



TARANTULA

Chinese Cell Phone Analysis Tool

Software Version 1.0 | User Manual Version 12.10.11

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

0. License and Support	1
0.1 License Period and Updates.....	1
1.2 Support Resources.....	1
1. Introduction	2
1.1 Tarantula Overview.....	2
2. Requirements	2
3. Software Setup	3
3.1 Software Download.....	3
3.2 Software Installation.....	3
4. Hardware Setup	4
4.1 Tarantula Hardware Setup.....	4
4.2. Connection to Suspect Cell Phone.....	5
5. Performing an Examination	6
5.1 Case Admin.....	6
5.2 Extract Tab.....	7
5.2.1 Initiate Connection with the Tarantula Hardware.....	7
5.2.2 Scan the Phone.....	9
5.2.3 Extract Data.....	10
5.3 Review Tab	11
5.4 Report Tab	12
5.5 Tools Tab	12
5. Warranty	13

0. License and Support

0.1 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 annually. 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

0.2 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

1. Introduction

1.1 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:	<ul style="list-style-type: none"> ▪ 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
------------------------------------	---

2. Requirements

System Requirements:	<ul style="list-style-type: none"> ▪ 1 Ghz 32-bit (x86) processor ▪ 512 MB of system memory ▪ [1] USB interface ▪ [1] USB interface (preferably on board) ▪ Windows XP, SP2 or above
Operating System Support:	<ul style="list-style-type: none"> ▪ Windows XP, SP2 or above
Software Requirements:	<ul style="list-style-type: none"> ▪ Microsoft .net framework ▪ Microsoft SQL Server CE ▪ Dongle driver ▪ Tarantula hardware driver ▪ USB to Serial (Spreadtrum) driver
Power Requirements:	<ul style="list-style-type: none"> ▪ Input: 100-240V 50/60Hz ▪ Output: DC 9V, 2000mA
Environment Requirements:	<ul style="list-style-type: none"> ▪ Ambient temperature: 32°F - 110°F ▪ Storage temperature: 0°F - 120°F ▪ Do not subject Tarantula hardware to excessive shock or vibration

3. Software Setup

3.1 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.

3.2 Software Installation

1

Tarantula Software Installation

- Run the file *setup.msi*
- The software will check if .NET Framework is installed. If not, it will go to the Microsoft website to download. After successful download, restart installation.
- Keep the default installation folder, click Next
- Confirm the installation and click Next
- Make sure the installation completes

2

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\`

3

Dongle Security Driver Installation

Tarantula uses a dongle for software security, run this file to install the dongle driver:

`C:\Program Files\eDEC Tarantula\dongle\dongle_winxp_32`

4

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`

4. Hardware Setup

4.1 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.



4.2 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.

Tip: 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.



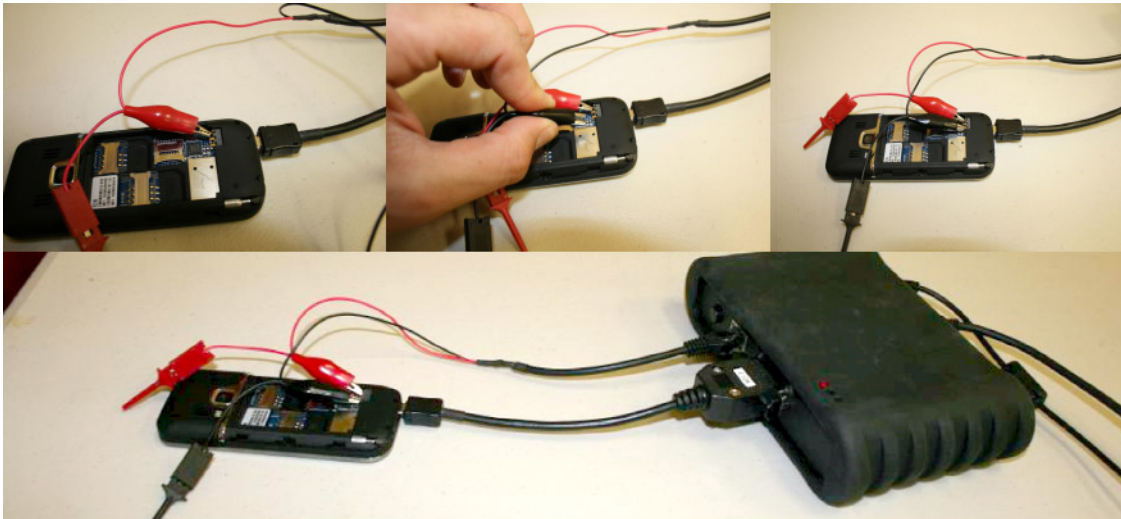
3 Connect Power Cable to Suspect Phone

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.

Tip: 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.



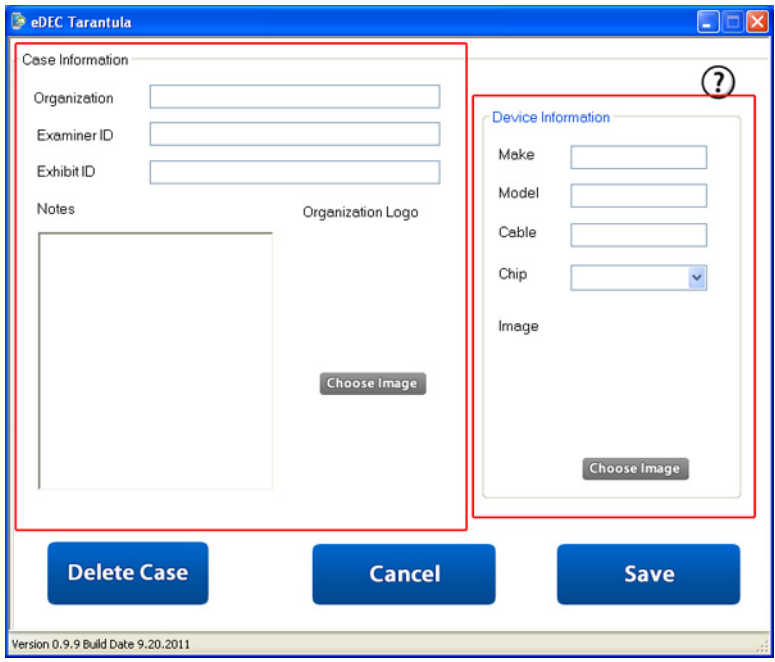
5. Performing an Examination

5.1 Case Admin

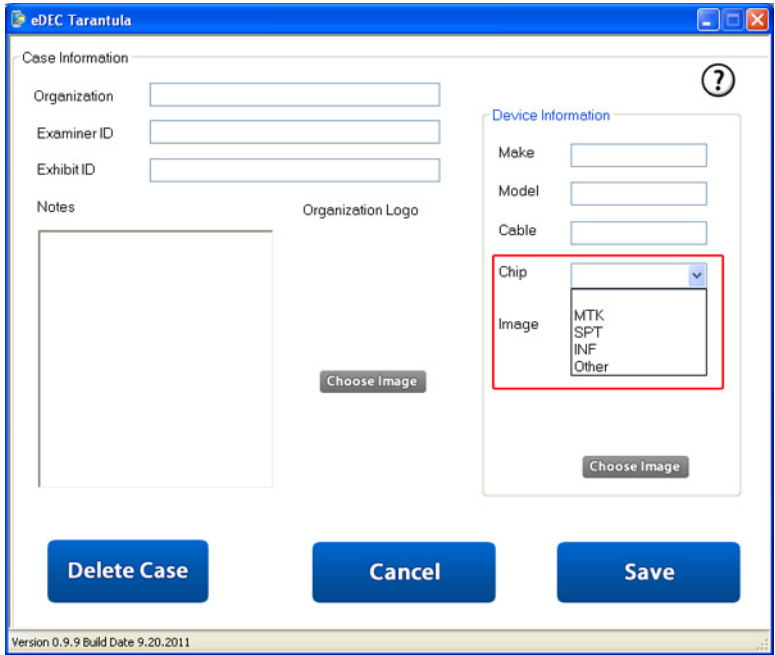
Click the **New Case** button to open a new case

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)”



Note: 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.

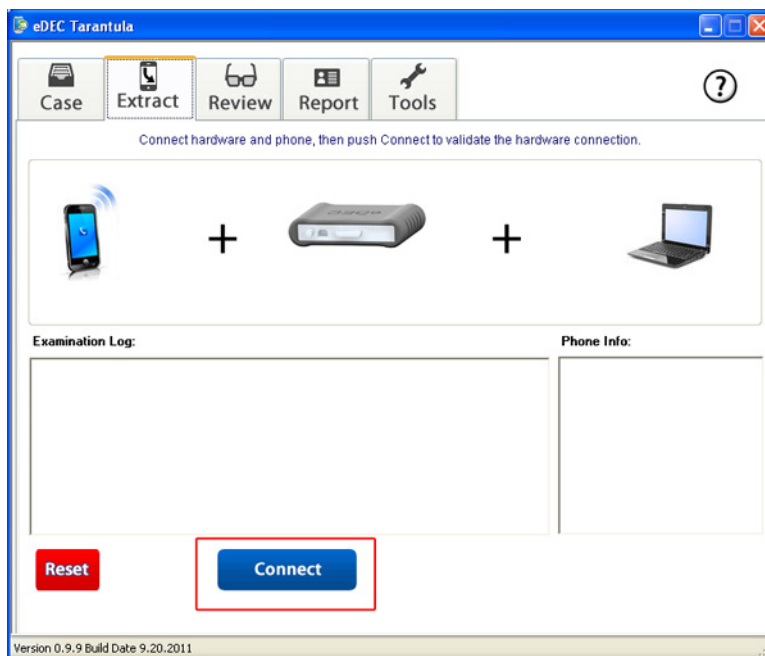


5.2 Extract Tab

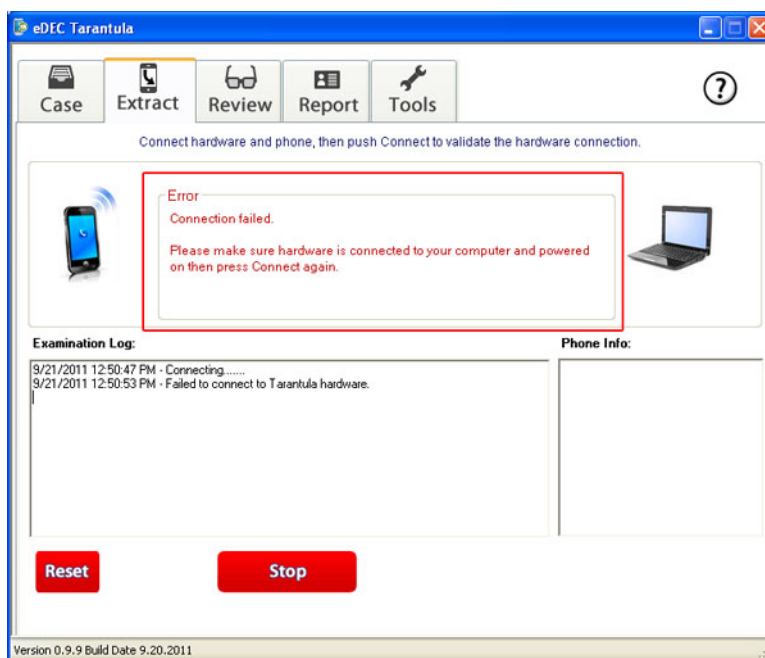
Note: At this time, make sure data and power cables are connected properly to the phone and to the Tarantula hardware (See section 4.2)

5.2.1 Initiate Connection with the Tarantula Hardware

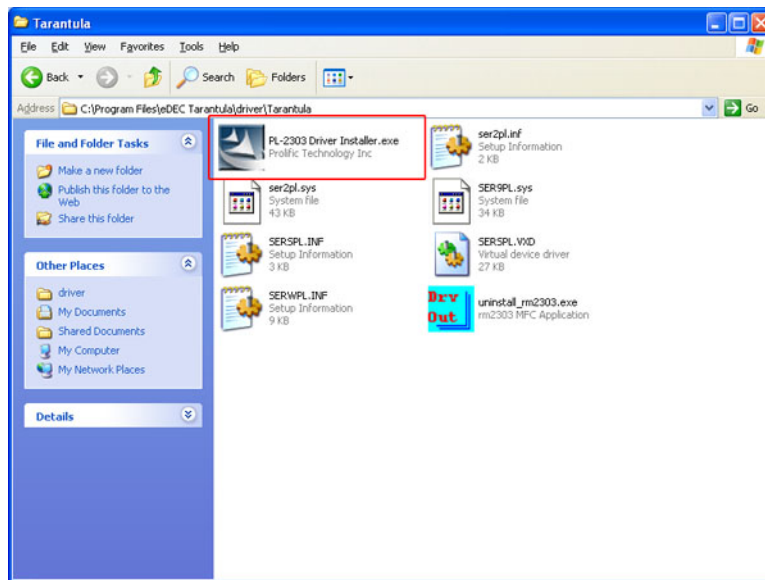
Press *Connect* to initiate a connection with the Tarantula hardware



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



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 **section 3.2 Step 2**, and shown in the picture below

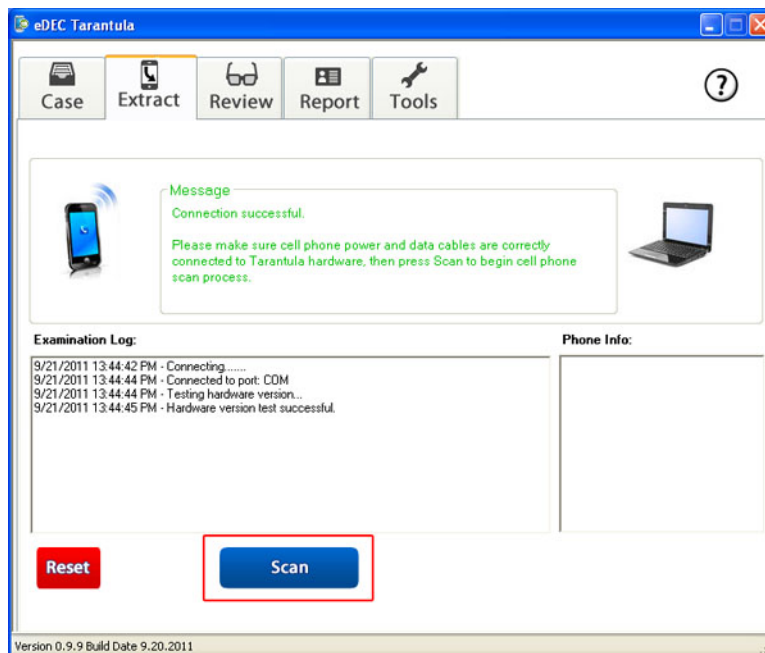


3. After successful installation, your system may need to be restarted.

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.

5.2.2 Scan the Phone

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



- 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 phone with a Spreadtrum chip is detected, Windows might ask to install a driver during the scan process. This may also happen during the extraction process. Point the driver to the location listed in **Section 3.2 Step 4**. After the driver is installed, retry the scan or extraction

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:

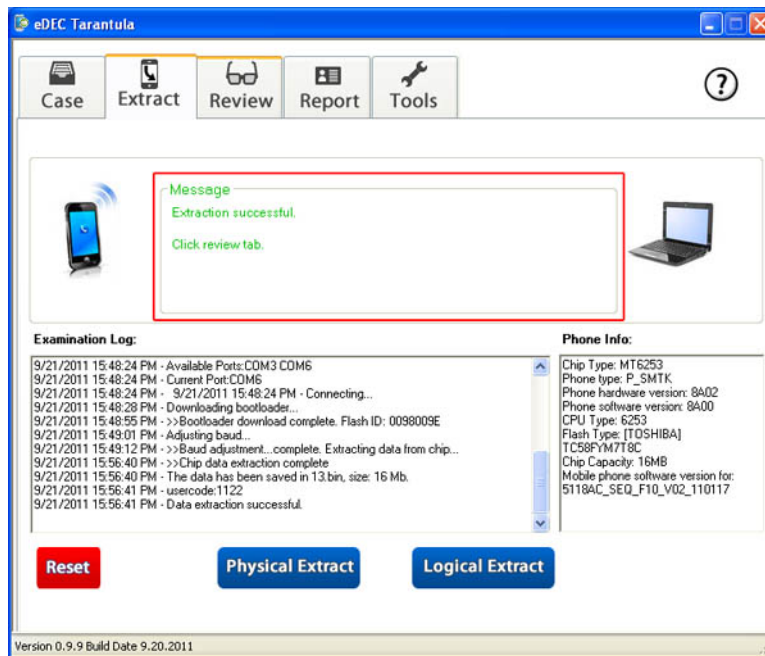
1. Remove the serial data cable from the phone and the Tarantula hardware and connect it back in to both
2. Remove the RJ-45 power from the phone and the Tarantula unit and connect it back in to both.
3. Turn the Tarantula unit off and back on
4. Restart the software
5. Try the scan again

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

5.2.3 Extract Data

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

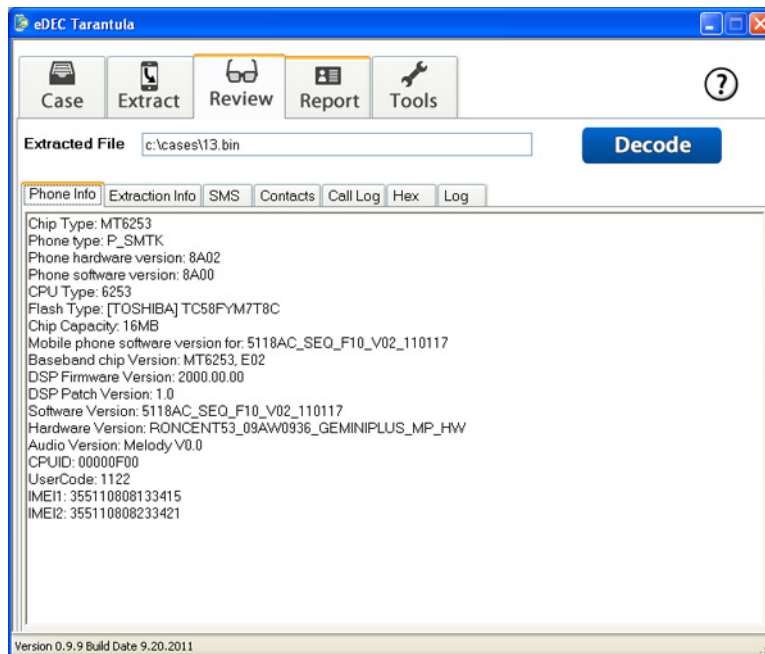
- The scan and extraction processes require user interaction with the phone at specific times. Press the power button on the phone at the right times by carefully following the on-screen prompts.
- If a successful extraction cannot initiate, please try the following:
 1. Make sure to follow the on-screen 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 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 above)
 3. Retry the extraction
- Information extracted physically and logically will be displayed in the **Phone Info** box on the right side of the Extract tab



- After successful extraction, move on to the Review tab

5.3 Review Tab

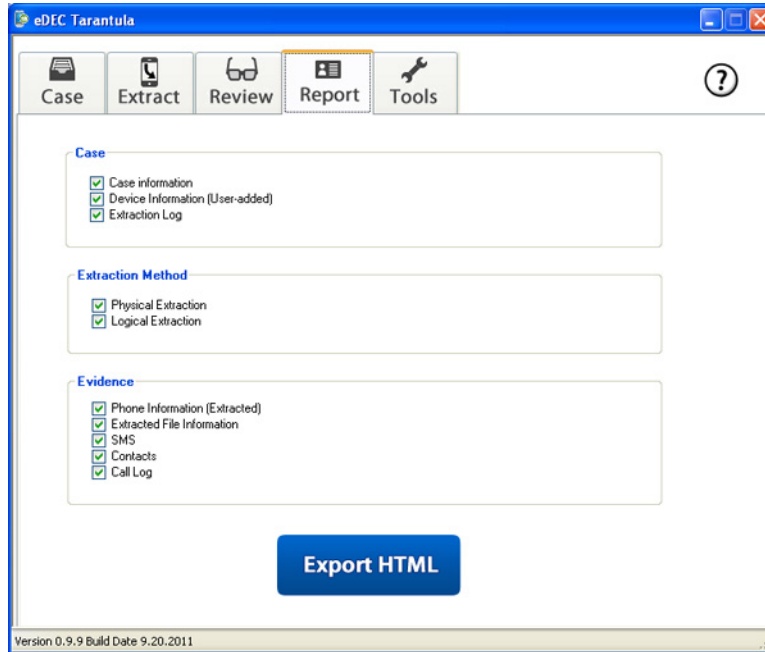
Click the **Review** tab to view and decode extracted information



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

5.4 Report Tab

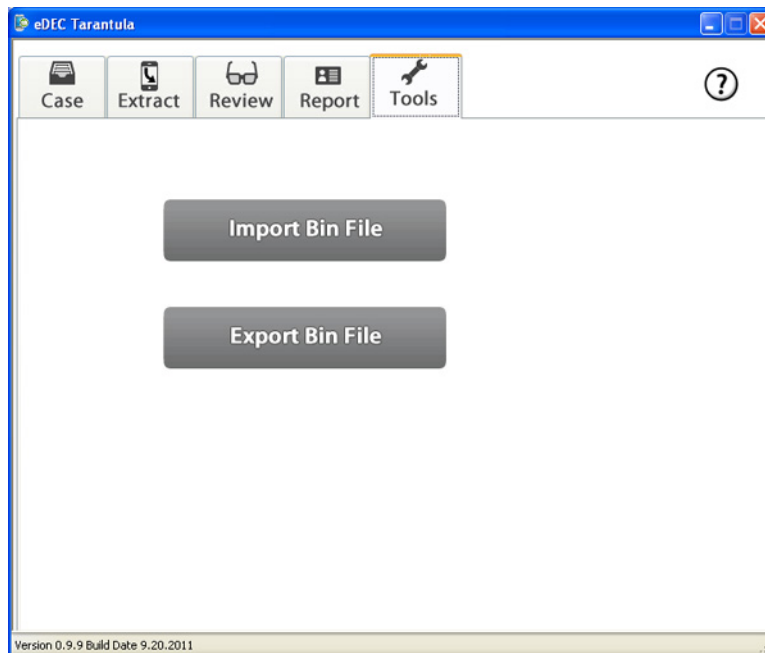
Click the **Report** tab to build a report



- Select which Case or Evidence items to export to a report
- Report assets 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.

5.5 Tools Tab

Click **Tools** tab for additional actions



- .bin files may be imported for decoding by clicking the **Import Bin File** button

- Please note the importing an external .bin file will overwrite any previously extracted .bin file. Create a new case to avoid overwriting data.
 - To properly decode an imported .bin file, select the correct chip type under the Case Info window. If the chip type is unknown, multiple types must be selected and tried by clicking **Decode** under the Review tab
- Previously extracted .bin files may be exported by clicking the **Export Bin File** button and choosing a location to save the file.

6. Warranty

6.1 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. Some states do not allow a limitation of damages so the foregoing limitation may not apply to you. This warranty gives you specific legal rights and you may also have other rights, which vary from state to state.

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.