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.
June 21, 2019, 01:32:22 am

This topic Search

Home Help Search Profile About us My Messages [1] Calendar Links HashTags Members Logout

EEVblog Electronics Community Forum » Products » Test Equipment » Tektronix TDS1000B and TDS2000B series hacks

« previous next »

Pages: 1 2 3 [All] Go Down REPLY NOTIFY MARK UNREAD SEND THIS TOPIC PRINT SEARCH

Author Topic: Tektronix TDS1000B and TDS2000B series hacks (Read 23833 times)

volvo_nut_v70 and 0 Guests are viewing this topic.

KK
Regular Contributor
Posts: 99
Country:

Tektronix TDS1000B and TDS2000B series hacks
« **on:** June 29, 2014, 05:00:21 am »
Say Thanks Reply Quote

Anyone know of a way to upgrade bandwidth on the Tek 1000B series scopes?

Assuming the hardware is identical on the 40-70-100 MHz units.

I want to upgrade a 40mhz 1001B scope I use with iview and a logic analyzer to 100mhz.

« *Last Edit: July 19, 2014, 03:16:11 am by KK* »
Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #1 on:** July 06, 2014, 10:03:02 am »
Say Thanks Reply Quote

Looks like I will dissemble the firmware file to see how to change the identifier.

Any tear downs yet on these scopes - TDS1001b/1002b/1012b?

Anyone know the main processor offhand?

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #2 on:** July 18, 2014, 06:01:45 am »
Say Thanks Reply Quote

Looks like the firmware is common for the TDS1000B/TDS2000B series Oscilloscopes.

I'm disassembling it to look at some of the remote commands. I've found some interesting things to look closer at.

VXWorks is used as the RTOS, and this scope uses a Freescale 68000 compatible processor.


1304995799616.jpg (76.19 kB, 640x480 - viewed 1047 times.)

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #3 on:** July 18, 2014, 06:02:25 am »
Say Thanks Reply Quote

DS1339C

i2C Clock


1304995782459.jpg (37.75 kB, 301x360 - viewed 885 times.)

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #4 on:** July 18, 2014, 06:03:29 am »
Say Thanks Reply Quote

Firmware flash

Spansion
S29JL064H

64Mbit flash memory 4Mbx16


1304995784713.jpg (97.67 kB, 640x480 - viewed 804 times.)

« *Last Edit: July 19, 2014, 08:25:04 am by KK* »

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #5 on:** July 18, 2014, 06:04:27 am »
Say Thanks Reply Quote

DRAM. 64Mbit 512Kx32 in 4 banks.


1304995786470.jpg (92.45 kB, 640x480 - viewed 674 times.)

Report to moderator Logged

KK
Regular Contributor
Posts: 99

Re: Tektronix TDS1000B series hacks
« **Reply #6 on:** July 18, 2014, 06:05:03 am »
Say Thanks Reply Quote

NS
ADG522

Country:

Can't find info. Must be the A/D.

1304995787850.jpg (88.18 kB, 640x480 - viewed 974 times.)

« *Last Edit: July 18, 2014, 06:06:49 am by KK* »

Report to moderator Logged

KK

Regular Contributor

Posts: 99

Country:

Re: Tektronix TDS1000B series hacks

« **Reply #7 on:** July 18, 2014, 06:06:16 am »

Say Thanks Reply Quote

Unknown NS chip

EE69RD
9858-00

Another similar chip not pictured is
NS
EE63RA
9857-00

1304995801028.jpg (79.07 kB, 640x480 - viewed 791 times.)

« *Last Edit: July 19, 2014, 08:21:22 am by KK* »

Report to moderator Logged

KK

Regular Contributor

Posts: 99

Country:

Re: Tektronix TDS1000B series hacks

« **Reply #8 on:** July 18, 2014, 06:07:42 am »

Say Thanks Reply Quote

Highspeed SRAM 128K x 8

1304995803363.jpg (98.36 kB, 640x480 - viewed 549 times.)

« *Last Edit: July 19, 2014, 05:40:15 am by KK* »

Report to moderator Logged

KK

Regular Contributor

Posts: 99

Country:

Re: Tektronix TDS1000B series hacks

« **Reply #9 on:** July 18, 2014, 06:08:44 am »

Say Thanks Reply Quote

Main ram

SRAM 1 Mbit 64K x 16

1304995805304.jpg (93.25 kB, 640x480 - viewed 698 times.)

Report to moderator Logged

KK

Regular Contributor

Posts: 99

Country:

Re: Tektronix TDS1000B series hacks

« **Reply #10 on:** July 18, 2014, 06:09:52 am »

Say Thanks Reply Quote

Altera Max II
EPM240

8K flash

1304995807652.jpg (74.13 kB, 640x480 - viewed 521 times.)

« *Last Edit: July 19, 2014, 08:20:01 am by KK* »

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #11 on:** July 18, 2014, 06:10:40 am »

Say Thanks Reply Quote

USB Driver

Cypress Semi CY7C67300-100AXI

1304995811918.jpg (87.53 kB, 640x480 - viewed 600 times.)

Report to moderator Logged

nctnico
Super Contributor

Posts: 16828
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #12 on:** July 18, 2014, 06:15:18 am »

Say Thanks Reply Quote

> **Quote from: KK on July 18, 2014, 06:07:42 am**
>
> Highspeed SRAM 128K x 8
>
> Must be sample memory

Probably not. The sampling memory (1k points?) is inside the sampling ASIC.

Report to moderator Logged

There are small lies, big lies and then there is what is on the screen of your oscilloscope.

tautech
Super Contributor

Posts: 14799
Country:

Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B series hacks
« **Reply #13 on:** July 18, 2014, 06:19:54 am »

Say Thanks Reply Quote

> **Quote**
>
> Looks like the firmware is common for the TDS1000B/TDS2000B series Oscilloscopes.

Now I'm interested.
I have TDS2102B in bits with a corroded pin on the USB chip.
I could possibly help if needed.

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #14 on:** July 18, 2014, 09:14:49 am »

Say Thanks Reply Quote

> **Quote from: nctnico on July 18, 2014, 06:15:18 am**
>
> > **Quote from: KK on July 18, 2014, 06:07:42 am**
> >
> > Highspeed SRAM 128K x 8
> >
> > Must be sample memory
>
> Probably not. The sampling memory (1k points?) is inside the sampling ASIC.

Yeah, it's only 2.5K points

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #15 on:** July 18, 2014, 09:22:11 am »

Quote from: tautech on July 18, 2014, 06:19:54 am

Quote

Looks like the firmware is common for the TDS1000B/TDS2000B series Oscilloscopes.

Now I'm interested.
I have TDS2102B in bits with a corroded pin on the USB chip.
I could possibly help if needed.

Here is the latest firmware V22.16 for TDS1000B and TDS2000B series models.
The file isn't encrypted or compressed.
(too big to attach- download here)
http://www.tek.com/oscilloscope/tds1001b-software/firmware-update-tds1000b-and-tds2000b-v2216

binwalk hasn't been helpful, but I have it in Ida Pro right now and I can see some interesting routines.

There are a bunch of 488.2 commands you can send it over USB using the Tektronix open choice talker/listener app.

Some of the undocumented commands from the firmware might allow for a model identifier change (bandwidth) and/or direct bandwidth change.

There are some interesting error messages in the firmware like-

Number of channels is 2 and you have selected a 4-channel Model
Display is MONO and you have selected a COLOR Model
Number of channels is 4 and you have selected a 2 channel model
Display is COLOR and you have selected a MONO model

success!; saving constants ...

« *Last Edit: July 18, 2014, 05:13:33 pm by KK* »

Report to moderator Logged

tinhead
Super Contributor
Posts: 1864
Country:

Re: Tektronix TDS1000B series hacks

Say Thanks Reply Quote

« **Reply #16 on:** July 18, 2014, 09:55:40 am »

what you doing is the wrong way, the firmware is for all models, so it does not matter what inside (unless you wish to search the whole firmware for model checks and patch it then). The best way is to patch the model itself, and this has been saved somewhere. The RTC clocke does have some user bytes, but htey can't be used (without special tricks) to store model. Are there any eeproms on the board? i bet the altera cpld is readback protected, but well, just try to dump it. If the model check is really in that cpld (and not eeprom) then it is still possible to change it, e.g. by watching the bus for call just before model check in fw, and then sending the crafted info back. When eepom used, then it will be much easier. Or even simple tricks like some "not populated" parts, TEK did that on other models and one can hack them very easy (which still did't change anything, without calibration mainly useless - and to run cal one need anyway some gears, so ppl who can calobrate have enought money anyways to buy higher TEK models).

Report to moderator Logged

I don't want to be human! I want to see gamma rays, I want to hear X-rays, and I want to smell dark matter ...
I want to reach out with something other than these prehensile paws and feel the solar wind of a supernova flowing over me.

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks

Say Thanks Reply Quote

« **Reply #17 on:** July 18, 2014, 10:17:01 am »

Interesting ideas.

Is it possible Tektronix made one motherboard for both the model series and then configures them with commands after final assembly to what kind of model it should be. I am pursuing the theory that I can issue a command to change the max bandwidth and/or model.

I have other oscilloscopes, this is just used with my tla714 logic analyzer for iview. The type of screen it uses and feature set are mostly irrelevant as I'm looking at the waveform on Windows 7 anyway.

Bandwidth matters. I decided to buy the lowest bandwidth model because I figured hacking it up to the max would be possible.

« *Last Edit: July 18, 2014, 04:27:30 pm by KK* »

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #18 on:** July 18, 2014, 03:59:30 pm »
Say Thanks Reply Quote

The 'B' series of these scopes introduced a USB port. Amongst the many advantages is that it works with the TLA Logic Analyzer software to overlay the scope signal with the logic analyzer signals and sync the signals.

They all have (only) 2.5K points memory. Although that doesn't matter in my application.

TDS1000B is a 2-channel monochrome LCD Series-

1001B - 40 Mhz / 500 MS/s
1002B - 60 Mhz / 1.0 GS/s
1012B - 100 Mhz / 1.0 GS/s

TDS2000B series is a 2 or 4 channel color LCD series-

2 channels-

2002B - 60 Mhz / 1.0 GS/s
2012B - 100 Mhz / 1.0 GS/s
2022B - 200 Mhz / 2.0 GS/s

4 channels-

2004B - 60 Mhz / 1.0 GS/s
2014B - 100 Mhz / 1.0 GS/s
2024B - 200 Mhz / 2.0 GS/s

« *Last Edit: July 18, 2014, 04:02:45 pm by KK* »
Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #19 on:** July 19, 2014, 03:18:58 am »
Say Thanks Reply Quote

Quote from: tautech on July 18, 2014, 06:19:54 am

Quote

Looks like the firmware is common for the TDS1000B/TDS2000B series Oscilloscopes.

Now I'm interested.
I have TDS2102B in bits with a corroded pin on the USB chip.
I could possibly help if needed.

Do you mean TDS2012B ?

Is your chipset identical to mine?

« *Last Edit: July 19, 2014, 05:38:48 am by KK* »
Report to moderator Logged

tautech
Super Contributor
Posts: 14799
Country:
Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B series hacks
« **Reply #20 on:** July 19, 2014, 05:47:32 am »
Say Thanks Reply Quote

Quote from: KK on July 19, 2014, 03:18:58 am

Quote from: tautech on July 18, 2014, 06:19:54 am

Quote

Looks like the firmware is common for the TDS1000B/TDS2000B series Oscilloscopes.

Now I'm interested.
I have TDS2102B in bits with a corroded pin on the USB chip.
I could possibly help if needed.

Do you mean TDS2012B ?

Is your chipset identical to mine?

Yes, yes.

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #21 on:** July 19, 2014, 05:49:57 am »
Say Thanks Reply Quote

> **Quote from: tautech on July 19, 2014, 05:47:32 am**
>
> > **Quote from: KK on July 19, 2014, 03:18:58 am**
> >
> > > **Quote from: tautech on July 18, 2014, 06:19:54 am**
> > >
> > > > **Quote**
> > > >
> > > > Looks like the firmware is common for the TDS1000B/TDS2000B series Oscilloscopes.
> > >
> > > Now I'm interested.
> > > I have TDS2102B in bits with a corroded pin on the USB chip.
> > > I could possibly help if needed.
> >
> > Do you mean TDS2012B ?
> >
> > Is your chipset identical to mine?
>
> Yes, yes.

Do the two white labeled chips flash & cpld have the same codes printed on them?

Report to moderator Logged

tautech
Super Contributor
Posts: 14799
Country:
Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #22 on:** July 19, 2014, 06:09:00 am »
Say Thanks Reply Quote

U800, F163. 166600
U801, F163. 166100. V21.20

In bits ATM.
Fails boot.
Pin 22 on U900 (USB chip) corroded through.

I need to be off grog for a week to have a steady hand to attempt to solder a very fine wire to the pad.
Other option is replacement. Bit nervous about that, but I will just have to man up.
Got plenty of other gear, so it's low priority.

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #23 on:** July 19, 2014, 06:32:58 am »
Say Thanks Reply Quote

Identical. So the only difference between the 1000B and 2000B 2 channel series is the display module.

Perhaps we can get these scopes up to 200Mhz

Report to moderator Logged

The following users thanked this post: MarkL

tautech
Super Contributor
Posts: 14799
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #24 on:** July 19, 2014, 06:53:08 am »
Say Thanks Reply Quote

> **Quote from: KK on July 19, 2014, 06:32:58 am**
>
> Identical. So the only difference between the 1000B and 2000B 2 channel series is the display module.
>
> Perhaps we can get these scopes up to 200Mhz

That would turn heads.
I have no gear for any in depth sniffing etc, only a decoding DSO.
I will help if I can.

Taupaki Technologies Ltd. NZ
Siglent Distributor

The only advice I could offer is to take note of **tinhead**'s interest.

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #25 on:** July 20, 2014, 02:06:08 pm »
Say Thanks Reply Quote

Quote from: tinhead on July 18, 2014, 09:55:40 am

> what you doing is the wrong way, the firmware is for all models, so it does not matter what inside (unless you wish to search the whole firmware for model checks and patch it then). The best way is to patch the model itself, and this has been saved somewhere. The RTC clocke does have some user bytes, but htey can't be used (without special tricks) to store model. Are there any eeproms on the board? i bet the altera cpld is readback protected, but well, just try to dump it. If the model check is really in that cpld (and not eeprom) then it is still possible to change it, e.g. by watching the bus for call just before model check in fw, and then sending the crafted info back. When eepom used, then it will be much easier. Or even simple tricks like some "not populated" parts, TEK did that on other models and one can hack them very easy (which still did't change anything, without calibration mainly useless - and to run cal one need anyway some gears, so ppl who can calobrate have enought money anyways to buy higher TEK models).

There is at least one flash. The main flash holds the program code, and maybe some model ID/sn. There are two other unknown chips that may have some memory.

I am more of a software guy, and have disassembled 80% of the firmware, because you know the 80/20 rule!

I found it interesting because it gives me an overview of what is going on.

My random thoughts are-

It's more complicated than I would have guessed. They are programming a USB chip, on the fly, to offload tasks.

There is a lot of printer driver code embedded. Tons of remote programming code.

What's interesting are two specialized menu's that can be enabled.

Service Mode
Engineering Mode

Service mode is documented, but doesn't do anything special.

Engineering mode, I suspect, will let you change interesting things like serial number and model type. There are error messages that prevent you from enabling 4 channels when the model hardware only has two, and color when the hardware is black & whiite.

There are no error messages for bandwidth.

Additionally, there is a lot of code for power analysis. It is enabled when a USB key is verified for TBS2PWR1

My first thoughts are that the TDS scopes can do the power analysis functions the TBS scope can. Tektronix decided to limit those functions to there TBS series.

That series also has similar bandwidth and 2.5K/points memory so I'm thinking the hardware is again identical.

The goal of this mission is to enable all bandwidth options fot the TDS1000B/2000B scopes and potentially enable the TBS2PWR1 functions since they are in the same firmware. It's not just a reference I see the entire functions and calculations in my dis assembly.

My focus now is to decode how to get into "Engineering Mode" through the front panel. Disassembly helped me find out there is such a thing.

« *Last Edit: July 20, 2014, 02:09:47 pm by KK* »

Report to moderator Logged

tautech
Super Contributor

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #26 on:** July 20, 2014, 02:37:50 pm »
Say Thanks Reply Quote

I can read all chips #'s on my PCB.
Tell me which you need.

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

Posts: 14799
Country:

Taupaki Technologies Ltd. NZ
Siglent Distributor

KK
Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #27 on:** July 21, 2014, 07:23:17 am »

> **Quote from: tautech on July 20, 2014, 02:37:50 pm**
>
> I can read all chips #'s on my PCB.
> Tell me which you need.

They match all the ones in my photos right? I think the main boards are identical.

Report to moderator Logged

KK
Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #28 on:** July 21, 2014, 07:29:22 am »

Zeroing in on it. Looking at the code that handles the front panel buttons to see the "secret" entry method.

The memory map appears to be-

0-4MB Main ram
4MB-8MB Flash program
8MB++ other hardware like usb controller etc

The model id and serial number are stored alongside the factory calibration data. These scopes let you re-calibrate through the service menu. Looking into where that data is stored.

Flash holds 4MB and the firmware file leaves about 647K free in the flash. The cal data might be at the end of the flash or it might be stored in some other chip.

« *Last Edit: July 21, 2014, 07:34:04 am by KK* »

Report to moderator Logged

tautech
Super Contributor

Posts: 14799
Country:

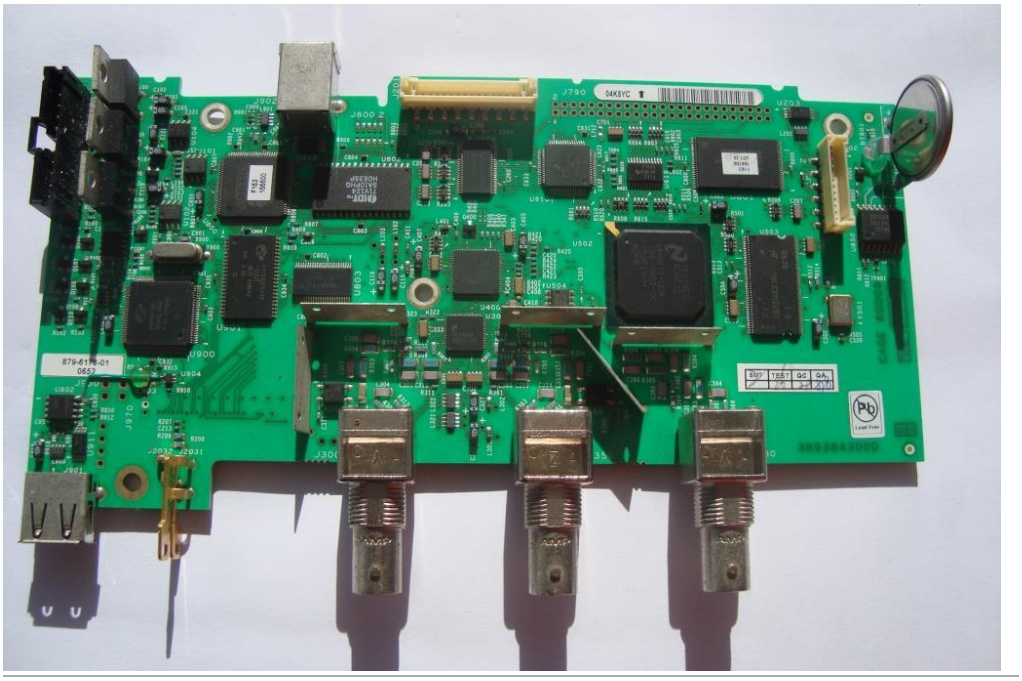
Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #29 on:** July 21, 2014, 07:41:45 am »

> **Quote from: KK on July 21, 2014, 07:23:17 am**
>
> > **Quote from: tautech on July 20, 2014, 02:37:50 pm**
> >
> > I can read all chips #'s on my PCB.
> > Tell me which you need.
>
> They match all the ones in my photos right? I think the main boards are identical.

Quite well.
There are minor variations with U502, 400, 301.

Looks like revisions.



TDS2012B MB.JPG (117.48 kB, 1024x683 - viewed 4666 times.)

« *Last Edit: July 21, 2014, 10:09:13 am by tautech* »

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #30 on:** July 23, 2014, 02:51:56 pm »

Say Thanks Reply Quote

Whats the chip next to the USB port. I didn't pull the board all the way out of my enclosure so didn't see that one.

Report to moderator Logged

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #31 on:** July 23, 2014, 03:00:02 pm »

Say Thanks Reply Quote

Interesting discoveries so far...

The service mode can be entered with the following procedure-

Power on scope
Press MEASURE button
Press CH1 soft button

Press and hold SINGLE SEQ button
Press and hold AUTOSET button

Wait 5 seconds

Release SINGLE SEQ button
Release AUTOSET button

Notice lower left of screen displays "Service mode ON"

Press UTILITY button

Press SERVICE soft button

Press Service Diag. soft button

Press Peek/Poke soft button

Isn't that nice. Tektronix included a way to read or write memory, live. Any location. Right from the front panel.

I'm correlating the disassembly with some configuration memory locations in ram. I believe I can test some config changes (changing bandwidth) on the fly. It won't be permanent with this method, but it will let me confirm what part of the code is handling that process.

Engineering Mode is entered in a similar, but as of yet unknown way.

I believe I see code that lets Tektronix quickly configure models with USB keys. They insert one key to configure the model to a TDS1001B or another to configure it to a TDS1002B with higher bandwidth.

Will be looking further into both angles.

« *Last Edit: July 23, 2014, 03:04:02 pm by KK* »

Report to moderator Logged

tautech

Super Contributor

Posts: 14799
Country:

Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #32 on:** July 23, 2014, 03:58:34 pm »

> **Quote from: KK on July 23, 2014, 02:51:56 pm**
>
> Whats the chip next to the USB port. I didn't pull the board all the way out of my enclosure so didn't see that one.

SOIC8 Atmel 24C1024W close to front panel USB

From the Tek Service manual:

Enable the Service Menu
1. Power on the oscilloscope.
2. Push the front-panel MEASURE button to access the MEASURE menu.
3. Push the top option button to access the Measure 1 menu.
4. Push and hold the front-panel SINGLE SEQ button.
5. Push and hold the front-panel AUTOSET button.
6. Wait at least two seconds.
7. Release the SINGLE SEQ button.
8. Release the AUTOSET button. A message appears in the lower left corner of the screen stating “Service mode ON.”
9. Push the front-panel UTILITY button. The last item in the Utility menu is now “Service.”

At completion of the Adjust procedure disable the “Service” menu through the UTILITY front panel button, the “Service” option button, and the “Service” Mode Off” option button.

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK

Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #33 on:** July 23, 2014, 04:52:31 pm »

24C1024W serial EEPROM 128K x 8

Aha! I wondered why I never spotted a smaller EEPROM even after suspecting there must be one.

« *Last Edit: August 12, 2014, 07:30:37 am by KK* »

Report to moderator Logged

KK

Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #34 on:** July 25, 2014, 08:34:19 am »

Since yours is already apart, can you read the memory and post it.

Meanwhile, I am reverse engineering the front panel code and matching it up to the key identifiers to figure out what key combo will get us into Engineering Mode.

The code is interrupt driven and creates jump tables at runtime in ram so it is a mess. The beauty of VXWORKS.

« *Last Edit: August 12, 2014, 07:31:12 am by KK* »

Report to moderator Logged

tautech
Super Contributor

Posts: 14799
Country:

Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #35 on:** July 25, 2014, 09:03:24 am »
Say Thanks Reply Quote

Sorry I do not have any sniffing gear.
Been wondering about getting some, what do you recommend to start with?

As far as I can tell, the 3 interconnect leads will have enough length to power up scope disassembled.
Just checked, it is no problem for the 3 leads.
Then access is easy.
You may have to add a GND lead, but probably not for your needs.

There is only a few screws and all the knobs just pull off.
Service manual describes full dis-assembly. I don't remember it being difficult at all.

I can send you the manual, PM me with your email.
« *Last Edit: July 25, 2014, 09:18:37 am by tautech* »
Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #36 on:** July 25, 2014, 09:55:14 am »
Say Thanks Reply Quote

I pulled the knobs and keys but then I noticed I would have to pull all the bnc's mounting hardware off too and just called it a night and pit it back together.

I'll work some more on the code angle.

The tll866a with an 8 pin soic clip will work without any hassle. It supports the memory and the clip means no wire mods.

Report to moderator Logged

KK
Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B series hacks
« **Reply #37 on:** July 25, 2014, 12:22:23 pm »
Say Thanks Reply Quote

Quote from: tinhead on July 18, 2014, 09:55:40 am

> what you doing is the wrong way, the firmware is for all models, so it does not matter what inside (unless you wish to search the whole firmware for model checks and patch it then). The best way is to patch the model itself, and this has been saved somewhere. The RTC clocke does have some user bytes, but htey can't be used (without special tricks) to store model. Are there any eeproms on the board? i bet the altera cpld is readback protected, but well, just try to dump it. If the model check is really in that cpld (and not eeprom) then it is still possible to change it, e.g. by watching the bus for call just before model check in fw, and then sending the crafted info back. When eepom used, then it will be much easier. Or even simple tricks like some "not populated" parts, TEK did that on other models and one can hack them very easy (which still did't change anything, without calibration mainly useless - and to run cal one need anyway some gears, so ppl who can calobrate have enought money anyways to buy higher TEK models).

Hi Tinhead,

You have a great reputation here. I appreciate your interest and response.

Your thoughts are interesting, especially the parts not installed and patching the device itself.

I'm an experienced MC68000 assembly programmer, so I thought it would be fun to dive into the firmware.

Not many products use the 68000 these days. But, the fact they used VXWORKS complicates everything. The code is mostly unlabeled and jump tables are obfuscated by VXWORKS, not on purpose I think.

There is a small i2c EEPROM. That's where the interesting things are stored. I am working that angle, but enjoyed the disassembly. It brought back old memories of 68K code
« *Last Edit: July 25, 2014, 12:27:17 pm by KK* »
Report to moderator Logged

KK
Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
« **Reply #38 on:** August 10, 2014, 02:25:18 am »
Say Thanks Reply Quote

I disassembled the scope again and dumped the i2c eeprom. It contains the boot code for the Cypress USB controller. No config/calibration data.

The memory map so far-

000000-00FFFF RAM 64K Cypress?
010000-010FFF Memory mapped I/O?
011000-012FFF Altera Max II CPLD?
013000-0FFFFF RAM?
100000-1FFFFF Unreadable/Privilege Exception
200000-3FFFFF Ram Spansion 48lC2m3202?
400000-56BEE4 Flash memory main
56BEE5-7FFFFF Empty but is reserved for Flash memory
800000-FFFFFF Unreadable/Privilege Exception - End of addressable memory

Being a 68000, maximum address space is 16MB. But, it appears only the first 8MB has been used.

To get into Service mode requires two simultaneous key presses. Engineering mode will likely be similar, as there is code to support two simultaneous key presses, but not three. Although the hardware register shows that it can at least see up to 4 simultaneous presses.

Each key is assigned a base code, and the code is +1 if the key is held. Key codes are spaced out by 2.

Knobs are memory mapped. The memory locations for each knob (2 channel scopes have 8 knobs) store a #$FF if they are turned to the right and a #$01 if turned to the left.

The Altera CPLD has 8K of user flash. It is possible the model config, serial number, and calibration data is stored there. In fact, it is likely. There is some code to suggest the serial number is stored in the ADG522 chip which is totally undocumented. So that is one other place.

Getting in through the OS is still the ideal way if possible.

Tautech- Can you take Hires photos of your key matrix. Particularly the traces so I can see how the matrix is setup compared to a two channel scope.

« *Last Edit: August 11, 2014, 06:29:05 am by KK* »

Report to moderator Logged

tautech

Super Contributor

Posts: 14799
Country:

Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #39 on:** August 10, 2014, 05:36:50 pm »

KK, image sent to your email(5MB)

TDS2012B Front panel.jpg (48.04 kB, 448x336 - viewed 542 times.)

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK

Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #40 on:** August 11, 2014, 06:32:12 am »

At this point I have documented much of the boot process, and can probably just patch the firmware where it gets the model id, and force a bandwidth upgrade.

I will use that option last and would still like to figure out how to enter engineering mode.

Making a custom firmware isn't such a bad option though since it would only patch a couple of bytes and these models are long in the tooth now and Tek isn't likely to issue any future firmware updates.

Report to moderator Logged

nctnico

Super Contributor

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #41 on:** August 11, 2014, 07:14:55 am »

If you can force a bandwidth upgrade it would be nice to see if it has any effect. Maybe the board needs some component changes as well.

Report to moderator Logged

Posts: 16828
Country:

There are small lies, big lies and then there is what is on the screen of your oscilloscope.

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #42 on:** August 11, 2014, 07:20:36 am »

Quote from: nctnico on August 11, 2014, 07:14:55 am

> If you can force a bandwidth upgrade it would be nice to see if it has any effect. Maybe the board needs some component changes as well.

It looks like the boards are identical for bandwidth options and even the 1000B and 2000B series boards appear identical.

The display module is color on the 2000B series but the Firmware is identical.

Report to moderator Logged

tautech
Super Contributor

Posts: 14799
Country:
Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #43 on:** August 11, 2014, 06:04:15 pm »

Quote

> I will use that option last and would still like to figure out how to enter engineering mode.

I wonder if any ex-Tek members could contribute by way of PM?

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor
Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #44 on:** August 12, 2014, 01:18:58 pm »

Quote from: tautech on August 10, 2014, 05:36:50 pm

> KK, image sent to your email(5MB)

Thanks for that! It helped me fill in some unknown key codes. Notice the Ref/menu button is silkscreened as Power App. On the TPS series scopes that button is labeled Application.

We should be able to activate the power application in these scopes as the code is all there. Of course, the TPS has battery operation so doing some of the measurements would require an isolation transformer on the TDS non-battery operated models.

Keycodes

Bezel 1-4
3A
3C
06
08
0A

0C Probe check
04 Print

12 Autorange
14 Ref/menu - Power App
16 Save/Recall
18 Utility
1A Measure
1C Cursor
20 Acquire
2C Display
2E Help

30 Default Setup
44 Autoset
46 Single Seq
48 Run/stop
4A Trigger Menu
58 Set to 50%
5A Force Trigger
5C Trigger View

Knobs
08 General purpose
09 Ch1 Pos
0A Ch2 Pos
0B Ch1 Volts
0C Ch2 Volts
0D Horz
0E Horz POS
0F Trigger Level

Report to moderator Logged

tautech
Super Contributor

Posts: 14799
Country:

Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #45 on:** August 12, 2014, 02:45:26 pm »

How are the key codes derived from Ch1 Volts, Ch2 Volts, and Horz ?
I realize all other buttons/knobs can be pushed, but these 3 can only be rotated L or R.

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

KK
Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #46 on:** August 12, 2014, 05:59:21 pm »

The key codes come in through a memory mapped register at:

0x000A8A04

The button id is the value listed or +1 if held. That's why the button ID's are spaced by 2.

I should have been clear on the knobs, they are individually memory mapped.

The base address is:

0x000A8Axx (where xx is the code for the knob)
#$FF is stored in that location if the knob is turned to the right
#$01 if turned to the left

Might be modified by 1 if (+/-) if pushed and 2 if held. But haven't confirmed that.

I don't actually have the key codes for knob presses, but I likely don't care. What I wanted to derive is the Autoset button which your picture helped me get.

I need to look in the disassembly where the two key codes #$44 and #$46 are checked because that is how you get into service mode. I expect the code to get into Engineering to be very close to that.

The Peek/Poke utility in Service mode is crippled. Peek works, but Poke does not allow writes. Looking in the disassembly there is some way to make Poke work and it gives a warning about "Write enabled, use caution". If you try to use poke, it says "Denied".

If I can get into Poke then I could conceivable set the bandwidth flag to give 200mhz bandwidth for that powered session. Not ideal, but it would help speed along where to patch the firmware if I end up going that route.

This is one of those projects, where the target is zero'd in on slowly every day or two, with some leaps and then bingo.

« *Last Edit: August 12, 2014, 06:01:43 pm by KK* »

Report to moderator Logged

EduardoLM
Contributor

Posts: 19
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #47 on:** October 14, 2015, 04:03:19 am »

Sorry to revive this old thread, but I just found it, it's VERY interesting, and I would love to see this puzzle solved. Did you have any progress KK?

I own a TDS1001C-30EDU, perhaps the most crippled one on the TDS series: only 30MHz. I can open, take pictures of it and / or make tests to help you on this mission!

Hope to hear from you, thanks!

Eduardo

Report to moderator Logged

KK
Regular Contributor

Posts: 99
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #48 on:** October 22, 2015, 10:42:25 am »

Can't say I made any more progress as other projects caught my attention, but would like to revisit one day for fun as the 68000 CPU is one of my favorites.

Report to moderator Logged

dav
Regular Contributor

Posts: 133
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #49 on:** May 15, 2016, 08:10:19 pm »

If you should find how to entering the engineering mode, please post it on the forum!

Report to moderator Logged

harm
Contributor

Posts: 5

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #50 on:** November 28, 2016, 07:40:57 pm »

Hi,
Any more news for TDS1000-2000 series hacks?

I've a TDS1002 scope with broken (monochrome) display. I want to replace/install color display. Will it work without 'hacking' the TDS1002 scope to TDS2002 and only wire the color display the right way (18pin mainboard to 15-pin display connector)?

Anyone done this before?

Report to moderator Logged

tautech
Super Contributor

Posts: 14799
Country:

Taupaki Technologies Ltd. NZ
Siglent Distributor

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #51 on:** July 16, 2017, 03:40:30 pm »

> **Quote from: dav on May 15, 2016, 08:10:19 pm**
> If you should find how to entering the engineering mode, please post it on the forum!

In this new thread:
https://www.eevblog.com/forum/testgear/tds-1000-2000-3000-bw-hack/

Report to moderator Logged

~~Avid~~ Rabid Hobbyist

braikin
Contributor

Posts: 7
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #52 on:** March 01, 2018, 01:58:54 pm »

The process in that thread didn't work for me (TDS2004B), but I was inspired to try looking at the firmware myself. Here's some of what I found, that might help people still stumbling upon this thread.

1. The model id is stored at the end Flash ROM along side the calibration data. Here's a bit of python which would patch the ROM if you're willing to desolder and re-program it. Based on observations others have made about the hardware, and the way the code branches based on model number, this will probably work. I used a TL866 to read the rom, but haven't tried programming (see #2).

```
with open('ROM.BIN', 'rb+') as patchedfw:
    # Model IDs
    #
    # 0x0B = TDS2022B
    # 0x0C = TDS2024B
    # 0x0D = TDS2002B
    # 0x0E = TDS2012B
    # 0x0F = TDS2014B
    # 0x10 = TDS2022B 1GS/s
    # 0x11 = TDS1002B
    # 0x12 = TDS1012B
    # 0x13 = TDS1001B
    # 0x14 = TDS2004B

    patchedfw.seek(0x7f0007)
    # Update model per list above.
    patchedfw.write(bytearray([0xf]))

    # Update Checksum
    patchedfw.seek(0x7f0004)
    data = patchedfw.read(0x9f2)
    bytes = [ord(b) for b in data]
    csum = pack(">I", sum(bytes))
    patchedfw.seek(0x7f0000)
    patchedfw.write(bytearray(csum))
```

The address references above are the physical addresses in ROM. They're mapped differently by FPGA in firmware. If you want to peek/poke from service menu, nvram starts at 0x002f0000.

2. Looking at the code, upgrading from any sample rate to another (e.g. 1GS/s to 2GS/s) will definitely result in an uncalibrated scope. Address 0x42b340 is start method which loads cal data. The very first branch in the method matches 2GS/s models and expects the cal data to be a few bytes longer.

I don't have the capability to fix cal, so I'll probably abandon further research like finding a way to do this which doesn't require ROM removed.

Report to moderator Logged

braikin

Contributor

Posts: 7

Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #53 on:** March 03, 2018, 11:11:49 am »

Cal issue is resolved, I'll patch my ROM. If I don't break anything soldering, I'll report back what happens in a couple days.

Cal data was organized into blocks. I had a thought autocal probably manages some of these blocks too:

```
[factory addr=0x7f0000 sz=2546 csum=0x48242,
 spc addr=0x7d652c sz=1564 csum=0x1bc53,
 trig_fpc addr=0x7d0000 sz=396 csum=0x11750,
 fiso_fpc addr=0x7d01c2 sz=11088 csum=0x15232b,
 fiso_fpc_peak_detect_5US addr=0x7c0000 sz=11088 csum=0x14bae7,
 fiso_fpc_peak_detect_10US addr=0x7c2b8e sz=11088 csum=0x16344a,
 fiso_fpc_peak_detect_25US addr=0x7c571c sz=11088 csum=0x158a91,
 fiso_fpc_peak_detect_50US addr=0x7c82aa sz=11088 csum=0x160cb1,
 fiso_fpc_peak_detect_100US addr=0x7cae38 sz=11088 csum=0x15a601,
 fiso_ch1_sample_offset addr=0x7d3d54 sz=2673 csum=0x1e307,
 fiso_ch2_sample_offset addr=0x7d493e sz=2673 csum=0x105c,
 fiso_ch1_pkdet_offset addr=0x7d2d50 sz=1980 csum=0x3d7d1,
 fiso_ch2_pkdet_offset addr=0x7d3552 sz=1980 csum=0x325,
 fiso_ch1_pkdet_lkup_corr addr=0x7d5528 sz=1980 csum=0x3dc38,
 fiso_ch2_pkdet_lkup_corr addr=0x7d5d2a sz=1980 csum=0x3d71a,
 trig_fpc_2 addr=0x7e0000 sz=396 csum=0x12bd9,
 fiso_fpc_2 addr=0x7e01c2 sz=11088 csum=0x129b8a,
 fiso_fpc_2_peak_detect_5US addr=0x7d6d60 sz=11088 csum=0x132c93,
 fiso_fpc_2_peak_detect_10US addr=0x7d98ee sz=11088 csum=0x13408d,
 fiso_fpc_2_peak_detect_25US addr=0x7dc47c sz=11088 csum=0x132590,
```

```
fiso_fpc_2_peak_detect_50US addr=0x7e6590 sz=11088 csum=0x1307bf,
fiso_fpc_2_peak_detect_100US addr=0x7e911e sz=11088 csum=0x12e5b2,
fiso_ch3_sample_offset addr=0x7e3d54 sz=2673 csum=0x47bef,
fiso_ch4_sample_offset addr=0x7e493e sz=2673 csum=0xf97,
fiso_ch3_pkdet_offset addr=0x7e2d50 sz=1980 csum=0x9e6d,
fiso_ch4_pkdet_offset addr=0x7e3552 sz=1980 csum=0x184af,
fiso_ch3_pkdet_lkup_corr addr=0x7e5528 sz=1980 csum=0x3d78f,
fiso_ch4_pkdet_lkup_corr addr=0x7e5d2a sz=1980 csum=0x3f20e]
```

The 4 sections who's size change when upgrading to 2GS/s are `fiso_ch?_sample_offset`. I did an auto cal, and observed checksum changed for those.

Report to moderator Logged

braikin
Contributor
Posts: 7
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #54 on:** March 04, 2018, 09:33:32 am »

Success!?

Software identifies as a TDS2024B everywhere I could think to check. I *think* I see more HF noise. FFT modes at 2GS/s work. 2.5ns/div works. If there's a test you'd like me to try, and I have the equipment, I don't mind giving it a try.

Obviously desoldering the the ROM isn't the easiest solution, but if you'd like to try it:

- Update to the latest firmware. V22.16. This may not be required, but this is the version I reverse engineered. Earlier firmware may or may not work.
- Desolder the ROM, dump its contents to a binary file.
- Keep a backup of the ROM file. If something goes wrong, you can only restore your unit to old firmware if you have a copy.
- Download the attached patch.py.
- If you're patching a 2ch model, change rom.write(bytearray([0x0c])) to rom.write(bytearray([0x0b])).
- Don't try to patch to an impossible configuration. You'll be left with a brick and required remove ROM and retry. Don't use a model with a different number of channels, don't user a model with a color display if you have black-white. If you make a mistake, the scope won't boot.
- Use patch.py to update your firmware, then reprogram.
- When you boot up the first time, Auto Calibration self test will fail. This isn't a problem. Just Auto Cal the scope, then cycle power.
- You're done.

Tips:

- Save a backup of old ROM, so you can rollback if needed.
- Three LEDs in upper left should light up as soon as you power on scope. If they don't maybe ROM isn't soldered well.
- If you've flashed an incompatible model number, you'll get stuck at the 3 LEDs.

img2.jpg (164.73 kB, 1035x776 - viewed 511 times.)

img1.jpg (87.22 kB, 969x727 - viewed 419 times.)

patch_tds1k2kb_rom.py.txt (1.02 kB - downloaded 145 times.)

Report to moderator Logged

braikin
Contributor
Posts: 7
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #55 on:** March 04, 2018, 11:51:13 am »

Last update... unless I find out more. I'm trying to measure rise times to confirm 200mhz. Generously, the best rise times i'm seeing are > 3ns implying < 100mhz.

Changing the Product ID doesn't seem to have increased bandwidth but did seem to enable 2GS/s. Maybe there's a small hardware difference in frontend, but that's beyond my skill to figure out. Also, the `factory` section of cal which contains stuff like: model id, serial number, etc, is about 2.5 kbytes. There may be other values that need manipulation. I'll poke around firmware a little more.

Report to moderator Logged

braikin
Contributor
Posts: 7
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #56 on:** March 05, 2018, 01:51:22 pm »

According to the service manual models are required to be calibrated with a sine wave matching their respective bandwidth. Upgrading software doesn't change the fact the hardware is still calibrated to -3db @ 60mhz? Effectively cal data is limiting bandwidth? Seems like tinhead implied this early in the thread?

What the software change did do: my scope now expects a 200mhz signal during cal. So, I guess the next step is to recalibrate (if that were possible).

If I can get a crude signal source I may try out of curiosity. Calibration is reversible as long as my NVRAM survives another desoldering.

Report to moderator Logged

texaspyro
Super Contributor
Posts: 1219

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #57 on:** March 05, 2018, 02:17:34 pm »

> **Quote from: braikin on March 05, 2018, 01:51:22 pm**
>
> If I can get a crude signal source I may try out of curiosity. Calibration is reversible as long as my NVRAM survives another desoldering.

Geeeeeez, put it in a socket!

Report to moderator Logged

braikin
Contributor
Posts: 7
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #58 on:** March 14, 2018, 01:08:59 pm »

Success!

I'm now seeing rise times ~2ns which is consistent with 200mhz.

Attached is an updated python script to patch more data in NVRAM cal section. This script should work correctly with 2 and 4 channel color models upgrading them to 200mhz 2GS/s. Upgrading non-color models is possible, but not all the way to 200mhz. See my previous post for instructions just use this script instead (and there's no need to edit it).

Basically some of the bytes in factory cal section are used to program a low pass filter of some sort. It looks like They're calibrated to get a consistent attenuation across all channels and vertical scales. Instead I just set the filter to max. So... I may get more inconsistency between channels and vert scales, but it works. I think a full cal would be better but after a couple days on ebay I can't find an affordable way to do that.

If you're interested; the function `cal_bwl_setup` is defined in FW at addr 0x437230. This function programs the LPF between 20mhz and full bandwidth. The values it writes to the LPF are stored in the factory cal section. Bigger values = more bandwidth. My patch sets them to 0x0f which is the largest allowed value for 200mhz. There's on value per channel and vert scale; and like a say above they vary slightly. My scope probably performs a little less consistent.

Good to bring some life back to my old scope! I hope I don't find anymore issues. Digging any further into what the calibration bytes to would be tough.

I feel like I'm talking to myself in an 5 year old thread. If you're interested in how this applies to non-color models, or you have some tests I should try... feel free to let me know.

patch_tds1k2kb_rom.py.txt (1.82 kB - downloaded 206 times.)

Report to moderator Logged

Argiros
Contributor
Posts: 10
Country: 00

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #59 on:** April 30, 2018, 07:42:54 am »

I am glad that you made it! Maybe I give it a try later.
I want to say that I make a BW model to a color. I figure out the pinouts and after many search I finaly did it. I saw the red the cyan all the colors.
Unfortunately my color lcd had two spots it came with that and I put again my b/w lcd. But I finaly did it. I ordered a new color lcd and finaly i will have a color model!

20180429_140634.jpg (262.52 kB, 2048x1152 - viewed 478 times.)

Report to moderator Logged

braiden
Newbie
Posts: 3
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #60 on:** May 01, 2018, 11:36:52 pm »

Wow, nice work making the color display work!

Its good to know your scope works after the upgrade. It means what I've done here should work for b/w models too. I wasn't sure it would, when I accidentally programmed a model id with a channel count mismatch i got a brick. Sounds like display mismatch is more forgiving.

I still haven't been able to find affordable hardware to do a cal, but I did pick up a 500mhz freq synthesizer. Results are: frequency response is not as flat as i'd like. Everything's good through the original 60mhz. After that the sin wave amplitude creeps up (as high as 125%) before coming back to 100% at 350mhz and dropping off pretty sharply after that.

If there's interest in what you'll get with the hack I can draw a bode plot. With caveats: I assume my signal source is level (spec is +/- 0.5db). I'm using cheap cabling and termination, maybe that's adding some induction(?).

I'd like to play with the attenuation setting in cal more, but the socket i got for rom doesn't fit.

Report to moderator Logged

braikin
Contributor
Posts: 7
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #61 on:** May 15, 2018, 11:07:03 am »

For what its worth, here's a plot of a nominally 3 VPP sin wave from 1-499mhz. Different test setups result in very different results. I'm using the stock P2220 probe with a BNC tip adapter plugged into a 50 Ω passthru terminator connected directly to signal source output.

newplot.png (25.74 kB, 700x450 - viewed 291 times.)

« *Last Edit: May 15, 2018, 11:13:06 am by braikin* »

Report to moderator Logged

oaba
Newbie
Posts: 4
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #62 on:** July 20, 2018, 12:42:16 am »

I have an TDS2002. I got the firmware out of flash Am19DL162 . How can I find the model numbers? Hence the different firmware and flash size. Or dou you have firmwares to compare?
Thanks in advance.

Report to moderator Logged

braiden
Newbie
Posts: 3
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #63 on:** July 20, 2018, 12:56:59 am »

I've only looked at TDS2002B, not the TDS2002 which may be totally different? If you're looking at a non-B model, there is this thread: https://www.eevblog.com/forum/testgear/tds-1000-2000-3000-bw-hack/

If its a "B" model, the model id is at 0x7f0007 in the physical ROM dump, and you should expect to find 0x0D corresponding to TDS2002B. Other model numbers are documented in patch_tds1k2kb_rom.py.txt linked above.

Within the "B" series there are no firmware differences between modules, they all run the same binary, the only relevant difference is the model and calibration data stored at the end of ROM, 0x7f0000 and 2546 bytes long.

Report to moderator Logged

vanbac
Contributor
Posts: 5
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #64 on:** August 20, 2018, 05:48:23 pm »

Quote from: Argiros on April 30, 2018, 07:42:54 am

> I am glad that you made it! Maybe I give it a try later.
> I want to say that I make a BW model to a color. I figure out the pinouts and after many search I finaly did it. I saw the red the cyan all the colors.
> Unfortunately my color lcd had two spots it came with that and I put again my b/w lcd. But I finaly did it. I ordered a new color lcd and finaly i will have a color model!

hello you.
modele: Tds1012b mono.
I see you've made a successful switch form screen color can you give me detailed instructions how to do thank you

Report to moderator Logged

clodnut
Newbie
Posts: 2
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks

Say Thanks Reply Quote

« **Reply #65 on:** September 06, 2018, 04:36:29 am »

Thanks for your work on this, braikin.

Your efforts have given my aged TDS1001B (Mono, 2 Ch, 40 MHz, 500 MS/s) a new lease of life as a 100 MHz TDS1012B.

5 ns/division scaling has become available and FFT mode confirms 1 GS/s acquisition.

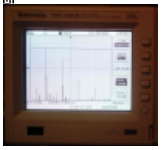
I tweaked your Python code to handle model ID 0x13 -> 0x12 for the TDS1000B series. Your approach of clearing the LPF settings seems to work for the TDS1000B-series, whose max. bandwith is 100 MHz rather than 200 MHz like the TDS20xxBs.

I don't have the kit to measure the new bandwidth properly but the stock probe and a Rasberry Pi outputting a square(ish) wave gives a 2.12 ns rise time, suggesting comfortably over 100 MHz bandwidth.

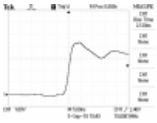
The calibration seems fine by eye (no weird offsets or dodgy scaling cycling through various ranges) but, again, I'm not set up to do a full cal.

Thanks again!

patched.jpg (73.08 kB, 1620x1440 - viewed 264 times.)



1gsps.jpg (87.37 kB, 1556x1436 - viewed 233 times.)



2.12nsrt.png (3.83 kB, 320x240 - viewed 230 times.)
patch_tds1k2kb_rom.py.txt (1.94 kB - downloaded 102 times.)

Report to moderator Logged

vanbac
Contributor
Posts: 5
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #66 on:** September 09, 2018, 11:56:33 am »

hello clodnut.
Congratulations you've successfully upgraded can you guide me the steps to upgrade on YouTube thank you very much.

Report to moderator Logged

DogP
Contributor
Posts: 34
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #67 on:** October 25, 2018, 08:30:07 pm »

Quote from: tautech on July 16, 2017, 03:40:30 pm

Quote from: dav on May 15, 2016, 08:10:19 pm

If you should find how to entering the engineering mode, please post it on the forum!

In this new thread:
https://www.eevblog.com/forum/testgear/tds-1000-2000-3000-bw-hack/

I didn't see engineering mode in that thread... did I miss it? In the case of the TDS 3000, the TDS3ENG hack is totally different, as it unlocks the available modules. The TDS 1000s and 2000s didn't have those modules, and instead "Engineering Mode" looks to be an option in the menu (similar to Service Mode).

Any further progress on any TDS 1K/2K stuff? I used to have one of these on my desk at work, and I just bought a 2024B for home. Not the best scope I've ever used, but nice and doesn't take up a lot of bench space... and the deal was too good to pass up. Since it's already the highest freq/sample rate 2024B, I guess there's no possible "upgrade".

I sifted through the firmware binary, and it looks like there are still some interesting mysteries to unlock. Maybe not all of them are important - engineering mode (doesn't look that interesting), the code to enable memory pokes from service mode (again, probably not very useful)... but how about the section with "A:\PAUL", "\GEORGE", "\RINGO", "\JOHN", and "A:\POLLY\LITHIUM". If I create one of those directories does it load up an XY plot of a Beatles or Nirvana album?

DogP

Report to moderator Logged

bootboot
Contributor
Posts: 6
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #68 on:** November 06, 2018, 08:45:12 pm »

Hi! Can you share me the backup ROM file?
My TDS2022B Can not bootup, it dead at 3 LEDs light.

Report to moderator Logged

vanbac
Contributor
Posts: 5
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #69 on:** December 08, 2018, 01:43:28 am »

Hello please help me I want to upgrade the bandwidth but I read data of ROM thank you.

1.jpg (759.37 kB, 2048x1536 - viewed 166 times.)


2.jpg (328.26 kB, 2048x1536 - viewed 133 times.)


3.png (205.34 kB, 1427x717 - viewed 140 times.)

BACKUP TDS2002B.BIN.txt (128 kB - downloaded 47 times.)

« *Last Edit: December 08, 2018, 01:50:19 am by vanbac* »

Report to moderator Logged

clodnut
Newbie
Posts: 2
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #70 on:** December 09, 2018, 07:23:06 am »

U902 is not the firmware flash -- it's just an I^2C EEPROM, apparently containing the boot code for the USB controller (according to this earlier post).

You will need to remove the S29JL064H flash memory chip, typically designated U801.

It's the one pictured in this post earlier in this thread. It's the chip with the label in the top left of the board shown in this post.

Then you need to read the chip, patch it using braikin's Python script and re-solder it into the scope.

Good luck!

Report to moderator Logged

vanbac
Contributor
Posts: 5
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #71 on:** December 11, 2018, 03:24:01 am »

Thank you for the tutorial, please wait my results.

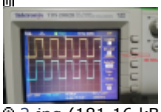
Report to moderator Logged

vanbac
Contributor
Posts: 5
Country:

Re: Tektronix TDS1000B and TDS2000B series hacks
Say Thanks Reply Quote
« **Reply #72 on:** January 04, 2019, 05:58:32 pm »

thanks "clodnut" very much, i have upgraded the bandwidth, this is my model.


1.jpg (163.7 kB, 942x606 - viewed 181 times.)


2.jpg (181.16 kB, 966x606 - viewed 144 times.)

Report to moderator Logged

Pages: 1 2 3 [**All**] **Go Up**

REPLY NOTIFY MARK UNREAD SEND THIS TOPIC PRINT SEARCH

« previous next »

EEVblog Electronics Community Forum » Products » Test Equipment » Tektronix TDS1000B and TDS2000B series hacks

LINK TO CALENDAR

Jump to: => Test Equipment ▼ go

Quick Reply

EEVblog Main Site EEVblog on Youtube EEVblog on Twitter EEVblog on Facebook