

NowSecure™

JTAG in Mobile Forensics

101 – JTAG Background and Required Tools

© Copyright 2014 NowSecure, Inc. All Rights Reserved.
Personal use only. No modification, redistribution, or commercial use without permission. Do not distribute.

Overview

JTAG in Mobile Forensics contains the following three modules:

101-JTAG Background & Required Tools is designed to familiarize you with the technical side of JTAG and the required equipment so that you can build your shopping list and get started in your own lab. We will also cover the software installation.

102-Connecting to the Device is the next module in the series. You will learn about phone disassembly, soldering and connecting the device to the JTAG hardware. We will be using the RIFF Box for this training and some basic software features will also be explained.

103-Imaging and Pattern/PIN Cracking is the final module. You will learn to get a full dump of the system NAND, locate the lock pattern or PIN, and extract the lock pattern/PIN from the contents of the file.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Overview

Welcome to JTAG 101 - Background and Required Tools!

This is the first of three modules that, when taken together, will greatly improve your lab's ability to successfully bypass a passcode/pattern lock on an Android device.

The goal of JTAG 101 is to familiarize you with the JTAG connection process and go in-depth to recover PIN and pattern lock data from the JTAG image file. We recommend that you take a hands-on training to gain experience with making the solder connections and connecting to JTAG hardware since we can only explain the process here.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Training Outline

1) **JTAG Technical Overview**
   - Why use JTAG?
   - JTAG defined
   - Test Access Port & Boundary Scan
2) Required Tools
   - Building the shopping list
   - Overview of various JTAG equipment
3) Installing the Software
   - Lab 1: Install the RIFF Box, ORT, and Medusa box software & drivers
4) Conclusion

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Introduction

So why are you taking this module? It may be because you have heard about JTAG and want to learn more, but more likely it's because you're getting frustrated with the rapid increase of locked Android devices coming into the lab.

Since many of the phones are pattern or PIN-protected, traditional forensic software solutions cannot extract the data.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Introduction

But what if bootloader or recovery mode aren't options? Investigators are left with only two other options: JTAG or Chip-Off. Chip-Off is an extremely effective solution, but the cost of entry is significant. A rework station like the one pictured can cost thousands of dollars and require unique adaptors for each make/model chip to be examined. However, JTAG is also quite effective and costs a fraction of the price.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

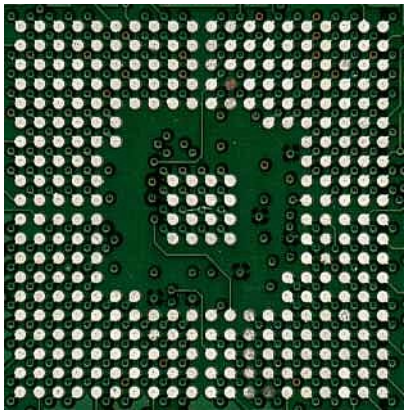
JTAG (Joint Test Action Group) was established in 1990 as a way to standardize boundary scan applications for testing circuit boards. Board manufacturers utilize JTAG to aid in product development and testing, giving them the ability to debug through automation.

This capability allows manufacturers to set and read certain values without direct physical access to the chip, which can be essential in certain applications.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

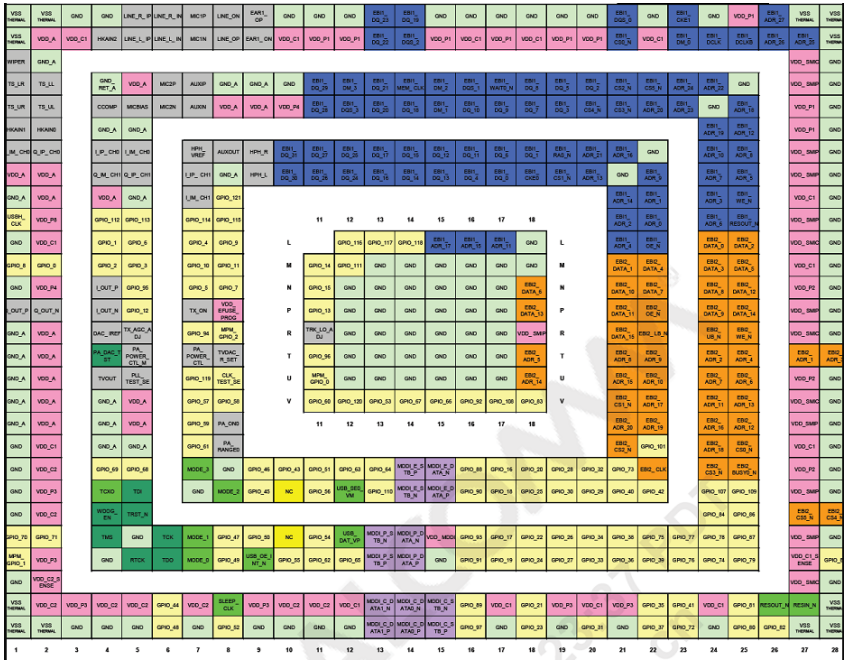
For example, a **BGA** (Ball Grid Array) device has connectors in the form of solder balls at the bottom of the chip. Once this chip is soldered to the circuit board, these connectors are no longer accessible, making the JTAG connection essential for boundary scan testing.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

Each one of the connections on the bottom of the CPU is connected to a lead on the circuit board. The image below is a CPU map of a MSM-7200 Qualcomm chip.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

Though many signals are transmitted through these conductors, only some of them are required for a typical mobile phone JTAG connection. The following connections (pads) are traced from the CPU to external locations on the circuit board:

TCK – “test clock,” synchronizes the internal state machine operations

TMS – “test mode state,” sampled at the rising edge of TCK to determine the next state

TDI – “test data in,” represents the data being shifted into the programming logic

TDO – “test data out,” represents the data being shifted out of the programming logic

TRST (required if present) – “test reset,” used to reset the controllers state

NRST (optional but preferred if present) – “normal reset,” resets the entire device to a known state

RTCK (optional but preferred if present) – “return clock,” allows for a maximum speed connection when connected

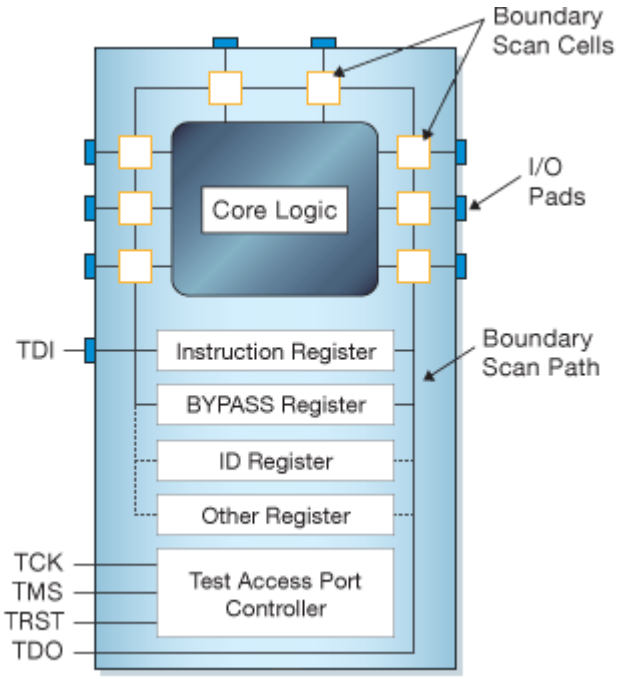
© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

These JTAG pads, collectively known as the **TAP** (Test Access Port), capture the signal between the core logic and a serial scan path. This scan path is called the Boundary Scan Register. The image below gives a depiction of how the paths interrelate:

You can see how the TDO is tied directly to the boundary scan path output and the TDI represents the inbound connection.

TCK and TMS control the processes through the TAP Controller.

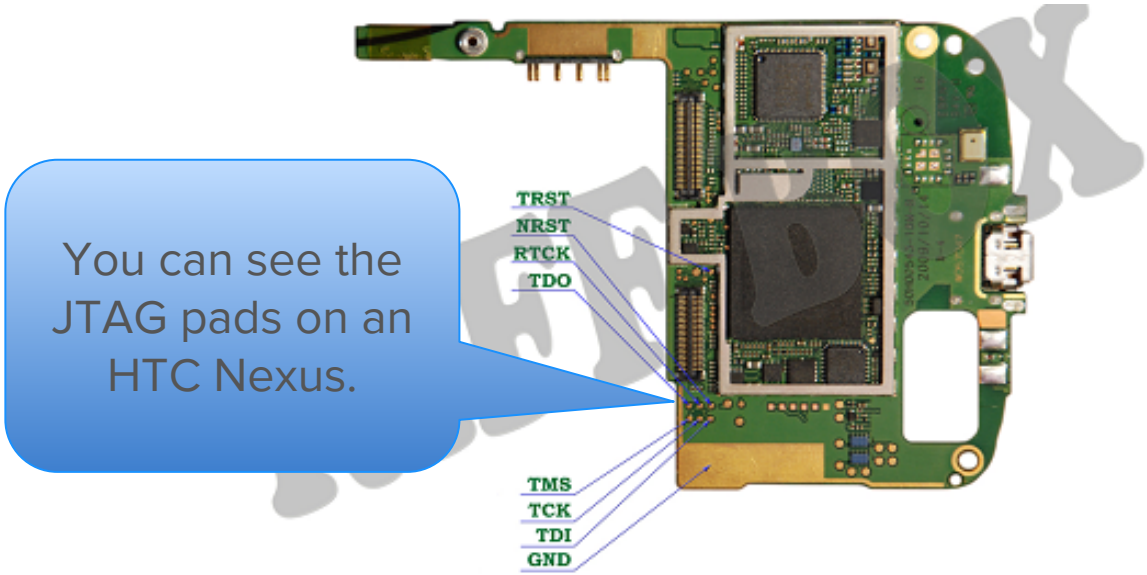


© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

To simplify this concept, the Boundary Scan Register (**BSR**) is what feeds us the data from the core logic.

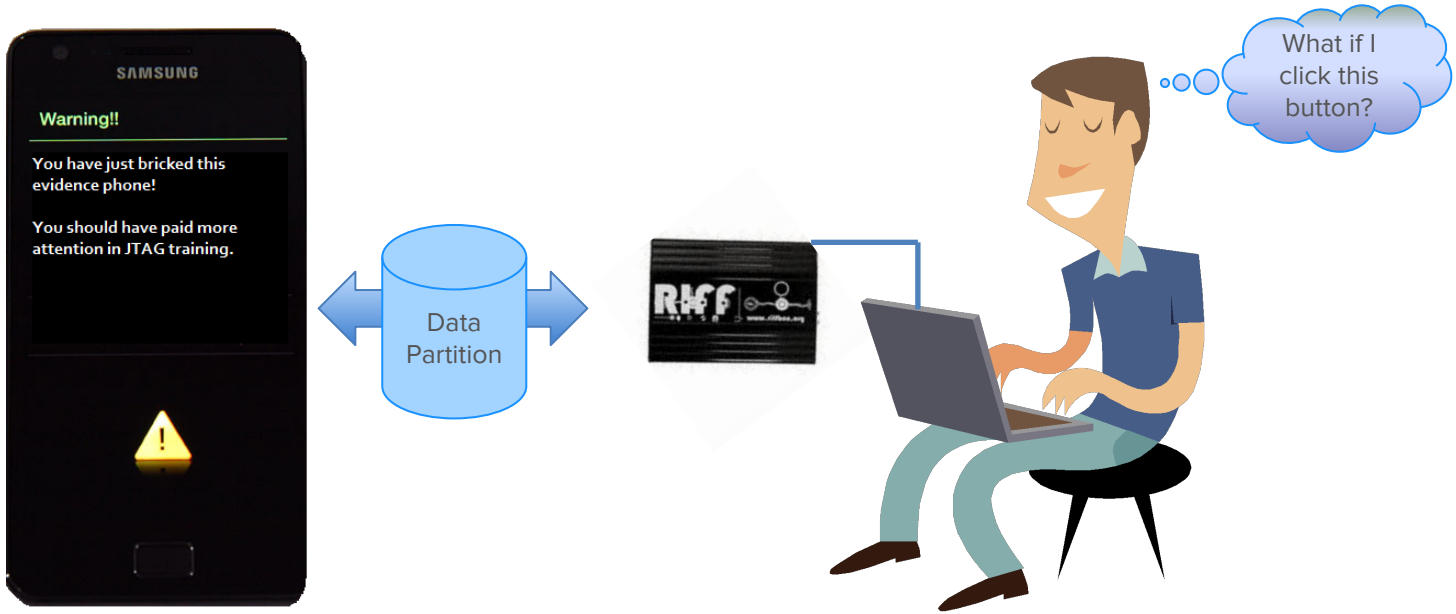
The JTAG software will access the TAP Controller through the TDI JTAG pad (input) and instruct the controller what to do next. The raw data is then output to the TDO JTAG pad directly off of the BSR.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

Keep in mind that JTAG allows for both read and write functions, so you must be careful not to inadvertently send data to the NAND. The RIFF Box software, for example, allows you to flash new partitions in an attempt to repair a boot partition or other damaged area of the NAND. Flashing data can be destructive, so stick to reading data unless you are certain you know what you are doing.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

This entire process is transparent to the investigator as long as the phone circuit board makes a good connection to the JTAG hardware. Once a good connection is made, the JTAG software does all the work through a simple GUI user interface!

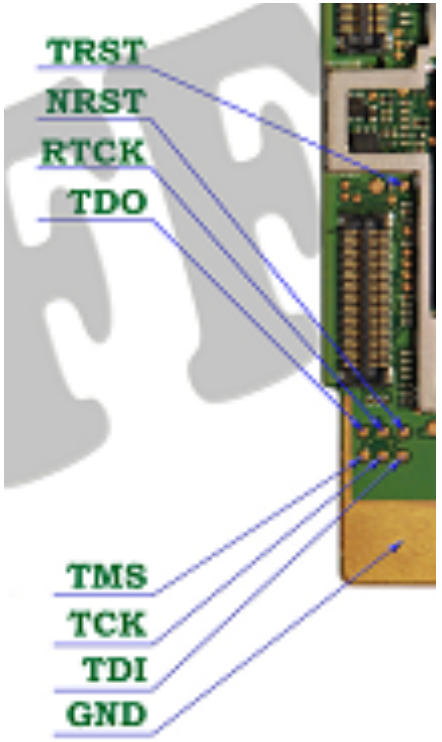
However, a poor solder connection, bad ground, or improper voltage will impede communication between the board and the JTAG hardware, so a good understanding of the underlying principles will help you troubleshoot.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

As you start to understand how a JTAG connection is established, it's important not to take for granted the location of the JTAG pads on the circuit board.

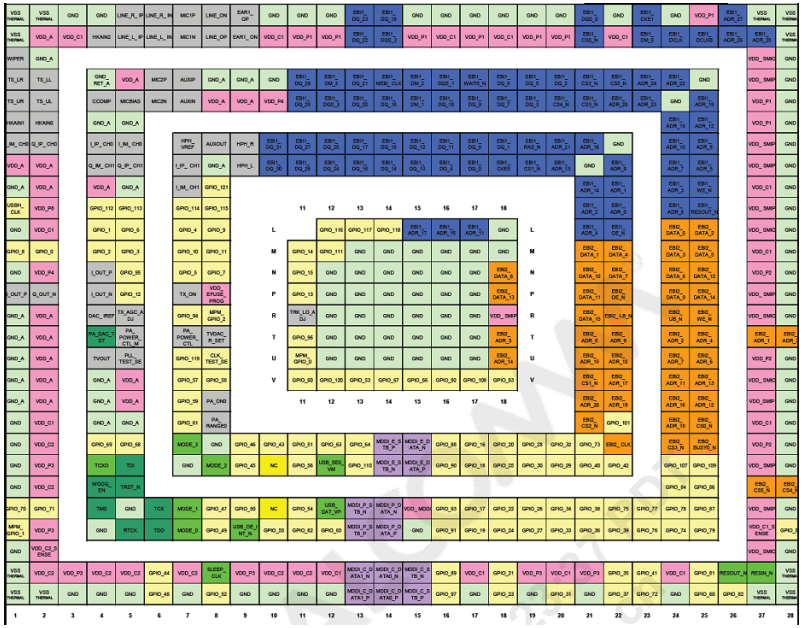
When you open your first phone, you will quickly realize that there are many pads on the printed circuit board that resemble a JTAG pad. Typically, the JTAG hardware manufacturer has already told you where the JTAG connections are located on the circuit board by mapping them out as you can see in the photo to the right.

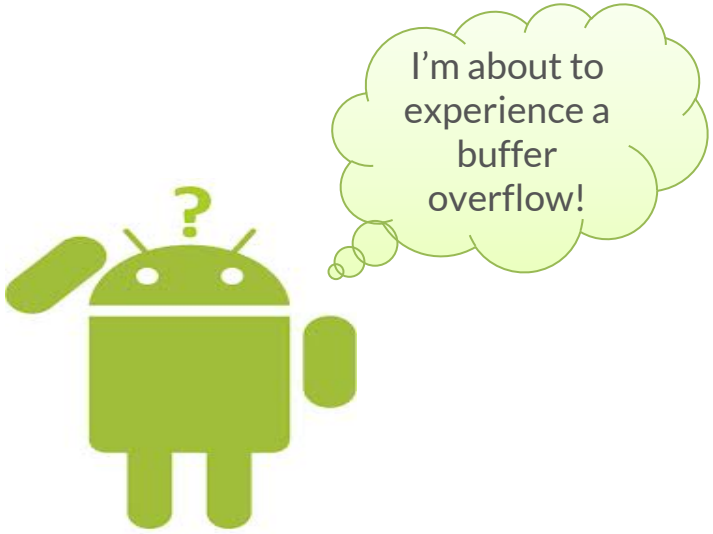


© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

But what if your particular phone is not listed in the RIFF software and the JTAG pinout isn't available? This is where that CPU map you saw earlier comes into play.

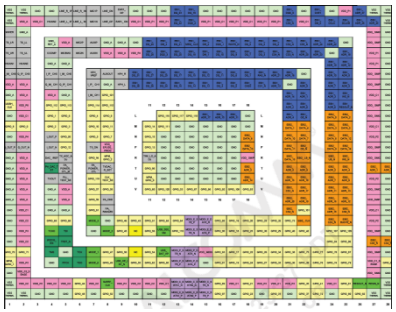


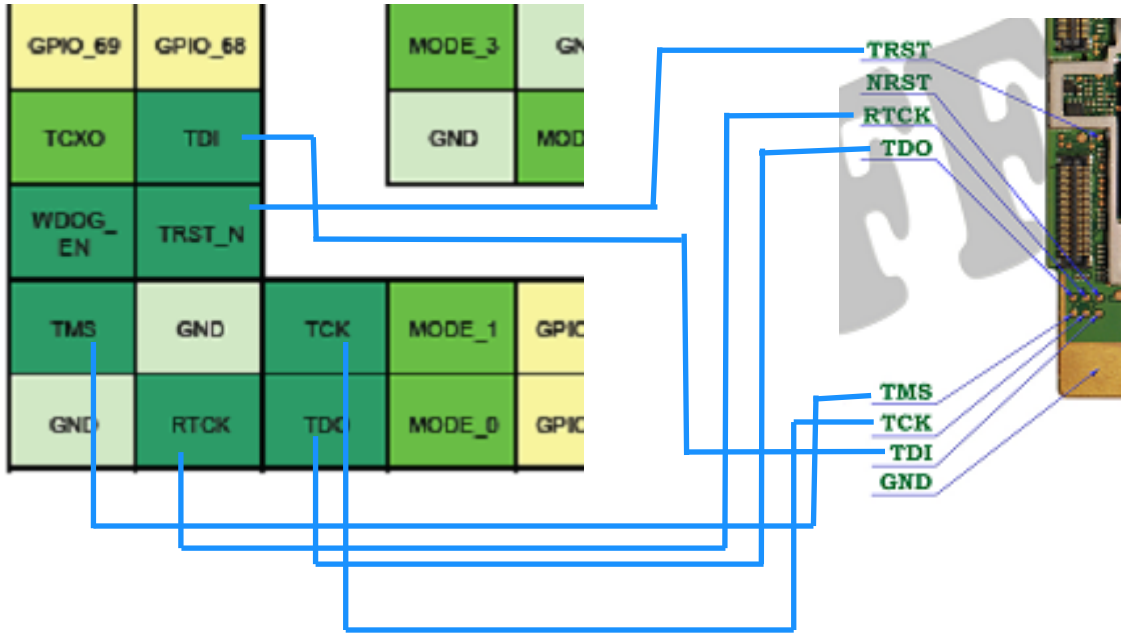


© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

The surest way to determine the unknown pinout is to remove the chip from the board and trace the CPU terminals to the appropriate pad as shown below. There are other methods as well because as you can imagine, this is no simple task.





© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

The likelihood that a typical forensic investigator would have the time or resources to obtain a test device and map out the JTAG pads is very slim. The alternatives are to either try a different JTAG box or to do some research on the internet to see if someone has posted the pinout of the device. Various JTAG hardware box manufacturers support dissimilar devices and often have an online support community.

Finding the JTAG pad locations is more than half the battle. Lucky for us, the software lists many of them! We will cover this more in detail in JTAG 102.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG Background

From a forensic investigation standpoint, our main objective is to gather data from the device without disturbing evidence or destroying the phone during disassembly and soldering. A good set of tools will make the job much easier and increase your odds of success!

The next section will explain all the equipment you will need to JTAG effectively.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Training Outline

1) JTAG Technical Overview
   - Why use JTAG?
   - JTAG defined
   - Test Access Port & Boundary Scan
2) **Required Tools**
   - Building the shopping list
   - Overview of various JTAG equipment
3) Installing the Software
   - Lab 1: Install the RIFF Box, ORT, and Medusa box software & drivers
4) Conclusion

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Required Tools

It is essential to have the right tools in JTAG. The TAP pads on the printed circuit board can be smaller than the tip of a pencil, so soldering can be a challenge without the appropriate iron tip, heat level, and solder.

In this section, we create a shopping list of items required for JTAG so that you can prepare yourself and budget accordingly. The overall cost of the required tools will be less than $1000!

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

Starting with the basics, you need a soldering iron. You can spend hundreds of dollars on a high-quality unit, but in reality, all you need is a simple 30-watt iron from your local electronics store.

Also, be sure to pick up a soldering iron holder as shown below. The sponge comes in handy when cleaning residue from the tip of the iron.

Approximate Cost

$50





© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

Solder is the key to a solid connection to the printed circuit board. A lead-free rosin core solder with a diameter of .02”/.5mm will work best for these small pads. A silver-bearing rosin core solder of 62/36/2 composition is an ideal choice for JTAG since it’s designed for surface mounted joints.

Don’t forget to pick up a solder wick so that you can remove the solder from the board when you are finished.

Approximate Cost

$15





© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

There are several techniques for making the connections to the JTAG pins on the printed circuit board. For ease-of-use and flexibility, we recommend using 30AWG Kynar wire. This wire is a great choice for JTAG connections because it is fine, insulated and solid, as well as easy to strip, solder, and bend.



Approximate Cost

$15

A 50’ roll is a good place to start.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

A desk-mounted illuminated magnifying glass will enhance your view by illuminating the surface of the board while you solder. Many of the connections are so small that soldering them without magnification would be nearly impossible.

Approximate Cost

$65



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

In order to connect through JTAG, you need to send power to the phone board. Often the USB connection powers the board, but for situations that require additional power, you will need an external power supply. You will only need about 6 volts at the maximum, and very few amps. A variable power supply capable of 0-15v DC and 0-3 amps will work perfectly and typically costs less than $100.

Approximate Cost

$100



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

A mobile phone repair kit is essential for disassembly and reassembly. Be sure to get a kit with several small screwdrivers, torx drivers, a side cutter, case tools (for splitting the phone case open), and needle-nose pliers.

Approximate Cost

$35









© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

A multimeter is required to test continuity and voltage levels. A meter capable of outputting a tone for ohm testing is ideal so you don't have to look at the screen when testing connections. Solder can easily run together, creating an unintended connection called a "bridge," when attaching the Kynar to the JTAG pad. This meter will come in handy to ensure the pads are not bridged.

Approximate Cost

$40



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

If you use Kynar wire to connect to the phone's circuit board, you will need jumper leads to connect to the JTAG hardware. The jumper leads are usually around 15" long and also come in handy for jumping power, among other tasks. The mini clips shown in the photo below are great, but also add some jumpers to your collection that have alligator clips on the end. Purchase about a dozen of these to be sure you have extras!

Approximate Total Cost

$45



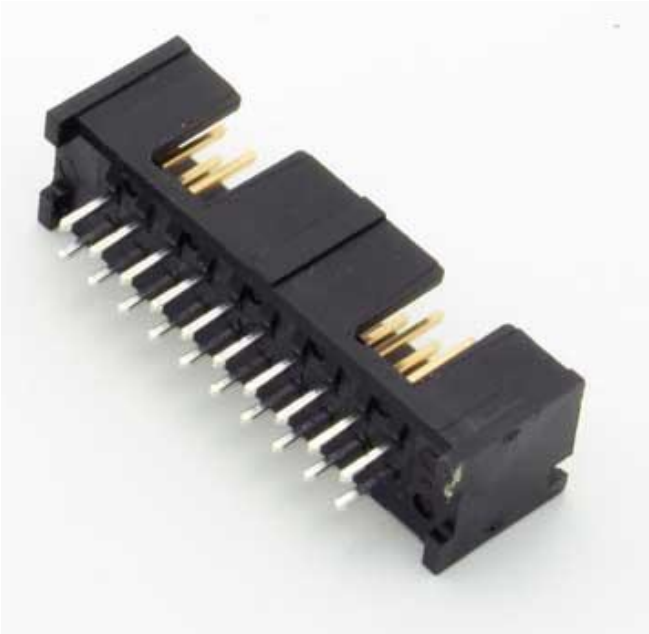
© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

A 20-pin PC header is useful for bridging the JTAG connection from the Kynar to the JTAG hardware ribbon. The JTAG ribbon has a female end so a male/male PC header will expose pins that jumper leads can easily access.

Approximate Total Cost

$5



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

You have a few options for JTAG hardware, but you can get an image of most phones using the RIFF Box.

The RIFF Box is by far the easiest and most user-friendly model because it has a great software suite and supports both CDMA and GSM devices. In addition, it handles the VREF connection (reference power) internally, so it saves you from having to solder an additional lead to the board.

Approximate Total Cost

$170



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

The Medusa Box is another great option and supports some models that the RIFF Box doesn't. Unlike the RIFF Box, this box requires you to solder a lead on the VREF pad to determine the CPU signal voltage.

Purchase of this box is optional, but its inclusion increases the supported devices list.

Approximate Total Cost

$160



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

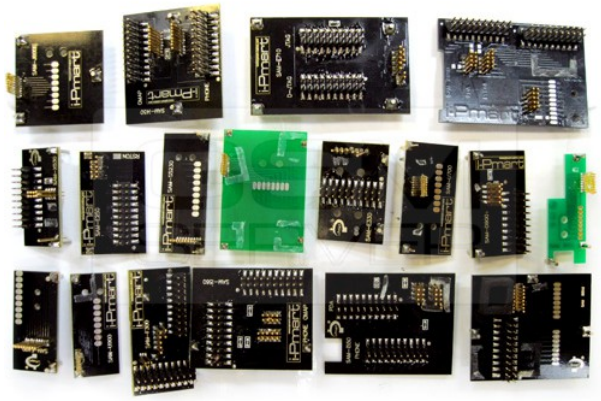
Shopping List

JTAG adapters, or “jigs” can save time by obtaining a connection to the board without soldering. They are designed to contact the appropriate JTAG pads by using “pogo pins” that get compressed to the pad. The downside is that these jigs are very fragile and often will not make a solid connection. Nonetheless, you can always try these first, and then solder the connection if you are unsuccessful.

Adapters are manufactured for a variety of devices. You can purchase them individually or in a complete kit.

Approximate Total Cost

$80



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Shopping List

Soldering iron and stand $50
Solder and solder wick $15
Kynar wire $15
Magnifying light $65
Power supply $100
Tool Kit $35
Multimeter tool $40
Jumper wires $45
PC Header $5
RIFF Box JTAG $170
Medusa JTAG $160
Optional adapters $80

Total: $780



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

As you can see, the cost of entry for JTAG is inexpensive, and with these supplies you'll have everything necessary to get into most JTAG-supported phones.

In the next few slides, we'll cover some of the equipment in more detail to give you a better understanding of how it all works.

Some of the equipment is self-explanatory, but it's worth going over the features to avoid any confusion. It may also help you later on in troubleshooting any unforeseen issues.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

We'll start with the power supply, because an improperly-configured power supply can quickly and permanently damage the circuit board.

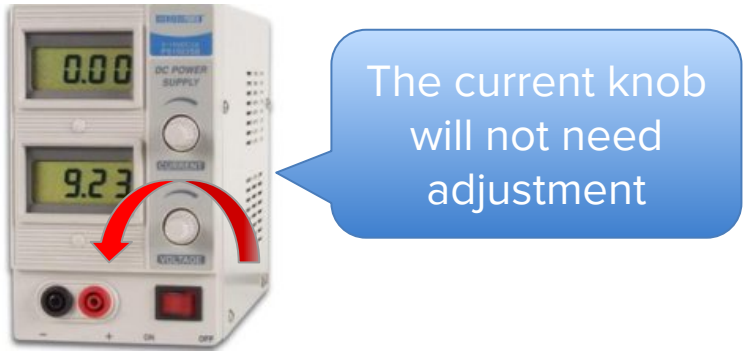
First, always check the voltage setting before connecting your mobile phone circuit board. If the voltage is not set properly, your day will go downhill quickly as smoke begins to rise from the CPU of your evidence!

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Simply turn on the power supply with nothing connected and turn the voltage down to zero- or to the recommended voltage if you know it. It is not necessary to adjust the current knob (the top knob) since the phone will draw what it needs, which is usually a very small amount.

The voltage is set to 9.23 on the power supply pictured below. The lower knob will turn down the voltage when turned counter-clockwise:



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

When connecting the power supply to the phone, you should use the existing battery terminals inside the phone's battery bay. Take a look at the battery to determine the appropriate polarity, and connect the to the power supply leads to the phone using jumper wires. You can examine the bottom of the battery to see which terminals correspond to the positive and negative pads on the battery:





© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

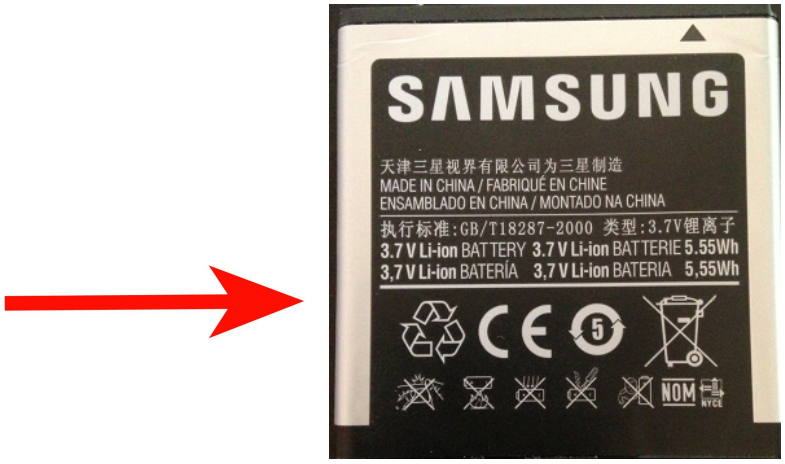


Click to open in YouTube.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

To determine the appropriate power supply voltage, take a look at the battery tolerance. Since a power supply in essence just replaces the phone's battery, the initial setting will be the same; in this example, it's 3.7 volts.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Simply set the power supply to 3.7 volts and you are ready to make a connection to the phone's circuit board. Turn the power supply off before making the initial connection!

The current reads zero because the board is not powered yet.

Once the board is connected and powered on, the current will rise, indicating that the board is drawing power from the power supply.

Note: Some devices will need additional voltage for a stable connection. Anything to 5 volts is typically safe.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Keep in mind that not all phones require a power supply. There are many options for powering the board:

- You can use the native battery, provided that the battery bay is present after disassembly and the battery is fully charged
- Your case may require a USB connection to power the board, which will usually generate about 4-5 volts to the board
- In some rare cases, the phone will require the battery terminals to be powered AND the USB terminal to be connected

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Remember, sometimes the battery voltage will not be enough, so if you are not able to get a stable connection try increasing the voltage to between 4 and 5 volts.

Caution: always disconnect the phone from the power supply before making voltage adjustments!

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

We will be covering some soldering techniques in JTAG 102 as well as phone disassembly.

For now, let's take a closer look at the JTAG hardware to become more familiar with its connections and overall functionality.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The first box we will cover is called the RIFF Box. This is your main piece of hardware because it's the easiest to operate and supports the most devices.

Keep in mind, all of the JTAG hardware boxes that we'll cover have been developed to repair mobile phones. Since we didn't become mobile investigators to repair phones, we'll spend the duration of this module learning to perform a complete file system dump instead.

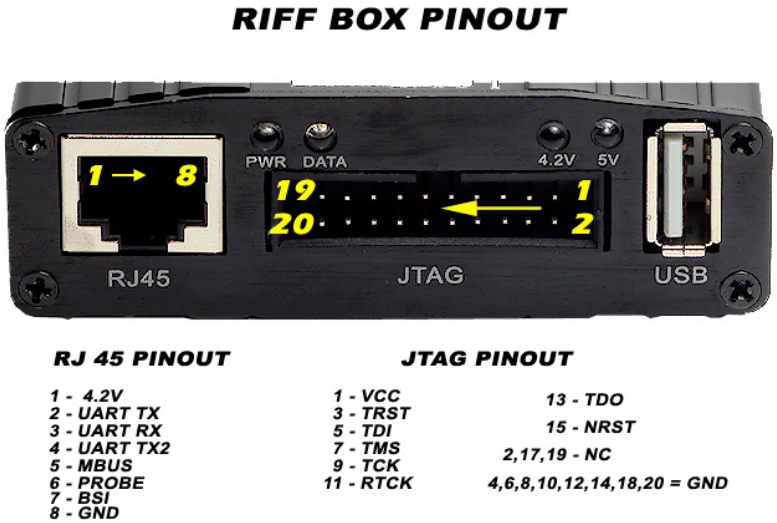


© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Regardless of whether you are repairing a phone or just reading data, the NAND the RIFF Box connections will be the same. The RIFF software does a great job of explaining how everything will get connected, but we will also cover it here to get you acquainted.

The image below shows the JTAG connection as well as the RJ45 pinout.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The RJ45 connection is mainly used for various tools, including a power supply jack as shown here:



You can power the phone's circuit board using this handy cable, essentially eliminating the need for an external power supply!

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

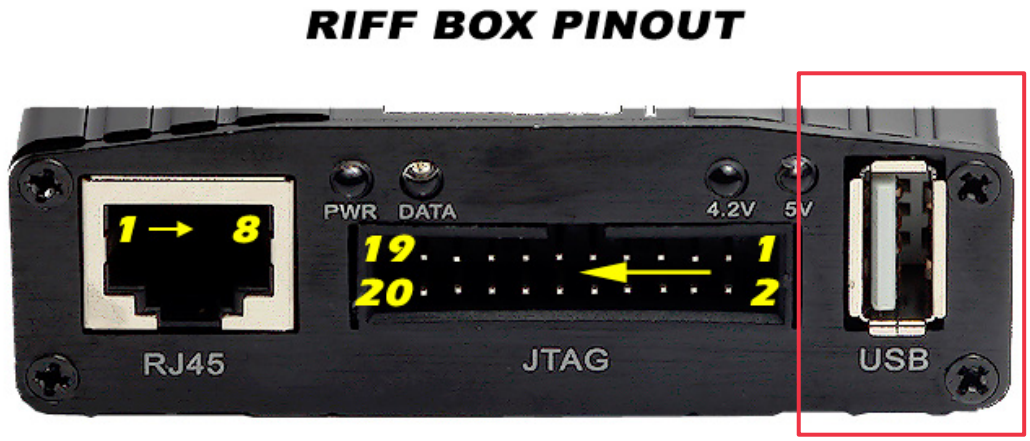
The RJ45 connection also contains a special probing lead that will return various probabilities that you are probing a specific pad, such as the TCK or the TDI.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The USB connection on the JTAG box will not be used.



RJ 45 PINOUT

1 - 4.2V
2 - UART TX
3 - UART RX
4 - UART TX2
5 - MBUS
6 - PROBE
7 - BSI
8 - GND

JTAG PINOUT

1 - VCC
3 - TRST
5 - TDI
7 - TMS
9 - TCK
11 - RTCK
13 - TDO
15 - NRST
2,17,19 - NC
4,6,8,10,12,14,18,20 = GND

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Finally, the flat tape 20-pin connector will interface with the box at the JTAG connection. The software shows you where each of the pins connect. Below, you can see that pin 3 is TRST, etc.

RIFF BOX PINOUT



RJ 45 PINOUT

1 - 4.2V
2 - UART TX
3 - UART RX
4 - UART TX2
5 - MBUS
6 - PROBE
7 - BSI
8 - GND

JTAG PINOUT

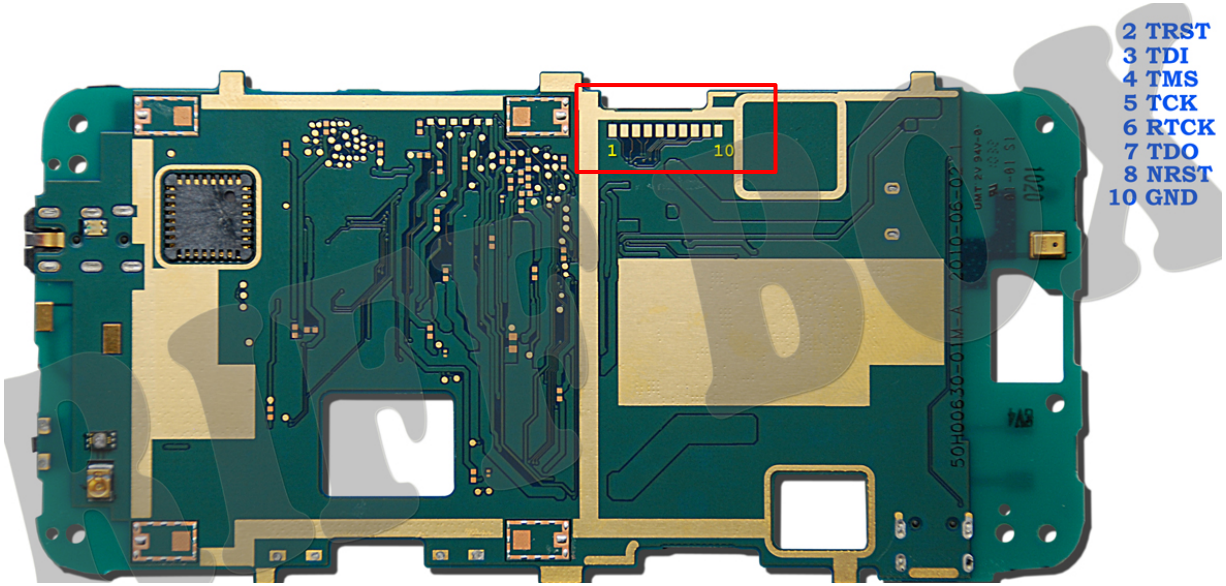
1 - VCC	13 - TDO
3 - TRST	15 - NRST
5 - TDI	2,17,19 - NC
7 - TMS	4,6,8,10,12,14,18,20 = GND
9 - TCK	
11 - RTCK	

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The RIFF Box JTAG terminals will need to be connected to the corresponding JTAG terminals on the phone's **PCB** (Printed Circuit Board). On the Droid Incredible below, you can see that there are 8 total leads that need to be connected, including the ground lead.

We will cover this more in detail in JTAG 102.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Earlier, we touched on the fact that the RIFF Box doesn't require any connection to VREF. Every phone circuit board has a defined I/O voltage level determined by the processor. This voltage level is known as VREF and is set internally by RIFF once you select the specific hardware model in the software interface. Some chips will have a 1.8 volt VREF while others have a 2.6v or 3.3v reference... it's all seamless with RIFF!

Other JTAG hardware boxes will require you to solder and connect the VREF JTAG pad so that the box can send the appropriate JTAG signal.

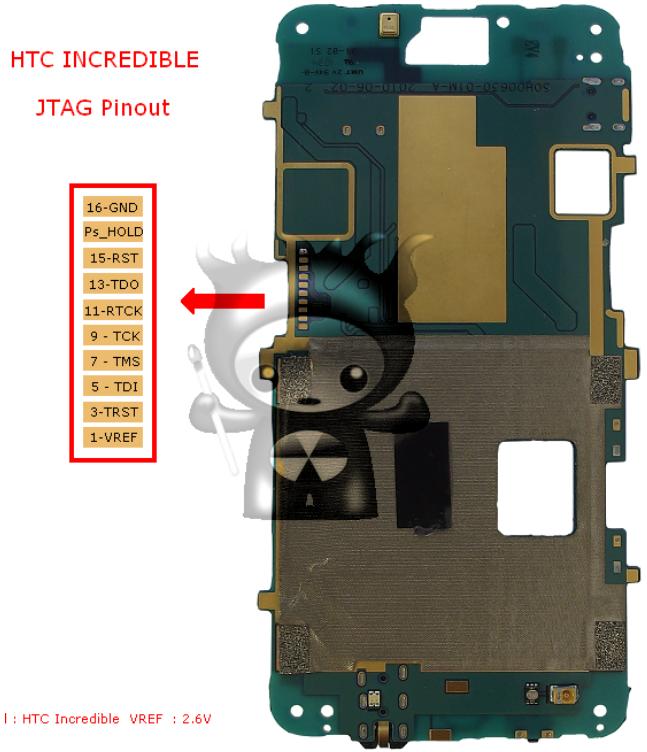
© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

For example, notice that the Omnia Repair Tool (**ORT**) hardware requires the VREF pad to be soldered on the Droid Incredible. It also requires the PS_HOLD pad to be soldered.

Medusa also requires this connection to be soldered.

NOTE: ORT is another manufacturer of JTAG hardware. We didn't add it to our shopping list of required items because typically you can accomplish what you need with the RIFF box or the Medusa Box.



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

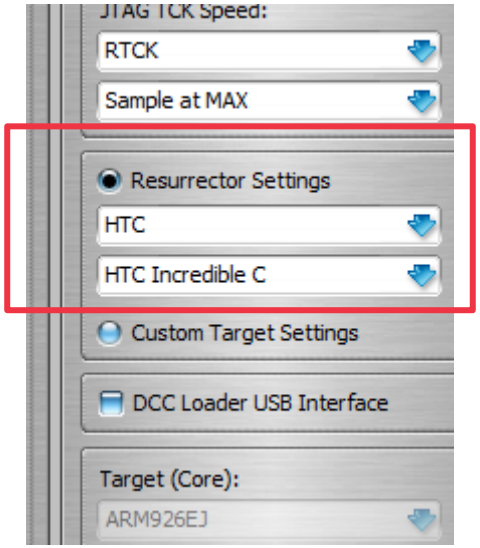
The RIFF Box adds more models to the list it supports almost daily, but some of the most popular include:

- Generic ARM Cores: ARM7, ARM9 (ARM920, ARM926, ARM946), ARM11, CORTEX-A8, CORTEX-A9;
- Qualcomm QSC Family: QSC1100, QSC1110, QSC6010, QSC6020, QSC6030, QSC6055, QSC6085, QSC6240, QSC6270;
- Qualcomm MSM Family: MSM6000, MSM6150, MSM6245, MSM6246, MSM6250, MSM6250A, MSM6260, MSM6275, MSM6280, MSM6280A, MSM6281, MSM6800A, MSM6801A, MSM6290, MSM7225, MSM7227, MSM7625, MSM7627, MSM7230, MSM8255, MSM8255T, MSM8260;
- Qualcomm QSD Family: QSD8250, QSD8650;
- Qualcomm ESM Family: ESM7602A;
- Qualcomm MDM Family: MDM6085 MDM6200, MDM6600;
- OMAP Family: OMAP1710, OMAP3430, OMAP3630, OMAP4430;
- NVIDIA Family: TEGRA2;
- Marvell/XScale Family: PXA270, PXA271, PXA272, PXA310, PXA312, PXA320.
- Samsung Processors: S5P6422, S5PV310

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Additionally, many of the more popular phone models can be selected from the make and model drop down menus in the software as shown below:



Simply select your make and model! We will cover this more in detail later on during the software portion of this lesson.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Some other quick things to point out about the RIFF Box:

- Connects to your workstation via USB
- In order to operate, requires the RIFF software, which will not open unless the box is physically attached to the workstation

The RIFF Box is by far the easiest for novice JTAG-ers to operate. If your device isn't supported by RIFF, you should to check with one of the other JTAG hardware providers to see if it is supported. Oftentimes you can select the CPU model in the software interface as an alternative as long as the JTAG pads are defined.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The JTAG box made by Omnia Repair Tool is called ORT-JTAG. Much of the overall concept is the same but this tool requires you to solder the VREF connection on every device. It also may require the PS_HOLD pad to be connected if specified.

Various VREF values include:

- Qualcomm – 2.6v or 1.8v
- Marvell – 3.3v
- OMAP – 1.8v



Once the lead is soldered and connected to pin 1, the JTAG box can internally determine the appropriate CPU voltage.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

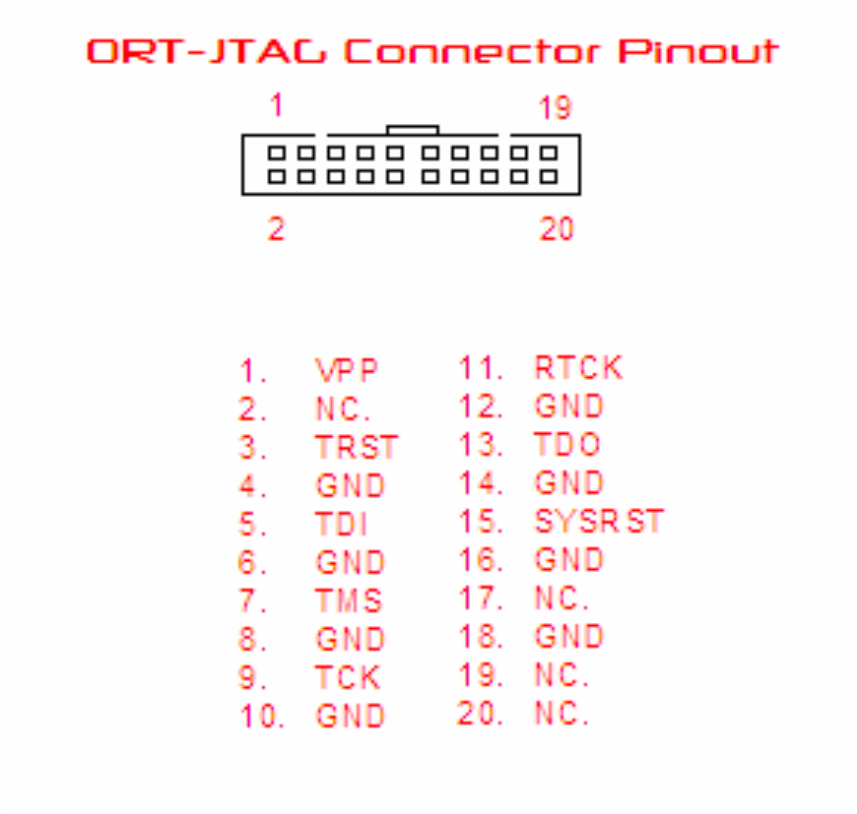
If the VREF pin is neither accessible nor known, you can power pin 1 on the JTAG box using your external power supply. Just be sure the voltage is set to the appropriate value based on your processor. Note that you are applying power to pin 1 of the JTAG hardware, not of the phone circuit board.

PS_HOLD can come in handy if the board does not stay powered on. Simply put, the PS_HOLD function is like holding the power button consistently. The RIFF Box does not have a PS_HOLD pin and requires you to hold the power button on if the board will not stay powered.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The ORT-JTAG box has a JTAG 20-pin harness similar to the RIFF Box, and the pinout is essentially the same:



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

ORT does not have a RJ-45 jack and will not perform any additional functions besides reading and repairing mobile phones.

The software interface is very basic and most of the support files are online behind a dedicated customer login. Once you purchase the box, you can register for access to the online support area where you will find PCB JTAG pinouts, repair files, software drivers, and more.

This box isn't very user-friendly, so it's not recommended as a tool for those just starting out. RIFF and Medusa will support all the same phones as ORT, so it's not required.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The last JTAG box that we will discuss is the Medusa Box. This JTAG hardware uses a RJ-45 connection exclusively and doesn't provide any other interface options.

Like the ORT box, the Medusa will require you to solder the VREF connection so it can establish the appropriate JTAG I/O voltage.



The Medusa also ships with a USB dongle that controls the license. It will not work without a properly-installed dongle.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

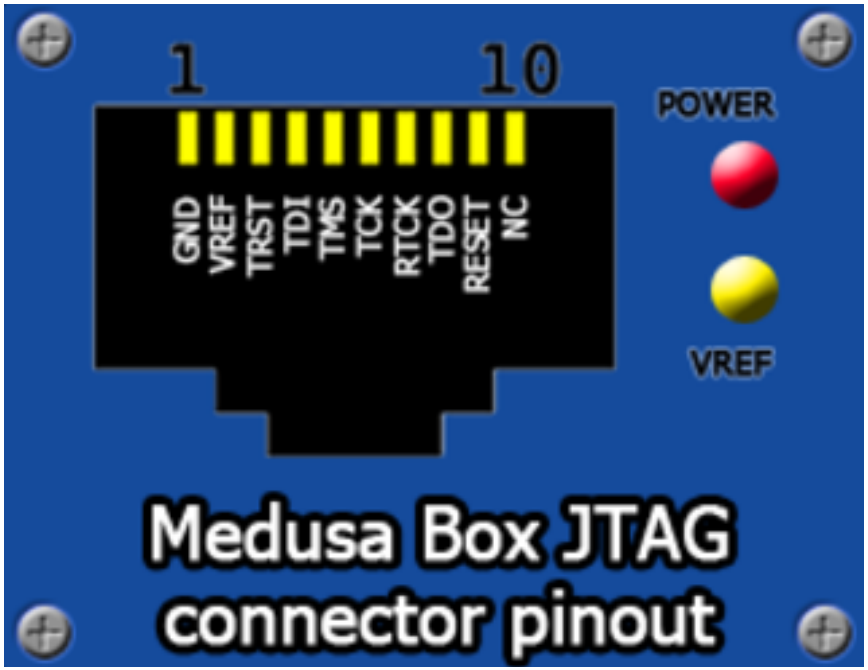
Models supported by Medusa Box are added almost daily, but some of the CPUs include:

Broadcomm BCM2133
Broadcomm BCM2155
Qualcomm MSM6245
Qualcomm MSM6246
Qualcomm MSM6250
Qualcomm MSM6250A
Qualcomm MSM6260
Qualcomm MSM6275
Qualcomm MSM6280
Qualcomm MSM6280A
Qualcomm MSM6281
Qualcomm MSM6290
Qualcomm MSM6800
Qualcomm MSM7200
Qualcomm MSM7200A
Qualcomm MSM7200B
Qualcomm MSM7201A
Qualcomm MSM7225
Qualcomm MSM7227
Qualcomm MSM7600
Qualcomm MSM8255
Qualcomm MSM8655
Qualcomm QSC6270
Qualcomm QSD8250
Qualcomm QSD8650
Qualcomm MDM6200
Qualcomm MDM6270 Modem
Marvell PXA270
Marvell PXA312
Texas Instruments OMAP850
Texas Instruments OMAP3630
Samsung S3C6410
Samsung S5PC110 Cortex A8 Mobile
Samsung S5PV310 (Exynos4210) Cortex A9 DualCore
ST-Ericsson NovaThor U8500

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

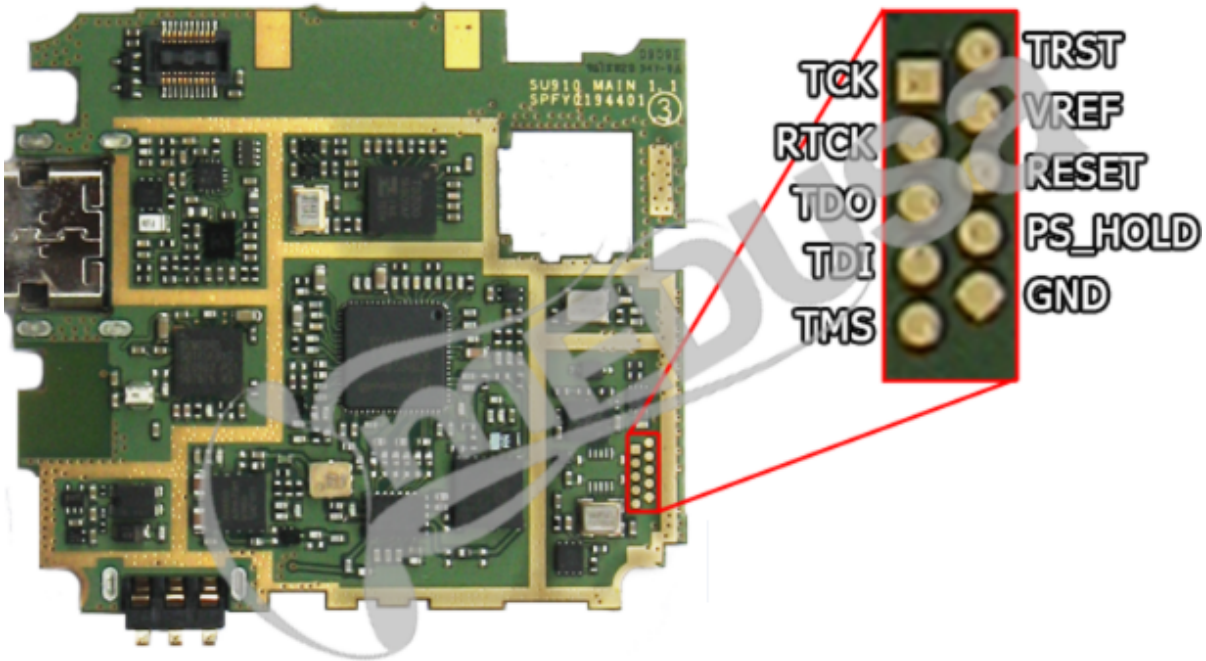
The following diagram shows how the RJ-45 terminals should be connected to the phone PCB:



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

Notice that the software gives you a photo of the board that maps out the JTAG pads. In this case, the additional pads are pictured (VREF and PS_HOLD):



© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

The software is fairly straightforward once you become familiar with the basics. We will cover how to install the software in the next section, and in JTAG 102 we will discuss how to use the software to perform a full binary dump of the NAND.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Equipment Overview

By now, you should have a better understanding of what JTAG is and of the tools that are required for you to be successful in your own lab. The next section will walk you through the installation of all three JTAG box driver and software packages.

You will need administrative rights to your workstation to complete the next section if you plan to follow along and install the software on your own machine.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Training Outline

1) JTAG Technical Overview
   - Why use JTAG?
   - JTAG defined
   - Test Access Port & Boundary Scan
2) Required Tools
   - Building the shopping list
   - Overview of various JTAG equipment
3) **Installing the Software**
   - Lab 1: Install the RIFF Box, ORT, and Medusa box software & drivers
4) Conclusion

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

In this section, we will walk through the entire process of installing the JTAG software and drivers for the RIFF Box and the Medusa Box.

You should already have administrative rights to your workstation. You also should ensure that you have some free space on your hard drive. The software doesn't take up much space, so it shouldn't be an issue for most users.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

We'll start with the RIFF Box software because that is our primary piece of JTAG hardware. Go to the RIFF website to download the latest software prior to plugging the RIFF Box into your USB port.

The software can be obtained from www.riffbox.org. Click on Downloads, and then click on the RIFF Box JTAG Manager software setup link. Note that there are some extra steps for the driver installation if you are running Windows XP.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

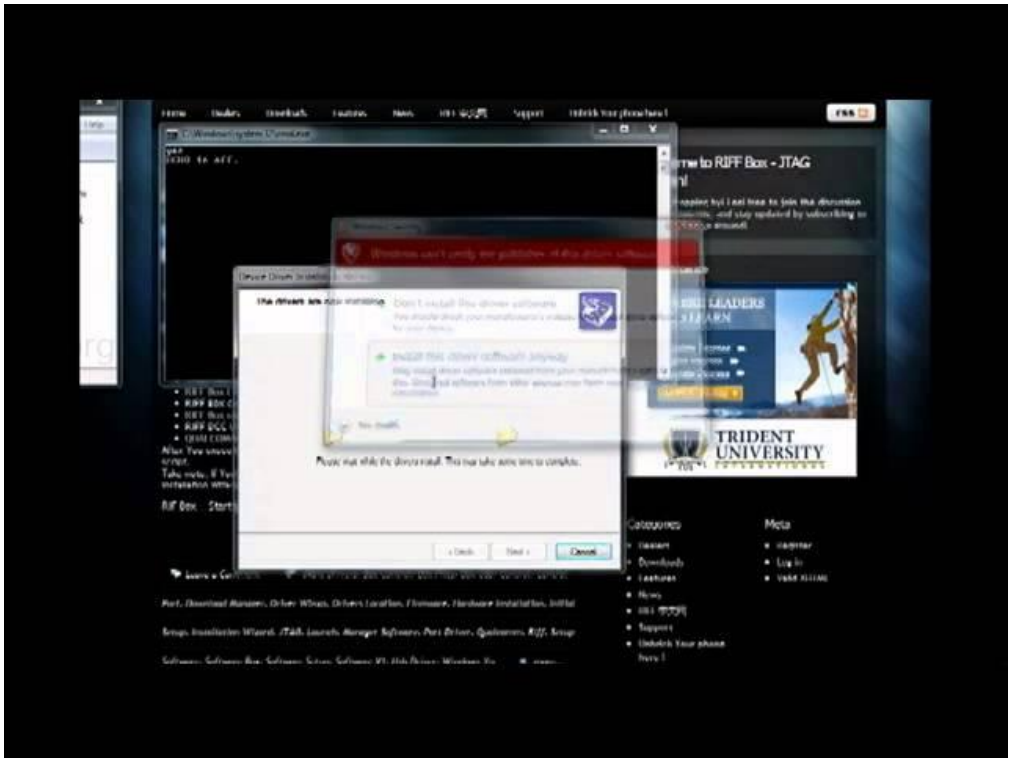
Install the software following the prompts, changing default directories if desired. If Windows prompts you with a driver security warning, you have no choice but to accept the unsigned driver.

Once the software is completely installed, you can plug your RIFF Box into the USB port on your computer.

Watch the video on the next slide as we demonstrate the installation process.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation



Click to open in YouTube.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

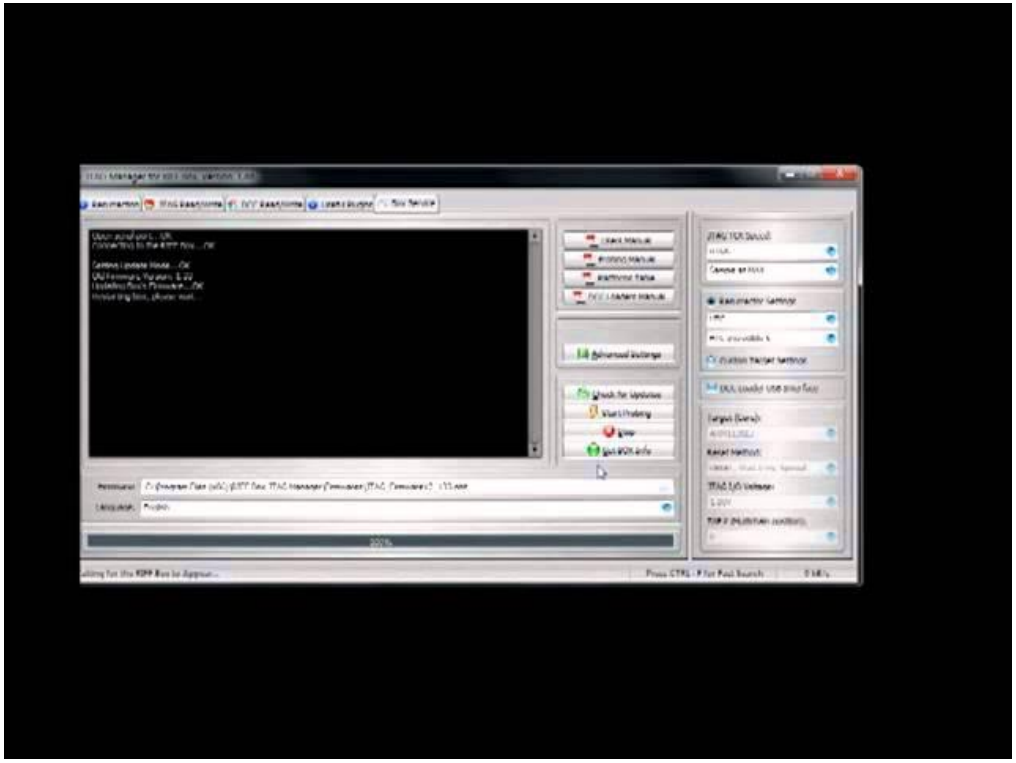
Launch the RIFF software and give it a try to make sure it works properly. We will go into the software and perform an update to ensure we are running the latest firmware.

Watch the video on the next slide to learn how to launch the software and update the firmware.

During the update mode, the RIFF Box will flash alternating green and red LEDs.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation



Click to open in YouTube.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

Congratulations! You have now successfully installed the RIFF software on your forensic workstation. This installation is typically trouble-free, so if you run into any errors during the installation, reference the RIFF Box website for more information.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

Next, let's install the Medusa Box software. First, you will need to download the software form the Medusa website. Navigate to http://medusabox.com/eng/download/software for all the required files.

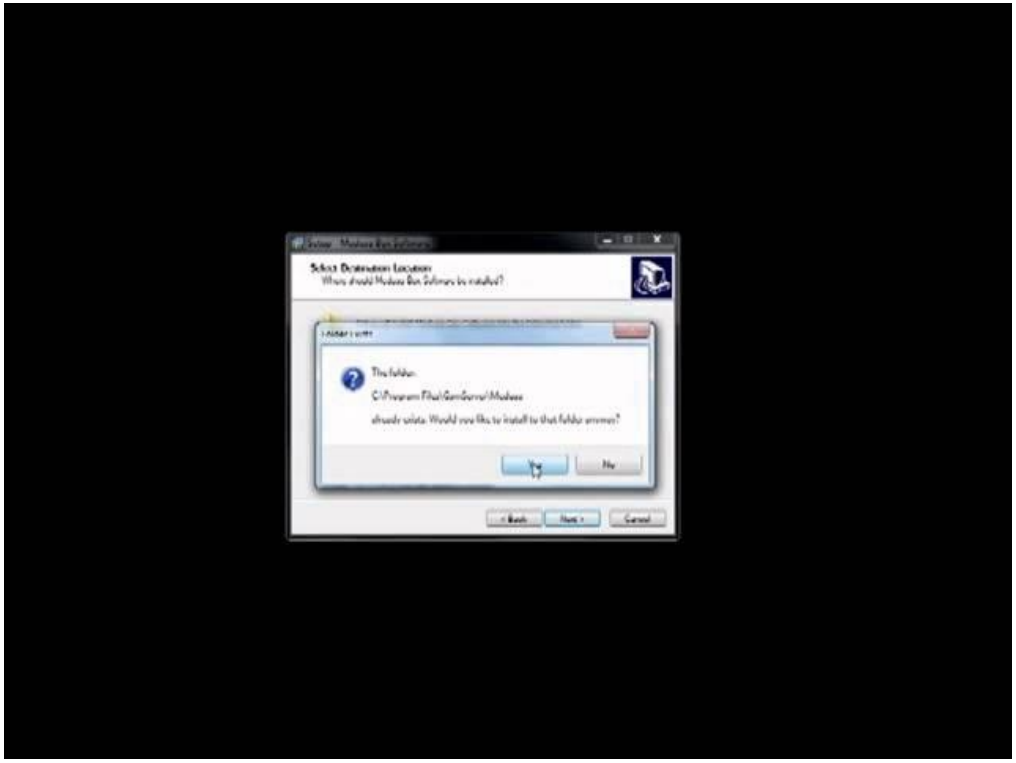
Download and install the Medusa Software Installer.

All of the drivers will be contained in a folder under Program Files/GSMServer/Medusa/Driver.

Watch the video on the next slide to see how the software is installed.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation



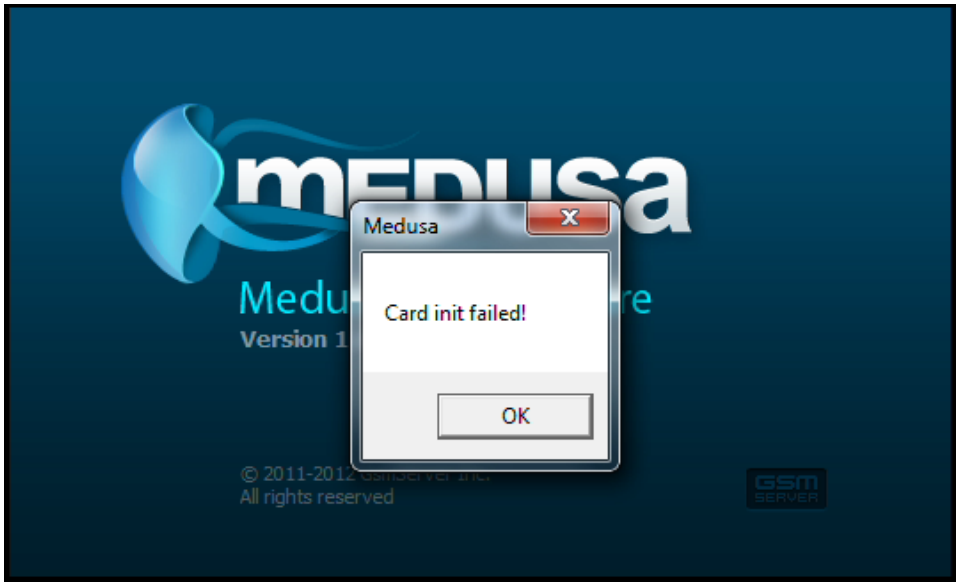
Click to open in YouTube.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

Once the software is installed, plug the USB cable into the Medusa box and insert your USB dongle into your forensic workstation.

When you attempt to run the software for the first time, you may see a Card Init Failed error:



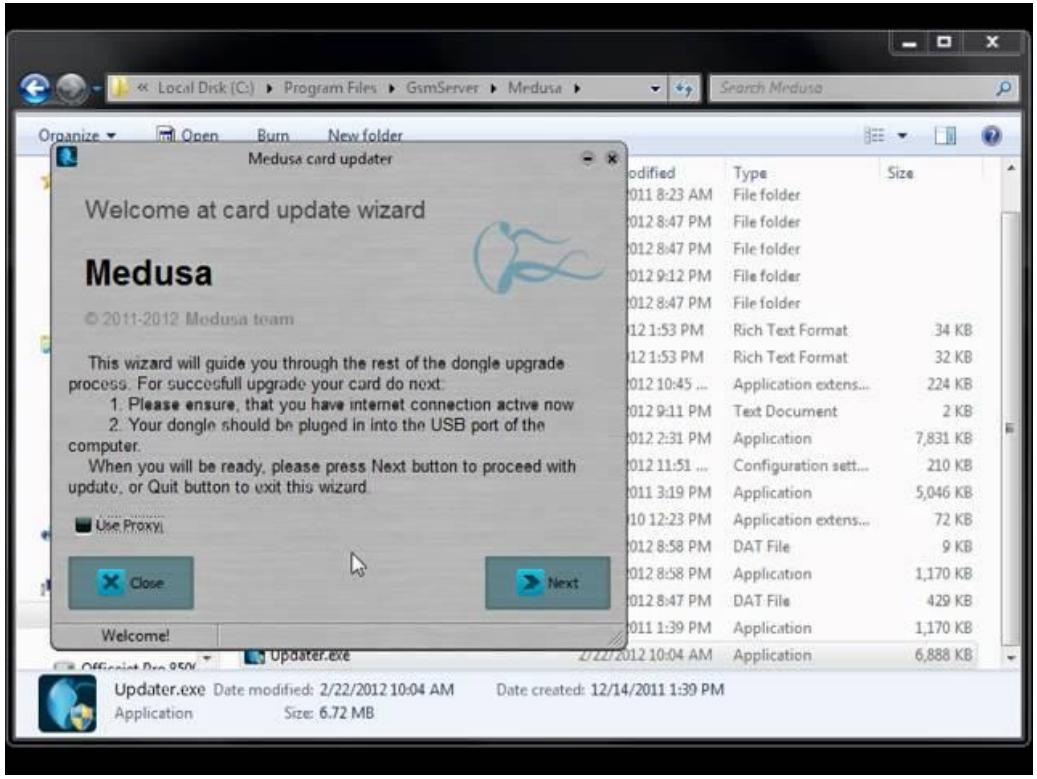
© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

This error is because the firmware or the drivers are not up to date on your dongle or Medusa box. The update process should fix the error, so take a look at the next slide to watch a video on how to update the firmware of your dongle and box.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation



Click to open in YouTube.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Software and Driver Installation

Once the firmware is updated, the software should start easily.

Start the Medusa software now.

When the software starts for the first time, it will finish installing the firmware that was downloaded in the previous step. Once that is complete, it will take you to the main screen where you can choose your device and begin the acquisition process.

If you run into any other errors during the installation or running the application, check the online support section for information on how to resolve the problem.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Training Outline

1) JTAG Technical Overview
   - Why use JTAG?
   - JTAG defined
   - Test Access Port & Boundary Scan
2) Required Tools
   - Building the shopping list
   - Overview of various JTAG equipment
3) Installing the Software
   - Lab 1: Install the RIFF Box, ORT, and Medusa box software & drivers
4) **Conclusion**

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Summary

You should now have a better grasp on what you need to set up your own JTAG lab. The equipment is affordable, and with the growing number of locked Android phones that cannot be imaged through traditional means, JTAG is becoming an essential tool.

Additionally, you are now familiarized with the basic JTAG process and its underlying functions. Knowing the configuration of the data in the memory of the device will help you defend your methods as well as give you more troubleshooting capability.

You have completed JTAG 101 and are now ready to move on to the next section!

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

JTAG 101 is Complete!

JTAG 102 will introduce you to phone disassembly and soldering techniques and walk you through the process of obtaining a full memory dump of the device using both the RIFF Box and Medusa Box.

Make sure you have acquired everything on your shopping list before moving on to JTAG 102 as we will be using all of it in that module.

© Copyright 2014 NowSecure, Inc. All Rights Reserved.

Recommended Downloads

Like this? Share with your friends (they'll thank you). Here's a tweet you can copy / paste:

> Want great #JTAG tips and tutorials? Check out "JTAG 101: Background & Required Tools" from @NowSecureMobile: https://www.nowsecure.com/resources/jtag-forensics-training/

If you like this training, you will love our other resources:

Reports & Trainings:

- Linux 101: Linux for Mobile Forensics
- Secure Mobile Development Best Practices

Free Tools & Software:

- Forensics Suite - Community Edition
- App Testing Suite - Community Edition

© Copyright 2014 NowSecure, Inc. All Rights Reserved. Do not distribute.



NowSecure™

This PDF was developed by NowSecure (@NowSecureMobile) and is not for redistribution. For corrections, comments or additional information please contact:

NowSecure Support
support@nowsecure.com
312-878-1100

Thank you for taking our course!

© Copyright 2014 NowSecure, Inc. All Rights Reserved. Do not distribute.