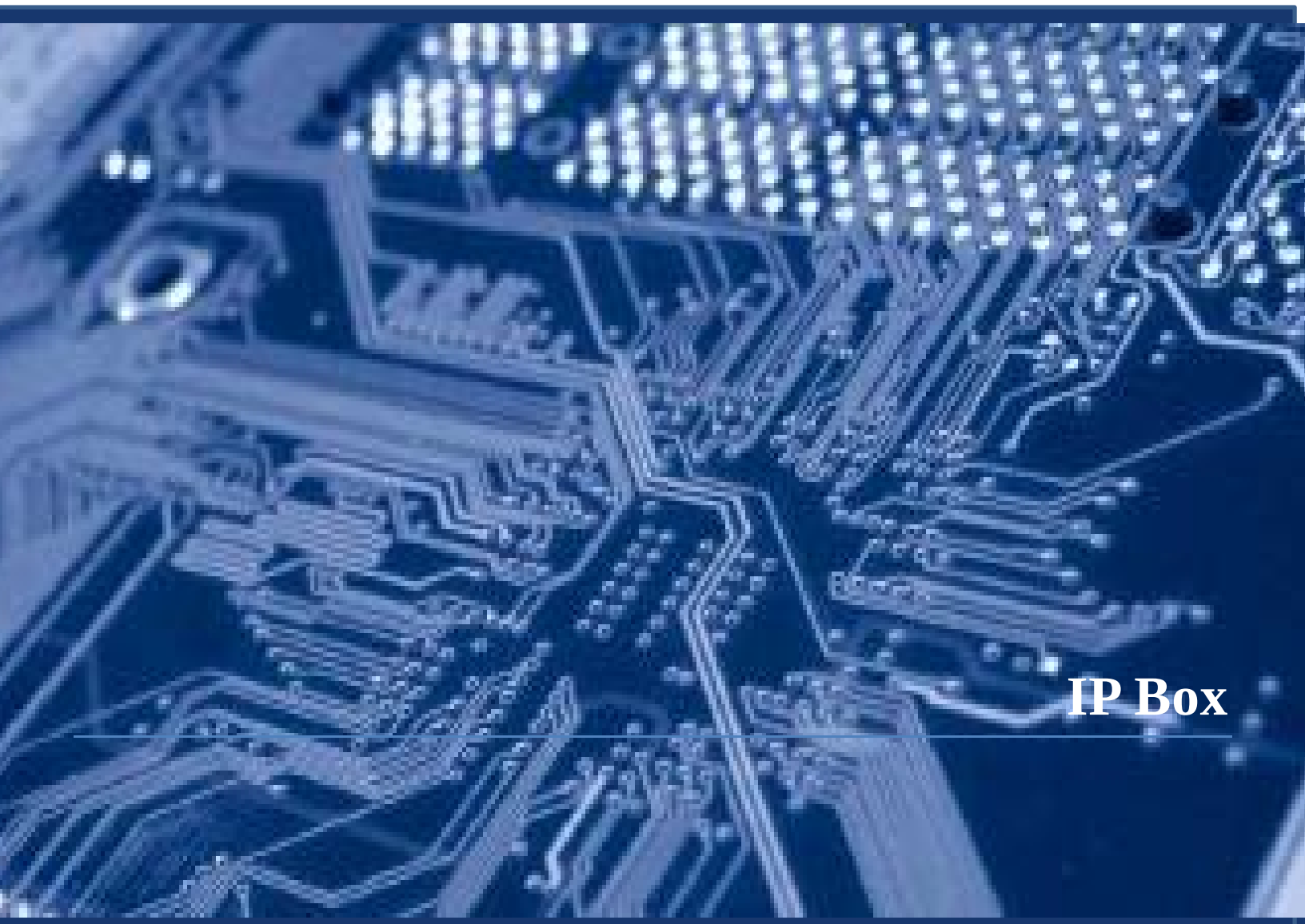
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation



IP Box

175 Lakeside Ave, Room 300A
Phone: (802)865-5744
Fax: (802)865-6446

http://www.lcdi.champlain.edu

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction:

When it comes to mobile device security, the first line of defense is usually a 4 digit passcode. The standard 4 digit passcode is a great way to protect unauthorized users from getting into personal devices. However, recent technologies have emerged that ultimately makes these passcodes obsolete. The tool that specifically does this is the IP Box. The IP Box is a comprehensive tool that brute forces iOS devices' 4 digit passcodes. This device can act either as a standalone tool or be used with a computer running manufacturer specific software. Using this tool allows the user to brute force 4 digit passcodes for devices using iOS 5 – iOS 8.1.2.

IP Box Equipment:

- IP Box
- iPhone 5 Cable
- iPhone 4 Cable
- Micro USB Cable
- Light Sensor

* If a light sensor is being used, IP Box needs to be manually reset after the first 5 attempts when the disable screen is displayed. This is done by holding the black button until there is a beeping, and then again pressing the black button to begin the attack once more. It is also important to note that if not using a light sensor, IP Box will not stop attempting to crack passcodes even if successful. In that scenario, if the user is not watching every pin input, they will not know which one was successful.

Setup:

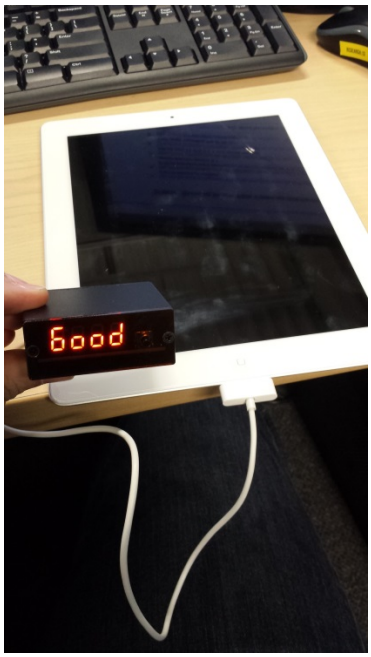
IP Box Software:

In order to obtain the latest IP Box software (V8.2) please visit:

http://www.gsm112.net/ip-box_main/eng.html

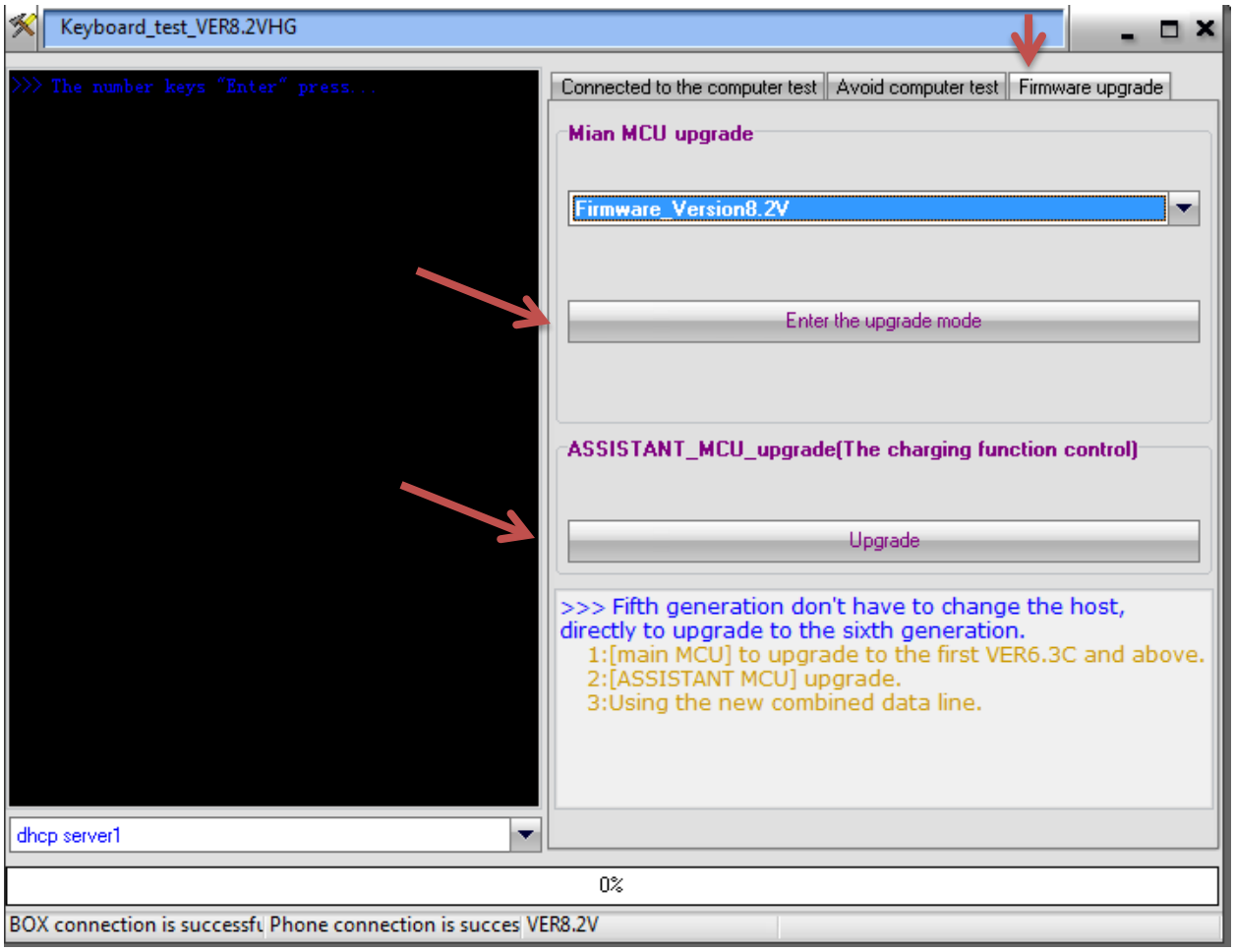
After the software is installed, navigate to the folder that was just downloaded and run Key_e.exe. After Key_e.exe is booted, follow these steps:

1. Connect the device cable to IP Box, this will be either the iPhone 5 cable, or the iPhone 4 cable (IP Box display will read “Good”)

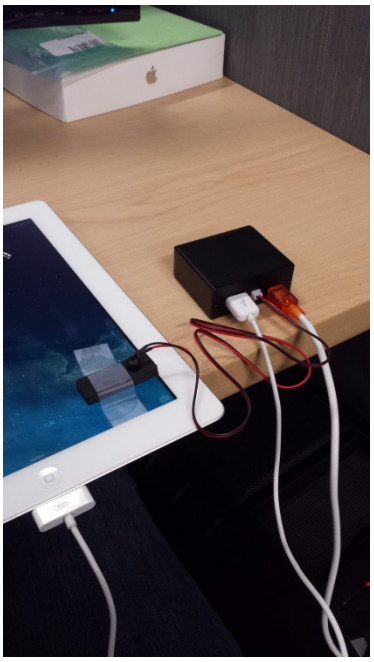


2. Next connect the Micro USB cable to IP Box and to the computer, IP Box display will read “USb” and key_e will display BOX connection successful in bottom left

3. Go to the “Firmware upgrade” tab and ensure the latest firmware is installed on the device by selected “Enter the upgrade mode”
4. Next under the “Assistant_MCU_upgrade” make sure that the charging function control is also upgraded by selected “Upgrade”

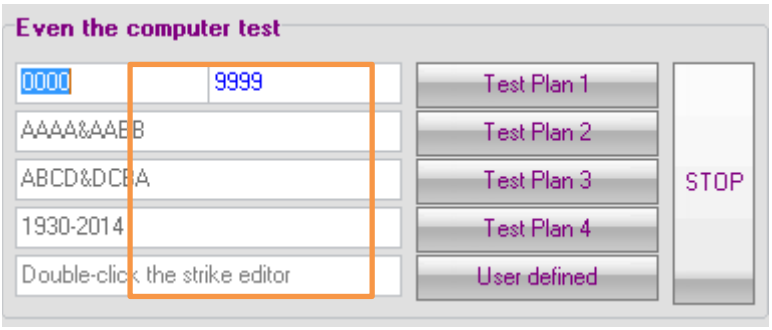


5. Lastly connect Light Sensor to IP Box and secure it to the device(This can be done by using either tape, or a rubber band)



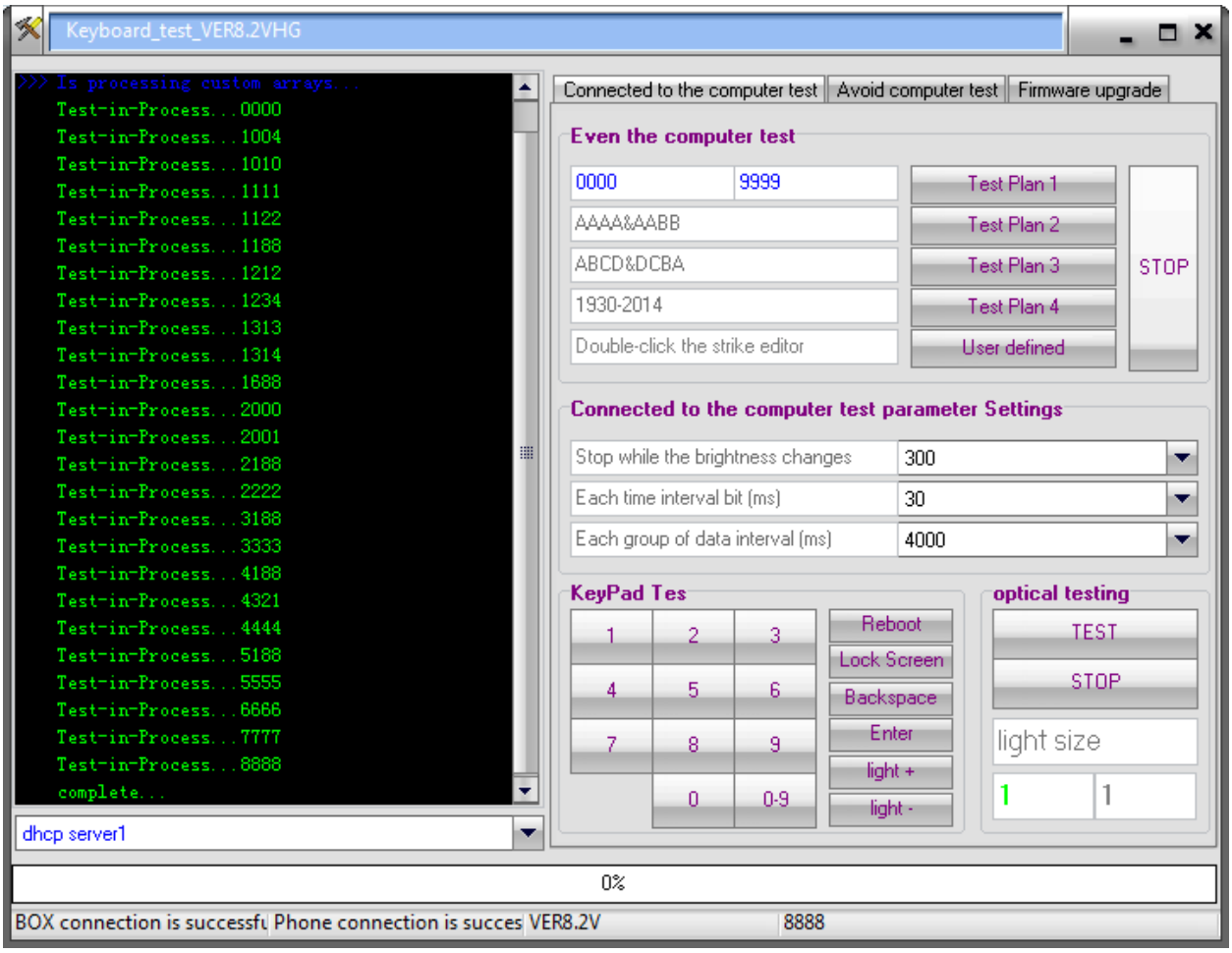
Attack Methods:

After IP Box is set up and connected to the target device, attacking can begin by selecting one of the 5 attack methods:



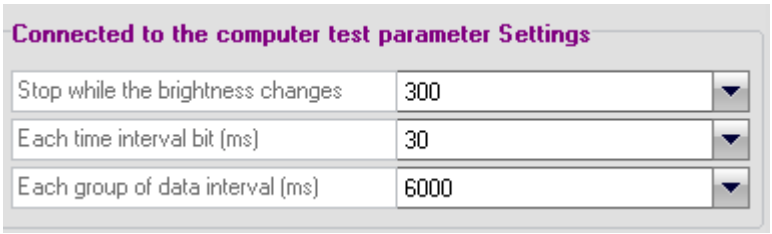
At this point the user may begin to interact with IP Box through the computer. This software will allow the user access to multiple functionalities of IP Box. There are 5 different attack methods implemented to crack iOS devices 4 digit passcodes. These consist of

- Test Plan 1
  - Simple brute force attack from 0000 to 9999
  - Beginning and Ending digits can be altered to any combination
- Test Plan 2
  - Paired number attack
  - Example: 0000, 0011, 0022
- Test Plan 3
  - Sequential attack
  - Example: 0123, 1234 …. 9876
- Test Plan 4
  - Birth year
  - Beginning with 1930 – 2014
- User Defined
  - Browse to your custom list of 4 digit passcodes
  - Will input codes in lowest to highest numeric order



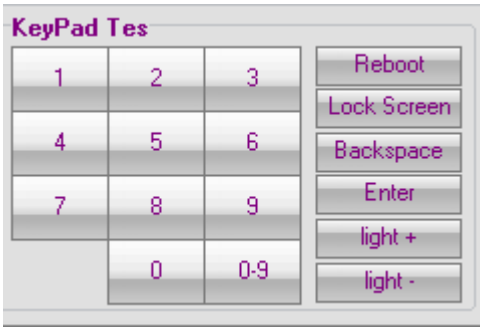
Shown above, Key_e.exe will keep a running record of all codes input for one test

Test Parameter Settings Interface:



- Brightness change
  - Changes the sensitivity of the light sensor
- Time Interval
  - 30 is the standard setting
- Data input Interval (milliseconds)
  - The recommended settings for iOS devices is 6000ms (6 seconds per passcode attempt) Running a number lower than the recommended 6000 may result in skipped passcode attempts.

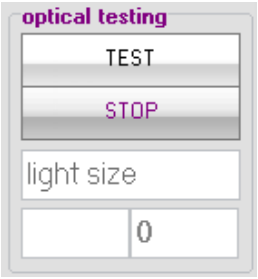
KeyPad Tes:



User can manually manipulate the device pin pad along with

- Reboot
  - Reboots IP Box
- Lock Screen
- Backspace
- Enter
- Brightness settings up or down

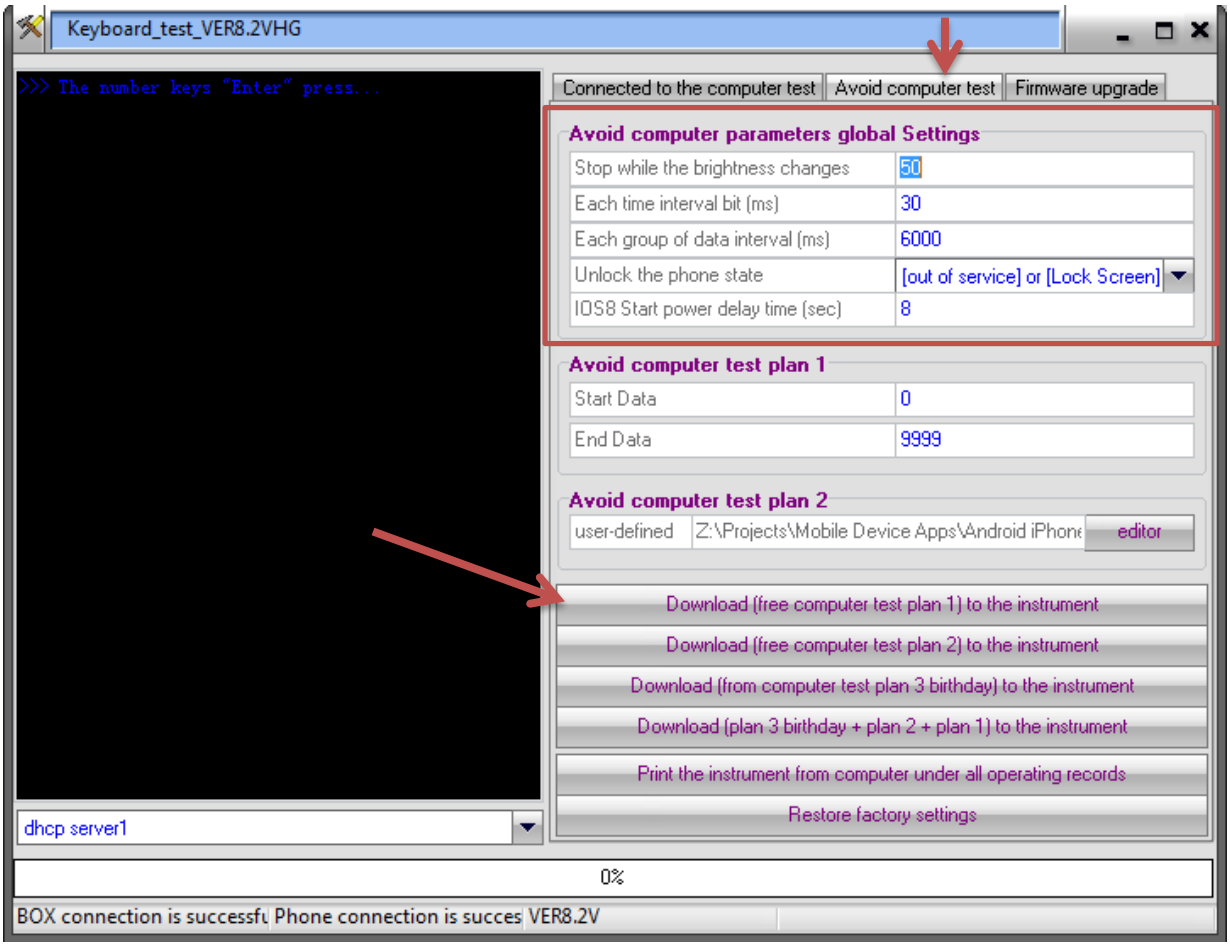
Optical Testing:



- Users can change the settings for the level of brightness change required to stop test

Stand Alone Mode:

To download attack methods to the IP Box, go to the “Avoid computer test” tab of Key_e.exe and select which method you would like to download.



Parameter Settings:

- Stop while the brightness changes
  - Set level of brightness change for light sensor
- Time interval bit (ms)
  - 30 recommended setting
- Data interval (ms)
  - 6,000 recommended setting
- Unlock phone state
  - Select valid option
- IOS8 Start power delay time
  - Only for when using IP Box iOS8 Adapter

Test Plan 1 Setup:

- Select the start and end numbers for the attack

Test Plan 2 Setup:

- Browse to custom user pin sequences

Download Section:

- Download Test plan 1 to the instrument
  - IP Box will run selected settings for test plan 1 in numerical order (XXXX – XXXX)
- Download Test Plan 2 to the instrument
  - IP Box will download selected file regarding custom user pin sequences
- Download Test Plan 3 to the instrument
  - IP Box will download selected settings from the above Test plans 1 & 2 along with a birthday attack
- Print the Instrument from computer
  - Will print all the currently installed test plans from IP Box
- Restore Factory Settings
  - 0000 – 9999

Once the desired attack method is downloaded to the box, unplug the box from the computer and connect the device cable to IP Box, displaying code "Good". Then connect the light sensor to IP Box and secure it to the screen of the device. Lastly, press the black button on IP Box and let it begin to go through passcodes.

When the IP Box successfully cracks a passcode, the light sensor will detect the difference in light and the IP Box will stop running and have a flashing display of the passcode that was used. Along with this, the user should hear a beeping sound coming from the box.

How IP Box works with different iOS versions:

iOS 5 Devices:

To crack iOS 5 passcodes, just connect the IP Box to the device and secure the light sensor. Once everything is set up press the black button on IP Box and let it begin cracking.

iOS 6 Devices:

To crack iOS 6 passcodes, connect the IP Box to the device and secure the light sensor. iOS 6 will lock the user out after five unsuccessful attempts. In order to prevent this lock out follow these steps:

1. Access the Emergency call screen
2. Dial 112 (Warning, this will call the local police if allowed to connect)
3. Press the home key
4. Press and slide up from the bottom of screen and open the calculator
5. A green stripe will appear on top of the screen, which will say "***the line is busy now***"
6. Press the green stripe to get back to the call screen
7. Simultaneously press the home button and address book icon
8. The phone should now be able to keep cracking passcodes without being disabled

iOS 7 Devices:

To crack iOS 7 passcodes, just connect the IP Box to the device and secure the light sensor. Once everything is set up press the black button on IP Box and let it begin cracking.

iOS 8-8.1 Devices:

To crack iOS 8-8.1 passcodes, just connect the IP Box to the device and secure the light sensor. Once everything is set up press the black button on IP Box and let it begin cracking.

iOS 8.1.1 – 8.1.3 Devices:

There is currently no known way to disable the lock out feature after five unsuccessful passcode attempts within iOS 8.1.1- iOS 8.1.3. However there is an aftermarket adapter available, this adapter will automatically restart the phone after five unsuccessful attempts, and once rebooted the IP Box will continue to enter codes where it left off. This solution will be time consuming because after the restart, the IP Box will only be able to enter one additional code before it has to restart again.

Conclusion:

We tested the IP Box with an iPad running 7.1.1 and it worked perfectly. We are still very interested in using the IP Box with newer versions of iOS 8, so in order to do this we have ordered the adapter to allow us to continue to do research on this tool.