





Part #:	Digi XBee3[®] Zigbee 3.0 with BLE	  
Description:	The XBee3 [®] Zigbee [®] 3.0 with BLE radio series features ISM 2.4 GHz radios at +8 dBm and +19 dBm power ratings.	 Download Datasheet

EEVblog Electronics Community Forum

A Free & Open Forum For Electronics Enthusiasts & Professionals

Hello volvo_nut_v70

Show unread posts since last visit.
Show new replies to your posts.
July 13, 2019, 03:16:03 am

 This topic

- Home
- Help
- Search
- Profile
- About us
- My Messages
- Calendar
- Links
- HashTags
- Members
- Logout

EEVblog Electronics Community Forum » Products » Test Equipment » DPO3000 Hacks


PCB Prototype for \$2
 (Any Color)



MSOX3104T ~~\$7,370.10~~
\$6,633.09
Save an extra 10%!



« previous next »

Pages: 1 2 [All] **Go Down**

- REPLY
- NOTIFY
- MARK UNREAD
- SEND THIS TOPIC
- PRINT
- SEARCH

Author

Topic: **DPO3000 Hacks** (Read 12538 times)

volvo_nut_v70 and 0 Guests are viewing this topic.

FivePoint0

Contributor
Posts: 28

DPO3000 Hacks

« on: January 13, 2015, 09:38:27 am »

Say Thanks Reply Quote

I know people on here love the Rigols, but . . .

Are there any hacks for the DPO3000? Been offered one at a reasonable price and it appears the 100 MHz and 500 MHz are the same hardware . . .

Report to moderator

TopLoser

Supporter

Posts: 1841
Country:

Re: DPO3000 Hacks

« Reply #1 on: January 13, 2015, 09:52:25 am »

Say Thanks Reply Quote

Well the plug in option modules are easily... erm... replicated!

Not heard of a bandwidth upgrade yet.

Report to moderator

FivePoint0

Contributor
Posts: 28

Re: DPO3000 Hacks

« Reply #2 on: January 15, 2015, 08:37:53 am »

Say Thanks Reply Quote

Yet all the bandwidth upgrade needs is for the user to type in a key.

Shame. I'd buy it just for the hack!

Report to moderator

abyrvalg

Frequent Contributor

Re: DPO3000 Hacks

« Reply #3 on: April 23, 2015, 08:53:40 am »

Say Thanks Reply Quote



Posts: 350

Country:



Looks like some things (including BW upgrade) can be done over GPIB, but I don't have a scope to verify. Somebody willing to try?

Some interesting commands:

:PASSWORD "password"- enable special modes

Valid passwords:

"XYZZY" - "user's password"

"INTEKRITY" - "backdoor password" (this is the right one for other "backdoor" mode commands)

"PUBLIC" - "public password"

"TRESPASS" - "developer password"

"MKTDEMO" -

:SETMODELID id - set model

Valid IDs:

0 - MSO/DPO3012 (MSO/DPO is selected by digital channels presence)

1 - MSO/DPO3014

2 - MSO/DPO3032

3 - MSO/DPO3034

4 - MSO/DPO3052

5 - MSO/DPO3054

:HWAccountant:SERIAL - get/set serial number

:HWAccountant:INSTRumentid - get instrument id (no set here, it is generated from model+serial)

:HWAccountant:ACQBandwidth bw - bandwidth upgrade

valid values:

300

500

:ARMDemo pass, num_days - activate demo mode

pass: "DontMakeTheWookieMad"

num_days 1-30

Report to moderator

The following users thanked this post: dzseki

Sync

Contributor

Posts: 13



Re: DPO3000 Hacks

« Reply #4 on: May 26, 2015, 10:05:20 pm »

Say Thanks

Reply

Quote

I cannot get these to work and my IDA skills are too bad to figure out what is happening.

As I said in the other thread, there should also be a debug console available that is accessible through TCPIP but I cannot figure out how to connect to it...

Report to moderator

j_hallows

Contributor

Posts: 8



Re: DPO3000 Hacks

« Reply #5 on: June 02, 2015, 08:13:21 am »

Say Thanks

Reply

Quote

Quote from: _Sync_ on May 26, 2015, 10:05:20 pm

I cannot get these to work and my IDA skills are too bad to figure out what is happening.

As I said in the other thread, there should also be a debug console available that is accessible through TCPIP but I cannot figure out how to connect to it...

This is for the DPO3000/MSO3000 not MDO3000. Different hardware.

These commands can be sent via TekVisa to the DPO3000/MSO3000.

Report to moderator

Jwalling

Supporter



Posts: 1158

Country:

Re: DPO3000 Hacks

« Reply #6 on: June 02, 2015, 08:30:47 pm »

Say Thanks

Reply

Quote

Quote from: _Sync_ on May 26, 2015, 10:05:20 pm

I cannot get these to work and my IDA skills are too bad to figure out what is happening.

As I said in the other thread, there should also be a debug console available that is accessible through TCPIP but I cannot figure out how to connect to it...

This is work?



Just a guess, but maybe Telnet? I have an MSO3034 - I'll give it a try later today and see what happens.

Jay

[Report to moderator](#) Logged

Jay

System error. Strike any user to continue.

 Jwalling

Supporter



Posts: 1158

Country:

This is work?

**Re: DPO3000 Hacks**« **Reply #7 on:** June 03, 2015, 03:06:46 am »[Say Thanks](#)[Reply](#)[Quote](#)**Quote from: Jwalling on June 02, 2015, 08:30:47 pm****Quote from: _Sync_ on May 26, 2015, 10:05:20 pm**

I cannot get these to work and my IDA skills are too bad to figure out what is happening.

As I said in the other thread, there should also be a debug console available that is accessible through TCPIP but I cannot figure out how to connect to it...

Just a guess, but maybe Telnet? I have an MSO3034 - I'll give it a try later today and see what happens.

Jay

OK, so using telnet didn't work, but using my browser (Firefox) brings up a Tektronix menu. I selected the tab "DATA" and I'm able to talk to the scope using GPIB commands. I then sent the following per abyrvag's post:

```
:SETMODELID 5
:HWAccountant:ACQBandwidth 500
```

Then power-cycled the unit. It did not make any changes. So I used the back door password first:

```
:PASSWord "INTEKRITY"
:SETMODELID 5
:HWAccountant:ACQBandwidth 500
```

Then power-cycled the unit again. Still no change. I'm probably doing something wrong; I'm an idiot when it comes to stuff like this... 🙄

Jay

[Report to moderator](#) Logged

Jay

System error. Strike any user to continue.

 Jwalling

Supporter



Posts: 1158

Country:

This is work?

**Re: DPO3000 Hacks**« **Reply #8 on:** June 03, 2015, 03:13:53 am »[Say Thanks](#)[Reply](#)[Quote](#)**Quote from: Jwalling on June 03, 2015, 03:06:46 am****Quote from: Jwalling on June 02, 2015, 08:30:47 pm****Quote from: _Sync_ on May 26, 2015, 10:05:20 pm**

I cannot get these to work and my IDA skills are too bad to figure out what is happening.

As I said in the other thread, there should also be a debug console available that is accessible through TCPIP but I cannot figure out how to connect to it...

Just a guess, but maybe Telnet? I have an MSO3034 - I'll give it a try later today and see what happens.

Jay

OK, so using telnet didn't work, but using my browser (Firefox) brings up a Tektronix menu. I selected the tab "DATA" and I'm able to talk to the scope using GPIB commands. I then sent the following per abyrvag's post:

```
:SETMODELID 5
```

:HWAccountant:ACQBandwidth 500

Then power-cycled the unit. It did not make any changes.
So I used the back door password first:

```
:PASSWord "INTEKRITY"
:SETMODELID 5
:HWAccountant:ACQBandwidth 500
```

Then power-cycled the unit again. Still no change. I'm probably doing something wrong; I'm an idiot when it comes to stuff like this... 🤔

Jay

OK, it's confirmed, I am an idiot. 🤔 Remove the quotes around the password:

```
:PASSWord INTEKRITY
:SETMODELID 5
:HWAccountant:ACQBandwidth 500
```

Voila, it reports that it is a MSO5054!

Thank you very much abyrgalg! 🙏 Now to do some bandwidth testing!

Jay

[Report to moderator](#)  Logged

Jay


System error. Strike any user to continue.

abyrgalg

Frequent Contributor



Posts: 350

Country: 




Jwalling

Supporter



Posts: 1158

Country: 

This is work?



Re: DPO3000 Hacks

« **Reply #9 on:** June 03, 2015, 07:10:59 am »

[Say Thanks](#)

[Reply](#)

[Quote](#)

Great! 🙏 Try ARMDemo also - my guess it should enable all options for a specified number of days.

[Report to moderator](#)  Logged

Re: DPO3000 Hacks

« **Reply #10 on:** June 04, 2015, 03:21:40 am »

[Say Thanks](#)

[Reply](#)

[Quote](#)

Quote from: abyrgalg on June 03, 2015, 07:10:59 am

Great! 🙏 Try ARMDemo also - my guess it should enable all options for a specified number of days.

Huh. That didn't seem to work...

I tried both:

```
:ARMDemo DontMakeTheWookieMad, 30
:ARMDemo DontMakeTheWookieMad 30
```

Wasn't sure about the comma...

My firmware revision is 2.07 - perhaps that may play into the equation as it's rather old.

In other news, with a 500MHz 600mV signal applied from my signal generator to each channel in 50 Ohm mode, all four channels measure a minimum of 520mV, so the scope exceeds the specification of a MSO5054. In fact, the amplitude is not what falls below spec first, but the triggering. at about 550MHz, the trigger starts becoming unstable.

Nice!

As a side note, my scope has a number of errors from 2010 that I'd like to clear. I've looked through the operators, programming, and service manual and did not find anything on what command(s) might do this. Would you or anyone else happen to know how to clear them?

Many thanks again! 🙏

Jay

« *Last Edit:* June 04, 2015, 03:31:33 am by Jwalling »

[Report to moderator](#)  Logged

Jay

System error. Strike any user to continue.

j_hallows

Re: DPO3000 Hacks

« **Reply #11 on:** June 04, 2015, 12:32:33 pm »

[Say Thanks](#)

[Reply](#)

[Quote](#)

Contributor

Posts: 8



Quote

I tried both:
:ARMDemo DontMakeTheWookieMad, 30
:ARMDemo DontMakeTheWookieMad 30

Did you do:

Code: [Select]

:PASSWORD INTEKRITY

First?

Quote

In other news, with a 500MHz 600mV signal applied from my signal generator to each channel in 50 Ohm mode, all four channels measure a minimum of 520mV, so the scope exceeds the specification of a MSO5054.

Does it say MSO5054 or MSO3054?

Report to moderator Logged

Jwalling

Supporter



Posts: 1158

Country:

This is work?



Re: DPO3000 Hacks

« Reply #12 on: June 05, 2015, 03:27:34 am »

Say Thanks

Reply

Quote

Quote from: j_hallows on June 04, 2015, 12:32:33 pm

Quote

I tried both:
:ARMDemo DontMakeTheWookieMad, 30
:ARMDemo DontMakeTheWookieMad 30

Did you do:

Code: [Select]

:PASSWORD INTEKRITY

First?

Quote

In other news, with a 500MHz 600mV signal applied from my signal generator to each channel in 50 Ohm mode, all four channels measure a minimum of 520mV, so the scope exceeds the specification of a MSO5054.

Does it say MSO5054 or MSO3054?

I tried with :PASSWORD INTEKRITY first and that didn't make any difference.

I updated the firmware to 2.40, no difference.

Oops. - that was a typo (or perhaps wishful thinking! 😊 Yes, it reports itself as a MSO3054.

The error logs can be retrieved with:

:ERRlog?

:ERRlog:NEXT?

There's two other references in the firmware with regards to the error logs.

:ERRlog:CLEar and :ERRlog:FILL

The CLEar doesn't seem to work.

FILL does not seem to do anything either.

Jay

Report to moderator Logged

Jay

System error. Strike any user to continue.

j_hallows

Contributor

Posts: 8



Re: DPO3000 Hacks

« Reply #13 on: October 05, 2015, 12:44:59 am »

Say Thanks

Reply

Quote

I just saw this on E-bay, (see attached Picture).

So I guess we have the wrong sequence for activating the modules.



Unlock-DPO3000.JPG (200.08 kB, 1600x900 - viewed 1199 times.)

« Last Edit: October 05, 2015, 12:46:56 am by j_hallows »

Report to moderator Logged

darkstar49

Regular Contributor



Posts: 143



Re: DPO3000 Hacks

« Reply #14 on: December 06, 2015, 01:33:14 am »

Say Thanks Reply Quote

Hi together,

HWAccountant:ACQBandwidth 500

indeed works fine, a 100Mhz model suddenly can trigger without problems on a 500Mhz signal, but... when displaying for example the frequency of that signal, it says low resolution (+- 2.5V P2P, and it's from a Rohde&Schwarz generator, quite clean 500Mhz sine wave), so I'm not too sure that hack alone does it... the "low resolution" warning starts at around 155Mhz, which suggests there's another soft-limit somewhere that needs to be 'extended'... My scope (MSO3014) has a serial > C020000, so definitely one that does NOT need Tek for the upgrade...

The ideal way would be to find out how the key is generated for the 500Mhz upgrade, because the scope's firmware definitely knows what to do when upgrading... Maybe some similar routines as for the MDO3000 ?? (if I got it right, the MDO3xxx option modules now contain not stupidly the option's name, but some encrypted form of it... so maybe the key generated by Tek for the DPO3K BW upgrade uses similar or identical routines...??)

Report to moderator Logged

Marchello

Contributor

Posts: 25

Country:



Re: DPO3000 Hacks

« Reply #15 on: December 06, 2015, 02:31:19 am »

Say Thanks Reply Quote

Is it possible to hack MSO4034? (not B version)

Best regards!
Mark

Report to moderator Logged

robert_

Regular Contributor



Posts: 151

Country:



Re: DPO3000 Hacks

« Reply #16 on: December 06, 2015, 05:29:55 am »

Say Thanks Reply Quote

Cant answer to this, but as i have a MSO3014, C02* at work, i did hack it some months ago. Worked fine, and bandwidth did improve, although it doesnt seem to meet the 3054 risetime spec. I measure around 1ns on a fast rise pulse, which measures around 600ns on a HDO6054 (samne on an old TDS7054), which would suggest around 350-400Mhz. Still a huge improvement over the standard 100Mhz, and enough to get my work done properly (where im dealing with around 3ns edges).

As for the options, i did install them the old way. Program one of these option modules (TDS3FFT borrowed from an old TDS3k, not needed anymore) with the option needed, insert in scope and transfer the licence from the module to the scope, reprogram with next option and repeat.

Report to moderator Logged

darkstar49

Regular Contributor



Posts: 143



Re: DPO3000 Hacks

« Reply #17 on: December 07, 2015, 02:31:33 am »

Say Thanks Reply Quote

And btw, these changes seem impossible to roll-back... so be careful playing around with this... ;-)
But if anyone has managed to undo such changes, comments are welcome...

Report to moderator Logged

darkstar49

Regular Contributor



Posts: 143



Re: DPO3000 Hacks

« Reply #18 on: December 07, 2015, 04:17:29 am »

Say Thanks Reply Quote

@Marchello...

Don't think so... DPO4K's are not bandwidth upgradeable, and other Tek models have shown to have high-pass filters in hardware to differentiate models (same board, but a few different components...),


so a bandwidth upgrade is possible in theory (up to 500Mhz for the 2.5GS/s models), but definitely requires hardware changes, and to my knowledge, these have never been attempted, nor documented anywhere...

Report to moderator  Logged

Marchello

Contributor

Posts: 25

Country: 



Re: DPO3000 Hacks

« Reply #19 on: December 07, 2015, 09:56:42 pm »

Say Thanks Reply Quote

Ok. Thanks to all!
I activated all options. (sim card holder + 24C08 + PICKITII + few strings)
BW let it be 350 MHz...

Best regards!
Mark

Report to moderator  Logged

tmbinc

Regular Contributor



Posts: 172



Re: DPO3000 Hacks

« Reply #20 on: December 08, 2015, 09:01:28 am »

Say Thanks Reply Quote

I did bandwidth-update my DPO5034 (they have 5GS/s even for the 350MHz models) by removing the lowpass (on one channel), see <http://debugmo.de/2013/03/whats-inside-tektronix-dpo5034/> .

I also hacked my DPO4034 (non-B) to "more" bandwidth by hacking the executable - not a nice hack by any means. The DPO4034 has the pre-amp which the DPO4034B and DPO5034(B) lack; but it only has 2.5GHz so that limits the usefulness a bit.

Report to moderator  Logged

darkstar49

Regular Contributor



Posts: 143



Re: DPO3000 Hacks

« Reply #21 on: December 11, 2015, 08:03:41 am »

Say Thanks Reply Quote

Once again, if anyone knows of other :HWAccountant:xxxxx commands... please let us know... there's definitely something missing by setting only the Acquisition bandwidth to 500...

Or alternatively: where did Abyrvalg get this 😞 Is there a chance to find more about these commands by disassembling the binaries ?? Or was that some 'insider info' 😞


Report to moderator  Logged

klaus11

Supporter



Posts: 156

Country: 



Re: DPO3000 Hacks

« Reply #22 on: December 11, 2015, 08:47:18 pm »

Say Thanks Reply Quote

Know any tricks for TDS5000B? 😊

Report to moderator  Logged

HP3458A, HP3245a, Keithley 2000, Fluke 87V, Rigol DP832, TEK TDS5052B, HP33120A

darkstar49

Regular Contributor



Posts: 143



Re: DPO3000 Hacks

« Reply #23 on: January 18, 2016, 07:35:37 pm »

Say Thanks Reply Quote

There are "tricks" for the TDS7000B (and others), I can't imagine why the code would be that much different for the TDS5000B...

But it looks like every model series has its own encryption key(s) and options bitmasks, so disassembling the code and finding those would always be step 1...

The logic is always the same... a key is an encrypted version of a bitmask (every bit set being a specific option), coded using the device ID and an (AES) encryption key.

So you (just ;-)) need the bitmasks for the different options, the logic to generate the unique device ID, and the AES key...

Report to moderator  Logged

klaus11

Supporter



Re: DPO3000 Hacks

« Reply #24 on: January 19, 2016, 09:42:57 pm »

Say Thanks Reply Quote

Quote from: darkstar49 on January 18, 2016, 07:35:37 pm



Posts: 156
Country: 00

There are "tricks" for the TDS7000B (and others), I can't imagine why the code would be that much different for the TDS5000B...
But it looks like every model series has its own encryption key(s) and options bitmasks, so disassembling the code and finding those would always be step 1...

The logic is always the same... a key is an encrypted version of a bitmask (every bit set being a specific option), coded using the device ID and an (AES) encryption key.

So you (just ;-)) need the bitmasks for the different options, the logic to generate the unique device ID, and the AES key...

Thank

[Report to moderator](#) [Logged](#)

HP3458A, HP3245a, Keithley 2000, Fluke 87V, Rigol DP832, TEK TDS5052B, HP33120A

darkstar49

Regular Contributor



Posts: 143



Re: DPO3000 Hacks

« **Reply #25 on:** January 22, 2016, 06:22:21 am »

[Say Thanks](#)

[Reply](#)

[Quote](#)

It may sound a bit more difficult than it actually is...

The binaries typically contain a lot of debug stuff, that ease finding the functions of interest, then looking after some forms of "load" instructions preceding function calls (like Encrypt(...)), you rapidly can find addresses of interest and find out the AES key, same approach for the option masks, there's usually one function for evaluating an option key, and that function references all the possible option masks at some point... not trivial, but with some reasonable assembler knowledge (32 bit x86 assembler for TDS500B I think ??), and some time, it should be feasible...

Regards

[Report to moderator](#) [Logged](#)

darkstar49

Regular Contributor



Posts: 143



Re: DPO3000 Hacks

« **Reply #26 on:** June 10, 2016, 09:07:51 am »

[Say Thanks](#)

[Reply](#)

[Quote](#)

For info, same logic applies for DPO3000 than for MDO3000, just one (BW upgrade) at a time...
AES key to be found in the binary, or.. ;-)
So use the mdo3keygen python stuff, works great (change the key) !

Again: only works for BW upgrades on DPO/MSO3K... NO other options via keys...

[Report to moderator](#) [Logged](#)

FivePoint03

Regular Contributor



Posts: 51

Country:



Re: DPO3000 Hacks

« **Reply #27 on:** August 24, 2016, 08:04:13 am »

[Say Thanks](#)

[Reply](#)

[Quote](#)

So you mean the AES key is different between DPO3000 and MDO3000 - help us out - how can I find the AES key for DPO3000 😊 ?

[Report to moderator](#) [Logged](#)

kazik70

Contributor

Posts: 17

Country:



Re: DPO3000 Hacks

« **Reply #28 on:** January 30, 2018, 02:37:55 am »

[Say Thanks](#)

[Reply](#)

[Quote](#)

Code: [\[Select\]](#)

DPO/MSP3000 Firmware v2.38 2/29/2012

"New Features:

- Bandwidth is field upgradeable (up to 500 MHz).
This option can be purchased and installed by the customer.
(Serial numbers < C020000 or < B020000 must be upgraded by a Tektronix service center)."

Not all DPO / MSO3000 can be hacked up to 500Mhz?
What are your serial numbers?
Has someone managed to hack <020000?

Report to moderator  Logged **darkstar49**

Regular Contributor



Posts: 143

 **Re: DPO3000 Hacks**

« Reply #29 on: January 31, 2018, 06:10:23 pm »

Say Thanks Reply Quote

No feedback so far on upgrading serials < X020000


I don't think you can break something for good... the point is that there's to my knowledge no known way to 'uninstall' the upgrade (regardless if it was done with a key, or with system commands...), so if you did, and it makes your scope somehow unusable, you're good to send it in for servicing... 🤔

« Last Edit: January 31, 2018, 08:56:11 pm by darkstar49 »

Report to moderator  Logged **kazik70**

Contributor

Posts: 17

Country:  **Re: DPO3000 Hacks**

« Reply #30 on: February 09, 2018, 05:21:28 am »

Say Thanks Reply Quote

I made an upgrade from DPO3012 to DPO3052. Serial number C02XXXX, firmware vesjon 2.40

And there was a difference with the description.

SETMODELID

- 1 - 3012
- 2 - 3014
- 3 - 3032
- 4 - 3034
- 5 - 3052
- 6 - 3054

The model changed in real time, but the bandwich after reboot the scope.

Can you help with the modules?

Report to moderator  Logged **Tardz**

Newbie

Posts: 2

Country:  **Re: DPO3000 Hacks**

« Reply #31 on: March 31, 2018, 05:05:14 am »

Say Thanks Reply Quote


Hi, I have a DPO3014 firmware V2.4, how to hack and activate all option ?

Report to moderator  Logged **abyrvalg**

Frequent Contributor



Posts: 350

Country:  **Re: DPO3000 Hacks**

« Reply #32 on: April 03, 2018, 07:18:23 am »

Say Thanks Reply Quote

Back to the "ARMDemo" thing: the parameter order was wrong, NumOfDays must be first. Somebody please verify:

Code: [Select]


```
:PASSW INTEKRITY
:ARMDemo 30,"DontMakeThewookieeMad
or:
:ARMDemo 30,"DontMakeThewookieeMad"
```

Report to moderator  Logged **abyrvalg**

Frequent Contributor



Posts: 350

Country:  **Re: DPO3000 Hacks**

« Reply #33 on: April 22, 2018, 09:43:15 am »

Say Thanks Reply Quote

ARMDemo confirmed to work. Use the first version (w/o quotes).

Report to moderator  Logged

The following users thanked this post: RomDump

 **darkstar49**

Regular Contributor



Posts: 143

 **Re: DPO3000 Hacks**

« Reply #34 on: April 24, 2018, 06:58:39 am »

Say Thanks Reply Quote

also for those who think that a frequency upgrade means their model ID changes:

The official Tektronix bandwidth upgrade does NOT modify the model ID !!!!!!!!!!!!!!! So this doesn't have any effect, other than showing the world that it's been hacked !! 🤖

Report to moderator Logged

The following users thanked this post: RomDump

Pages: 1 2 [All] **Go Up**

REPLY NOTIFY MARK UNREAD SEND THIS TOPIC PRINT SEARCH
« previous next »

Share me



EEVblog Electronics Community Forum » Products » Test Equipment » DPO3000 Hacks

LINK TO CALENDAR

Jump to:

Quick Reply

 **BUDGET MULTIMETERS !!** 
ANENG, UNI-T and more...

[EEVblog Main Site](#)

[EEVblog on Youtube](#)

[EEVblog on Twitter](#)

[EEVblog on Facebook](#)