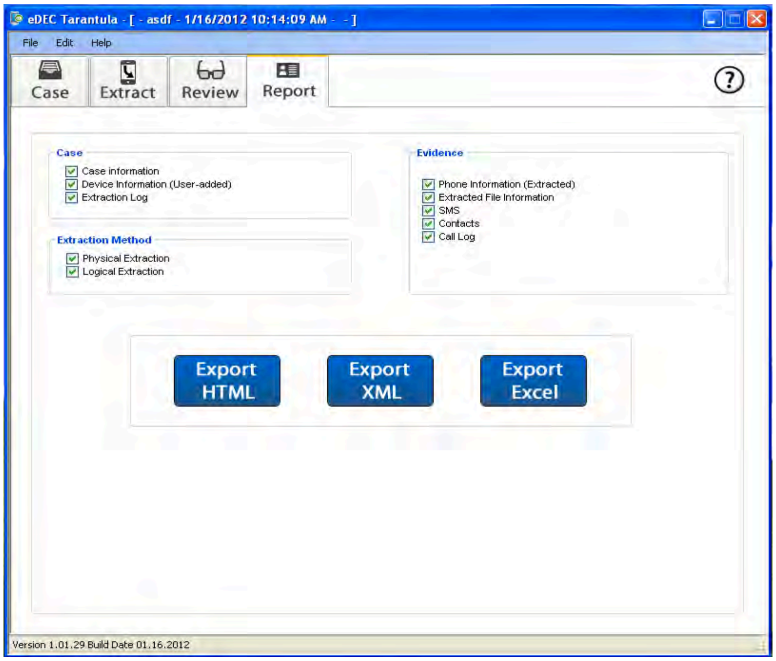
```
Chip Type: MT6225
Phone type: P_SMTK
Phone hardware version: 8A05
Phone software version: 8A00
CPU Type: 6225
CPUID: 039B0400
Flash ID: 002088C4
Flash type: M30L0T7000T0
Chip Capacity: 16MB
Mobile phone software version for: D500.U4.L7.V3.03.T4
Chip Capacity: 16MB
Baseband chip Version: MT6225, E05
DSP Firmware Version: 2006.06.14
DSP Patch Version: 1.0
Software Version: D500.U4.L7.V3.03.T4
Hardware Version: D500_V2.0
Audio Version: Melody V0.0
UserCode: 1111
IMEI1: 356953010040152
IMEI2: 356953010040160
```

Version 1.01.29 Build Date 01.16.2012

- If a logical extraction took place, any extracted information will populate under the information tabs
- If a physical extraction took place, the name of the extracted binary file will show in the **Extracted File** field.
- Click **Decode** to parse data from the .bin file into the information tabs

6.4 Report Tab

Click the **Report** tab to build a report



Case
☑ Case information
☑ Device Information (User-added)
☑ Extraction Log

Extraction Method
☑ Physical Extraction
☑ Logical Extraction

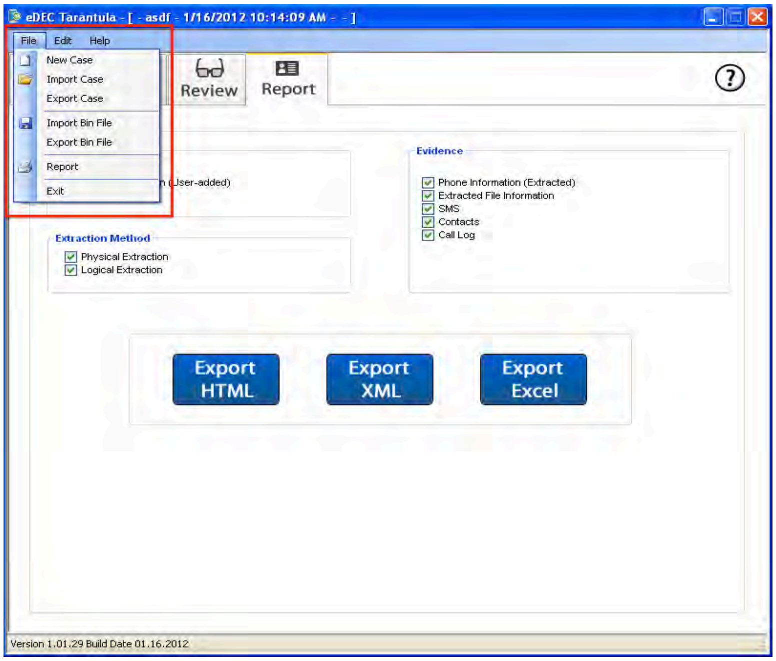
Evidence
☑ Phone Information (Extracted)
☑ Extracted File Information
☑ SMS
☑ Contacts
☑ Call Log

Version 1.01.29 Build Date 01.16.2012

- Select which Case or Evidence items to export to a report
- Report assests are saved separately in the selected folder. If you would like to bundle them in a separate folder, make a new one and choose to save there.

6.5 Import and Export

Click the **File** from the header toolbar for additional actions



n (User-added)

Extraction Method

☑ Physical Extraction
☑ Logical Extraction

Evidence

☑ Phone Information (Extracted)
☑ Extracted File Information
☑ SMS
☑ Contacts
☑ Call Log

Binary File Import/Export

- .bin files may be imported for decoding by clicking the **Import Bin File**
  - To properly decode an imported .bin file, select the correct chip type under the Edit Case window. If the chip type is unknown, select and test each chip type in the drop-down then click **Decode** under the Review tab
- Previously extracted .bin files may be exported by clicking the **Export Bin File** and choosing a location to save the file.
- Exported binary files will also include a Text file with a timestamp and hash, which can be used for auditing purposes.

Case File Import/Export

- Cases can be imported and exported by clicking on **Import Case** and **Export Case**
  - Tarantula uses a .tcdf extension when importing and exporting cases
  - Cases can be exported and will include .xml data
- When a case with the same Organization name is imported, the imported case will say (Copy) next to Organization name

Please Note:

Importing an external .bin file will overwrite any previously extracted .bin file. Create a new case to avoid overwriting data

7. Warranty

7.1 Tarantula Hardware

If within one (1) year from the date of purchase, the product fails due to a defect in material or workmanship, eDEC Digital Forensics will repair if possible or replace it free of charge. This warranty applies only to the original purchaser and is not transferable.

eDEC DIGITAL FORENSICS WILL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES TO PURCHASER, OR ANY OTHER PARTY, FOR ANY LOSS, DAMAGE, INJURY OR EXPENSE OF ANY KIND OR NATURE CAUSED DIRECTLY OR INDIRECTLY BY THE PRODUCT OR THE FAILURE OF THE PRODUCT TO OPERATE PROPERLY. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

THIS WARRANTY IS IN LIEU OF ALL OTHER EXPRESS OR IMPLIED WARRANTIES. ALL IMPLIED WARRANTIES, INCLUDING THE WARRANTY OF MERCHANTABILITY AND THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, ARE HEREBY MODIFIED TO EXIST ONLY AS CONTAINED IN THIS LIMITED WARRANTY, AND SHALL BE OF THE SAME DURATION AS THE WARRANTY PERIOD STATED ABOVE. SOME STATES DO NOT ALLOW LIMITATIONS ON THE DURATION OF AN IMPLIED WARRANTY, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

The warranty does not apply to: (a) damage caused by accident, abuse, in handling, dropping; (b) acts of God; (c) units which have been subject to unauthorized repair, opened, taken apart or otherwise modified; (d) units not used in accordance with directions; (e) damages exceeding the cost of the product; (f) depreciated or loss of charge time; (g) the finish on any portion of the product, such as surface scratches and/or weathering, as this is considered normal wear and tear.

Warranty service is available by mailing postage prepaid to the authorized service facility provided. Warranty does not cover the cost of postage to send the product in for service. Purchaser is responsible for safely sending the product to repair facility. Please be sure to wrap the product securely when mailing to avoid shipping damage. A valid copy of original invoice and Return Merchandise Authorization (or RMA) are required for all warranty services. Please contact support@edecdigitalforensics.com in order to obtain an RMA.