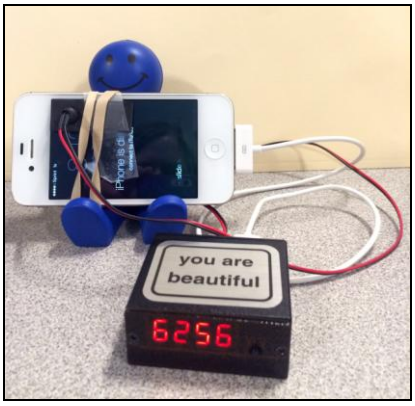
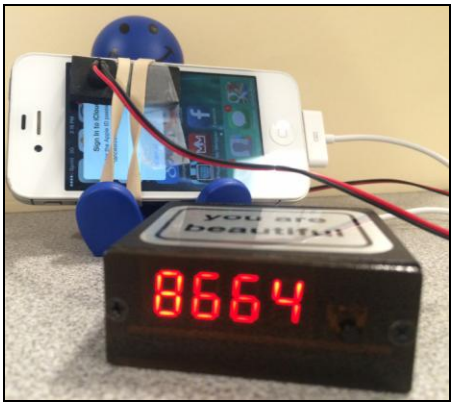
There is a new 'black box' that originates from phone unlocking, hacking and repair market called the iP-BOX, which can be used to defeat simple 4 digit pass codes on any iOS device, including all versions of iOS1 through iOS8. For certain devices running iOS6, there is a process that must be followed in order to set the device into "Infinite Unlock Condition" in order to run the iP-BOX, but other versions of iOS require no further exploit. Directions for placing an iOS 6 device into "Infinite Unlock Condition" can be found at the end of this document. There is minimal documentation available for the device, and much of the available documentation is in Chinese.

This document is intended to assist forensic examiners in learning basic operation of the device, as well as to provide information about how the device operates. It is not intended to endorse use of the device, as that decision will be made based upon your own agencies policies and procedures, as well as legal authority to break pass codes on a case by case basis. It is also not intended as a comprehensive description of testing of the device – the software is updated frequently, and resulting changes in the operation of the device and software may mean that future versions deviate somewhat from what is described here. Additionally, some testing has been done regarding what communications occur when the device is attached to the software via a computer with an internet connection. This testing has only been done with version 6.3 of the software at this point, and so users in Law Enforcement positions or in situations involving sensitive information should test the current version of the software/device prior to its use, and should be sure their use of the device is in accordance with their agencies policies, procedures, and with their legal authority in each specific case.

iP-BOX Components and Overview: The iP-Box kit consists of the box itself, iPhone cables, a USB cable, an optical sensor, and the associated iP-BOX software. The device can be operated either in a standalone fashion after firmware updates and password attacks (referred to as "tests" in the iP-BOX software and documentation) are set up via the software, or it can be connected to a computer during operation.

The iP-BOX operates by sending pre-defined pass code lists to the targeted iOS device. Each attempt takes approximately 6 seconds to perform, and so the dictionary containing all numbers between 0000 and 9999 would take between 6 seconds and approximately 17 hours to complete. Custom dictionaries can cut down on the amount of total time used to attack the pass code, and may be utilized before a full attack if desired. The images below show the box set up to operate in stand-alone mode on a pass code protected iPhone 4S. The optical sensor has been attached to the screen, and the appropriate iPhone cable has been connected to the phone. In the image on the left the test is in progress, and in the image on the right, the test has completed successfully, and the password has been broken and was found to be 8664.





Battery/Power Tips: As stated earlier, using an attack that includes all numbers between 0000 and 9999 can take up to 17 hours, and obviously the iOS device's battery may not last that long. In the image

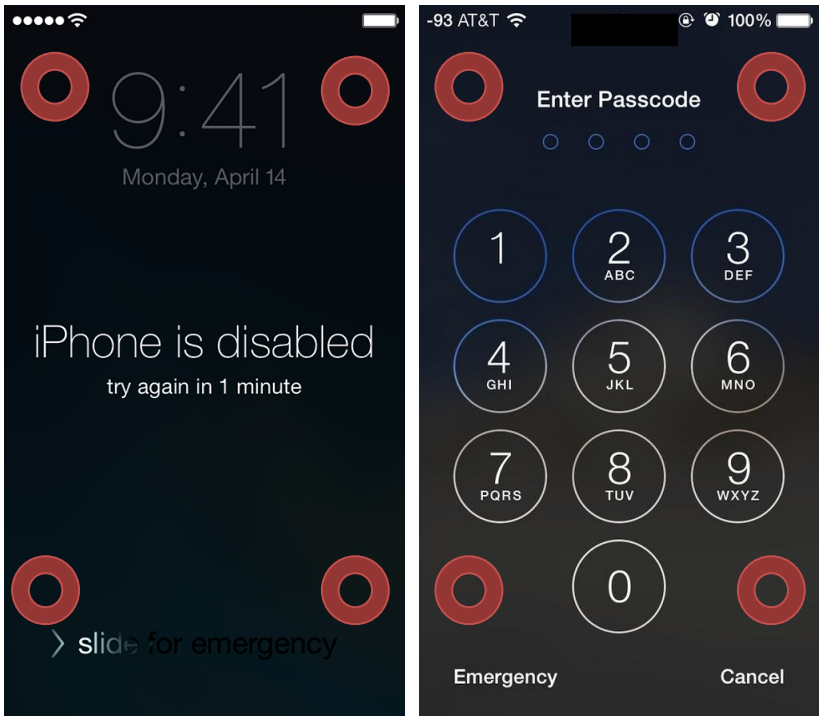
Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824

above, the box is powered by the device battery. To prevent the battery from dying, the USB cable from the kit can be plugged in to a standard powered USB wall outlet adapter, and power will be passed through the device to the phone. If an outlet is unavailable and the battery of the iPhone goes dead, simply recharge the phone, reconnect it to the box, and press the button on the front of the box twice to restart the attack at the last used sequential number.

Optical Sensor: The optical sensor is the tool's trigger to signal success. When the correct code is sent to the phone, the phone's screen changes from the lock or phone disabled screen to the user's background screen, and as a result the background light output changes. The box signals success by beeping and flashing. If the optical sensor is placed in the wrong place (anywhere there are light changes on the screen of the device) or the screen is touched and changed by the user during the attack process, the box may stop and provide a false success signal.

If the user's unlocked home screen is very similar in color to the lock screen, the device may be successful in cracking the pass code but the optical sensor may not detect enough light change to trigger the success notification. If you allow the device to operate unattended or overnight, and find that the phone has changed from the "Phone is disabled – Connect to iTunes" screen to the "Enter Passcode" screen, this is likely the reason. The iP-BOX broke the password at some point but the phone's screen timed out and the device re-locked after inactivity. The sensitivity of the optical sensor can be adjusted using the iP-Box software to account for this issue, or you may need to remain present during the operation of the device to observe when the pass code is broken.

For best results, try placing the optical sensor in the areas indicated on the image below by red circles. It is helpful to use rubber bands or tape to secure the optical sensor to the screen of the device.

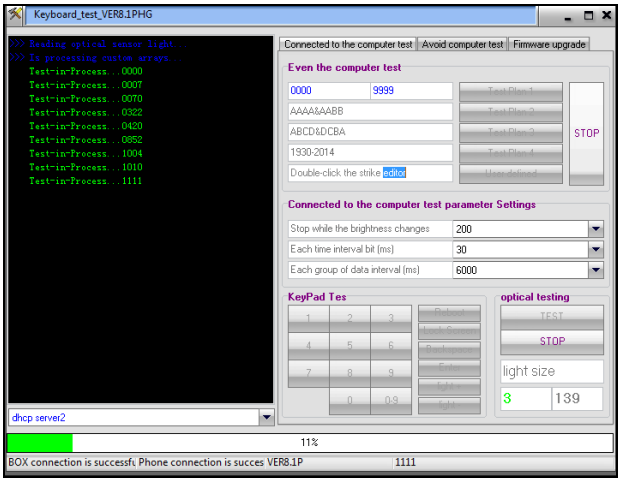


False Positives: In the event that the tool beeps to signal success but the pass code is not broken, the password attempt can be restarted. To restart the attack, simply press the button on the front of the box twice, which will restart the attack at the next sequential number.

Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824

iP-Box Software: The iP-BOX software is used to configure pass code test patterns, to run those test patterns against a target iOS device, to adjust settings for the test, and to perform firmware upgrades to the iP-Box. An overview of the software begins on page 4 of this document.
The user can choose from several free test patterns such as a birthday attack (which contains patterns that match MMYY), or all numbers between 0000 and 9999. The user can also create a custom number based dictionary attack. Each attempt takes approximately 6 seconds to perform, and so the dictionary containing all numbers between 0000 and 9999 would take between 6 seconds and approximately 17 hours to complete, while a custom dictionary containing 100 most commonly used pass codes would take around 10 minutes to complete. Custom dictionaries can cut down significantly on the amount of total time used to attack the pass code, and may be utilized before a full attack if desired. Contact the author of this document directly at cmurphy@cityofmadison.com if you are interested in a custom pass code list of 100 commonly used pass codes.

The iP-BOX software is then used to interface with the box and load the chosen test patterns for an offline attack of the device, or alternatively, the attack can be run directly using the software, through the box, to the phone or iPad. The screen shot below shows an attack in process using the software through the box to the device. A custom pass code list is being used in that example.



Unsuccessful Attacks: If the attack is allowed to run completely and fails, try slowing down the interval between attacks and restarting the attack. Also, if you used the software through the device for the original attack, try re-running the attack with the box only, or visa-versa. Remember, any changes you make in the settings for the test in the software must be sent to the box to be applied.

"Infinite Unlock Condition" for iOS6 devices:
To access the Infinite Unlock Condition, follow these steps:

1. Access the Emergency Dialing interface and dial 112
2. Press home key to get back to interface "slide to unlock"
3. Press the bottom of keyboard
4. Slide the screen up to get to the calculator
5. Then there appear a green stripe on top of the screen, which will show "***the line is busy now***"
6. Press the green stripe to get back to the calling interface. In the middle of the screen there is the address book / contacts icon
7. Press the home key and address book simultaneously to access to infinite unlocked situation
8. Connect IP-BOX to the phone and move the Sensor to the screen, press the black key of the equipment to unlock

Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824

** Note that the "Infinite Unlock Condition" requires that the phone is not in Airplane mode, and that a call to the 911 Emergency center might be completed, as dialing 112 in the US can be forwarded to the 911 system. Obviously, this is not ideal as you will be adding to the call history on the phone, are connected to the mobile network, and are interacting with the phone directly. This is a deviation from a normal forensic process, but in the event that it is the only option such deviation may be necessary in order to defeat the device lock. ***If you need to perform the above steps, be sure to document your actions carefully!***

Potential for Target Device Wipe: While there are reports that the device might wipe a device that has been set by the user to wipe after 10 unsuccessful attempts, testing by the author has not resulted in that outcome. Additionally, Apple security announcements seem to confirm that it is possible to attack some un-patched iOS devices beyond the user set limit by use of hardware devices (see links at the end of this paper for further information).

Software overview: The iP-BOX software has three main tabs including "Connected to the computer test", "Avoid computer test" and "Firmware upgrade."

The "Connected to the computer test" tab contains interfaces for configuring password attacks and interacting with the iP-BOX and phone.

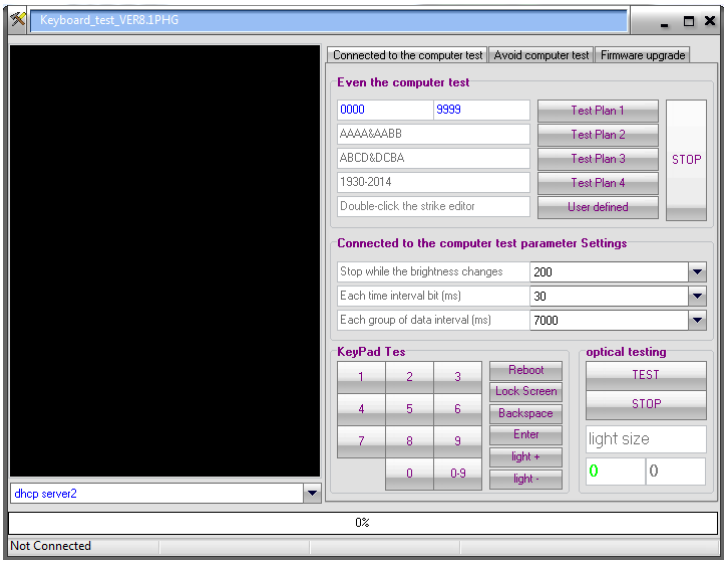
The "Avoid computer test" tab contains interfaces for configuring password attacks to be sent to the iP-Box. Note that after configuration, both the box and a phone must be connected in order to send the configured test/attack plan to the box, as the box draws its power source from the phone's battery.

The "Firmware upgrade" tab contains the interface for updating the firmware on the box. Again, both the box and a phone must be connected in order to upgrade the firmware on the box because the box uses the phone as a power source.

If you are using the iP-BOX in a digital forensics lab setting, is strongly suggested that a test phone/non-evidentiary device while updating the firmware or the box itself to avoid exposing your evidentiary device to the Internet and untested versions of firmware for the device. An overview of each of the three main tabs including "Connected to the computer test", "Avoid computer test" and "Firmware upgrade" follows.

Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824

"Connected to the computer test" Tab: This tab contains interfaces for configuring password attacks and interacting with the iP-BOX and phone.



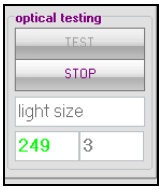
"Even the computer test" options:

- **Test Plan 1** is the full number attack 0000-9999. Note that you can adjust this to start at 9999 and go down to 0000, or you can start at any number and end at any other sequential number.
- **Test Plan 2** will send paired patterns of numbers to the phone (0000,0011,0022 … 7799,8899,9999)
- **Test Plan 3** will send ascending and descending sequential patterns of numbers to the phone (0123,1234,2345…, 9876,8765,7654…)
- **Test Plan 4** will send birth year sets to the phone (1930,1931,1932… 2012,2013,2014)
- **User defined test plan** will send your custom list to the phone. Double click in the box labeled "Double-click the strike editor" to open and edit your custom pass code list.
- **Stop:** Ends whatever test is in progress.

"Connected to the computer test parameter Settings" options:

- **Stop while the brightness changes –** the dropdown box presents values between 10 and 300. Use these options to change the sensitivity of the optical sensor up or down.
- **Each time interval bit (ms) –** Interval options between 1 and 90 are presented. The default is 30 and seems to work.
- **Each group of data interval (ms) –** interval options between 100 and 20,000 are presented. Changes to this option speed up or slow down the rate at which pass code attempts are presented to the device. While you can choose to speed up the attack, the phone itself cannot accept attempts at a rate higher than 1 per 6 seconds. The targeted phone will vibrate each time a pass code attempt is sent to it. If you find that there isn't a vibration for each code passed to the phone, increase this interval to slow the attack.

"optical testing"
Use this area to test the approximate light change between the phone's dark screen and lock screen in order to estimate the level to use for "Stop while brightness changes" option.
A screen shot of a test in progress is shown below:



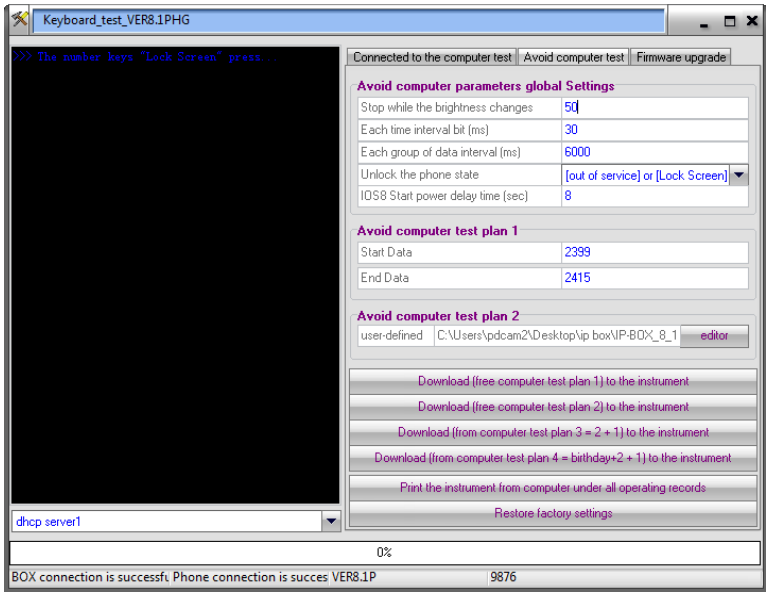
"Keypad Tes"

- **Reboot –** Reboots the iP-Box.
- **Lock Screen** - Presents the lock screen on the phone attached to the iP-Box.
- **Keypad –** Can be used to enter pass codes directly to the device manually. Hit **Enter** after keying in the 4 digit attempt to send it to the phone.
- **Light + / Light-** can be used to directly increase or decrease the brightness of the screen of the phone attached to the iP-Box. This can be used to adjust the screen brightness in conjunction with the optical testing box to its right to determine what the brightness change level should be set to.

- The dhcp server dropdown will allow the user to choose from 4 different servers in order to download firmware updates and free test plans.
- The progress bar displays the progress of test pattern being run. Codes that have been attempted will show in the black box, and the current code being tried will display below the progress bar.

Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824

"Avoid computer test" Tab: This tab contains interfaces for configuring password attacks to be sent to the iP-Box.



Avoid computer test plan 1 – by default is set to start at 0000 and end at 9999. Any options can be entered here, including custom ranges as shown above. So you could start at 9999 and end at 0000, or use any range of numbers you wish.

Avoid computer test plan 2 – is a user defined pass code list. This is the same user defined list as used in the "Connected to the computer test" tab and can easily be edited in a text editor. The file being edited is named "user_tab.inf."

Download buttons:
The download buttons are used to send the chosen test plans to the iP-Box device.

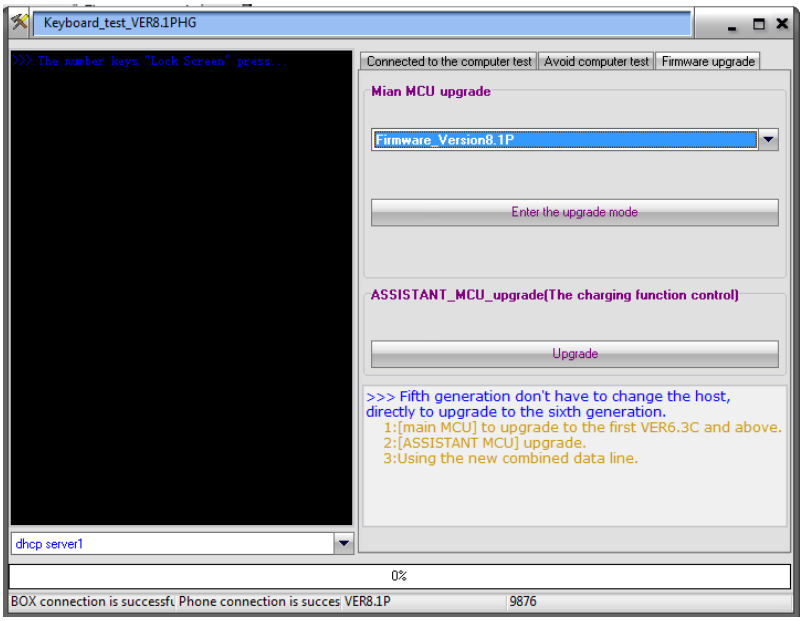
- **Download (free computer test plan 1) to the instrument** will send test plan 1 (0000-9999, or whatever you have defined) to the box.
- **Download (free computer test plan 2) to the instrument** will send the user-defined custom pass code list to the box.
- **Download (from computer test plan 3=2+1) to the instrument** will send test plan 1 and test plan 2 to the box.
- **Download (from the computer test plan 4=birthday+2+1) to the instrument** will send test plans 1 and 2 plus a birthday attack (DDMM then MMDD) to the box.
- **Print the instrument from computer under all operating records** will print to the computer screen the currently installed test plan from the box.
- **Restore factory settings –** Restores the iP-Box to factory default settings.

Avoid computer parameters global Settings:

- **Stop while the brightness changes**
  This box will be automatically populated if a phone is attached, and can be changed to adjust the sensitivity of the optical sensor.
- **Each time interval bit (ms)**
  This box will be automatically populated if a phone is attached, and can be changed to alter the speed of the attack. Default of 30 seems to work well.
- **Each group of data interval (ms)**
  This box will be automatically populated if a phone is attached, and can be changed to alter the speed of the attack. Default of 6000 seems to work well. If you decrease this too much, the phone can't accept pass codes as fast as they are being sent and the attack will likely fail with skipped attempts.
- **Unlock the phone state**
  A dropdown list with these options:
  1. [Out of Service] or [Lock Screen]
  2. [Password] or [Dialing]
  3. [IOS8 only_1]
  4. [IOS8 only_2]
  5. [IOS8 only_3]
  6. [IOS8 only_4]
- **IOS8 Start power delay time (sec)**
  This box will be automatically populated if a phone is attached, and can be changed to alter the delay of the attack by a chosen number of seconds.

Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824

"Firmware upgrade" tab: The "Firmware upgrade" tab contains the interface for updating the firmware on the iP-BOX.



"Mian MCU upgrade"
The dropdown box will indicate the version of the firmware upgrade. When the device is connected, you will be prompted to upgrade the firmware if necessary. Firmware upgrades seem to be quite frequent.

"The Enter the upgrade mode" button prepares the box for upgrade. It may take 20 seconds or so to enter upgrade mode.

Once the software prompts you that it is ready, the **"Upgrade"** button sends the firmware update to the box, and alerts you if the update was successful.

Notes on Testing and Documentation: Because the iP-BOX is so new to the forensic community and the software and hardware originates from China, documentation about its operation is very limited. Testing is ongoing, both related to the software and hardware. The software may cause antivirus software to alert, and when scanned using Virus Total the software is identified as a potentially unwanted application. Testing using Wireshark and Network Miner shows that the iP-Box software does connect to a Chinese IP for firmware updates. The iP-Box software also connects to a second Chinese site when connected to a phone with a test in progress. However, from testing done so far, it does not appear that any phone related data is passed back from the box and software to the remote site. Testing was done with firmware version 6.3, and has not been repeated at this point for newer versions. If you are interested in .pcap files or other documentation related to the testing process, please contact the author directly.

If you work in an environment where the use of such hardware and software is prohibited, this device may not be an appropriate solution available to you. If you work in an environment where you cannot be connected to the internet during an examination, the box can be used in stand-alone mode after being updated with the software, using a test phone to provide power to the iP-Box during the process.

Helpful resources regarding the device and the exploits that it is using to operate successfully can be found below:

http://lists.apple.com/archives/security-announce/2014/Nov/msg00000.html
http://forum.gsmhosting.com/vbb/f937/ip-box-smart-tool-official-distributer-reseller-list-1873352/
http://www.teeltech.com/mobile-device-forensic-tools/ip-box-iphone-password-unlock-tool/
http://www.datagenetics.com/blog/september32012/

Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824

About the Author:

Cynthia Murphy is a Detective with the City of Madison, Wisconsin Police Department and has been a law enforcement officer since 1985. She is a certified computer forensic examiner and has directly participated in the forensic examination hundreds of digital devices pursuant to criminal investigations of various types of crimes including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and other investigations. She has successfully utilized her skills in the investigation, prosecution, and occasional exoneration in numerous criminal cases involving digital evidence and has testified as an expert in both state and federal court. Det. Murphy earned her MSc. (Hons) from University College, Dublin in Forensic Computing and Cybercrime Investigation, and is a certified instructor and co-author of the SANS 585 Advanced Smartphone Forensics course. She can be reached at cmurphy@cityofmadison.com for questions or comments regarding this document.

Detective Cindy Murphy, MSc.
Madison Police Department
211 S. Carroll St. Madison, WI 53703
608-267-8824