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.
November 05, 2021, 03:00:35 pm

| | This topic ▾ | Search |

News:
No news is good news. Be excellent to each other.

🏠 Home   ❓ Help   🔍 Search   👤 Profile   About us   ✉ My Messages   📅 Calendar   Links   👥 Members   ⊖ Logout

EEVblog Electronics Community Forum » Products » Test Equipment » Search » Search Results

🌐 Search results for: how to

Pages: [**1**]

1 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
    « Message by **smgvbest** on *November 22, 2020, 04:33:33 am* »

Quote from: hpls on November 22, 2020, 04:08:44 am

Hi
I have an e4403B, I would like **to** start activating the option 049 color display ...
I tried **to** follow these steps but I believe I am doing something ...
can someone detail the steps more?
I'm using Putty as a serial moni**to**r ...
I can make the morning calls until 9 ...

doing this procedure I need **to** do what else?

My steps:
0. Set the serial terminal **to** 19200,8n1
1. DIP sw # 4 set **to** ON
2. break the boot process with 0x06
3. sword 04139614 4ef9
4. sword 04139618 d8a4
5. DIP sw # 4 set **to** OFF
6. gu
7. SA restart in normal mode
8. Press "r" and we are in the moni**to**r now 😎
9. Change the serial port speed.
> slong 815F4 1001A
10. Change speed of the serial terminal **to** 115200, 8n1

---

does you SA actually have a Color Display?
depending on the Unit some where not shipped with a Color Display and hence the need for Opt 049 when installing a color display
if you have a color display and its not s**how**ing color then you need **to** create a license for 049,   information of which is in this
thread on **how to** do

                                                                              Reply   **Quote**   **Notify**

2 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **mankan** on *November 20, 2020, 08:44:40 pm* »

Many thanks PA0PBZ, now have a updated option 227 **to** A.02.08 and latest version of J25/J36 B01.02. A friend reminded me that I have a oscilloscope running Windows 98. HP54820A FTW 😁

I tried 2 browsers myself, Firefox and Chrome on Windows 7. **How** did you succeed?

So now I'm just lacking the 226 Phase noise.

Regarding J35/J36: I could install both, but I ended up keeping the J35/J36 B.01.02 version since its newer and it seems option J36 is included in J35 newer versions which requires extra memory A72. My unit reports personality J35 as installed but reports no name for its J35 license. **How**ever J36 license is still installed and reports FM deviation.

                                                                              Reply   **Quote**   **Notify**

---

3 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **analogRF** on *September 30, 2020, 06:58:11 pm* »

let me pose a fresh and more useful and interesting challenge with regard **to** these analyzers:

how can we convert E4404B (6.7GHz) **to** E4405B (13.2GHz) if at all?

All boards and modules including the critical ones (attenua**to**r and RYTHM) are common between these two
so the frequency must be limited by software only

of course calibration after such upgrade is a must and can pose a problem since the cal procedure is not possible by hobbyist

but still it would be awesome 😁

                                                                              Reply   **Quote**   **Notify**

---

4 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **xymox** on *September 24, 2020, 04:18:19 am* »

Yea I have been thru the "calibration" guide.. Hehehe.. Im still not sure **how to** set Course and Fine in the timebase in the service menu..

I do have something off on both my units. If I give them my rubidihum clock std 10Mhz it displays slightly off center if I set the SA for 1hz res bw and 100 hz span. Also the freq counter is off a bit..

Amplitute is reading slightly off at various frequency points.

These are not much off, but with this many years on these devices, its normal **to** have drift.

Also if we want **to** swap boards around between units and maintain these over the next 10 years we just gotta be able **to** calibrate them.

These calibration adjustments must also be kept in some flash. If the flash goes or gets wiped, thats it. No hope of recovery.

We gotta be able **to** do TME.. I can't find old versions of TME. Or maybe some old different program used **to** calibrate.

I have sent a nice email **to** Ron Nersesian. He has a awesome career that goes way back with HP. Back **to** the good old days of HP. I have suggested that hobbyists fuel young engineers and so thier future cus**to**mers could well be buying this older gear from ebay. i suggested its helpful for EoL devices that are locked away with keys **to** maybe get a free online key gen process. This would fuel many hobbyists in**to** engineers and maybe future cus**to**mers. It wont hurt Keysight sales as hobbyists cannot afford **to** buy new gear and companies using this kind of test equipment don't buy old gear like this.

Im sure I wont get a response. BUT the email did not reflect back. So I did find the right email **to** use for him.

WTH... Why not try...

BTW the self calibration license has provisions for a single serial number instrument. That would have **to** be way cheaper then a single seat.

Maybe I can get a trial license. If so, I can capture all the GPIB..AND calibrate my unit at least once..

                                                                              Reply   **Quote**   **Notify**

---

5 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **smgvbest** on *September 24, 2020, 03:45:43 am* »

> ### Quote from: xymox on September 24, 2020, 03:26:45 am
>
> > ### Quote from: smgvbest on September 24, 2020, 01:40:07 am
> >
> > BTW: I just started a new thread in the repair forum for repairing the Tracking Genera**to**r thats getting a Source Unlevel error if anyone is interest
>
> You will eventually need **to** calibrate it. We gotta figure out **how to** do that..
>
> I am trying **to** get Keysight **to** simply quote me on TME.. I want a license for "self Maintainers" and for a single serial number unit. They responded once and asked me what the company name was, I **to**ld them it was for personal use and they never responded again. I would pay them for this.. As long as it was not a insane number. BUT they seem **to** be going in the direction that will lead **to** the system getting hacked in**to**. At the least the GPIB stuff that goes back and forth during calibration can be captured and easily figured out. Im going **to** ask one more time.
>
> I want this https://cal.software.keysight.com/?id=2525023 under this license.. https://www.keysight.com/us/en/assets/7018-01623/data-sheets/5989-6956.pdf for 1 unit, a ESA E4402B.. Its supported..
>
> I VASTLY prefer **to** use software legitly. As long as its not **to**o expensive, I am happy **to** pay it.
>
> Keysight seems **to** be unpleasant and stupid.
>
> What they should do is just allow all these **to**ols and things **to** go free. Real businesses are not buying these older devices, hobbyists are. Like me, a Ham radio guy.. They are NOT loosing sales **to** this old gear...
>
> Maybe I need **to** target someone higher up the chain at Keysight..

Keysight is not in business **to** support hobbyist. that's not their business model. for TME you're looking at 5K+ i believe. Hobbyist arent buying these usually either, at a cost of 3K+ for a broken one most hobbyist can not afford that. every now and then you find you for much less. I did, I got very lucky and the repair was simple. the TG may be a different issues. it's been repaired before. I need **to** figure out if the Source Unlevel is the LO Control board (i hope) or the BITG which is not documented

Far as calibration, first run a performance test **to** see if it need **to** be calibrated. All documented in the calibration guide

Reply   Quote   Notify

---

6   **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **xymox** on *September 24, 2020, 03:26:45 am* »

> ### Quote from: smgvbest on September 24, 2020, 01:40:07 am
>
> BTW: I just started a new thread in the repair forum for repairing the Tracking Genera**to**r thats getting a Source Unlevel error if anyone is interest

You will eventually need **to** calibrate it. We gotta figure out **how to** do that..

I am trying **to** get Keysight **to** simply quote me on TME.. I want a license for "self Maintainers" and for a single serial number unit. They responded once and asked me what the company name was, I **to**ld them it was for personal use and they never responded again. I would pay them for this.. As long as it was not a insane number. BUT they seem **to** be going in the direction that will lead **to** the system getting hacked in**to**. At the least the GPIB stuff that goes back and forth during calibration can be captured and easily figured out. Im going **to** ask one more time.

I want this https://cal.software.keysight.com/?id=2525023 under this license.. https://www.keysight.com/us/en/assets/7018-01623/data-sheets/5989-6956.pdf for 1 unit, a ESA E4402B.. Its supported..

I VASTLY prefer **to** use software legitly. As long as its not **to**o expensive, I am happy **to** pay it.

Keysight seems **to** be unpleasant and stupid.

What they should do is just allow all these **to**ols and things **to** go free. Real businesses are not buying these older devices, hobbyists are. Like me, a Ham radio guy.. They are NOT loosing sales **to** this old gear...

Maybe I need **to** target someone higher up the chain at Keysight..

Reply   Quote   Notify

---

7   **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **xymox** on *September 23, 2020, 05:23:07 am* »

Well this software is nearly unusable for my use. For some freaky reason its limited **to** a 10Mhz span no matter what I do. This is comeplty useless for me. At the high freq is useless. Like **how** do you look at wifi ? This limitation seems **to** be with the hardware. I can simulate other devices and they have different max spans, but still not full. Even brand new keysight gear does not do the full span like the actual device will..

Because of this, the software seems crippled for my use.

Reply   Quote   Notify

8   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 19, 2020, 05:06:15 pm* »

Just got back from work,   amazing whats gets done when I am tied up

@tv84
@abyrvalg

you both are awesome!!   thanks for the hard work
I would love **to** have a PM chat **to** understand a bit of **how** you do this, it intrigues me

@suj thank you for your help as well

                                                                  Reply   Quote   Notify

---

9   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 19, 2020, 01:02:54 pm* »

> **Quote from: tv84 on September 19, 2020, 12:51:20 pm**
>
> S**to**p the press! (and the dumps...)
>
> Enc_seeds validated OK!
>
> @suj license correctly validated.
>
> **How** dumb!! **How** could I've missed that structure!!!!

Other than some banging head on wall this sounds good right?
I was just getting ready **to** do the dump

                                                                  Reply   Quote   Notify

---

10   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **tv84** on *September 19, 2020, 12:51:20 pm* »

S**to**p the press! (and the dumps...)

Enc_seeds validated OK!

@suj license correctly validated.

How dumb!! **How** could I've missed that structure!!!!

EDIT: Mystery solved! This proc is BIG ENDIAN and my search function only searches in LITTLE ENDIAN (will correct it)! Sorry all for all the trouble but it was a new experience. A special recognition **to** @abyrvalg. Amazing talent!

                                                                  Reply   Quote   Notify

---

11   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **abyrvalg** on *September 19, 2020, 11:31:57 am* »

Dumping "vendor key 5" should be enough - this is old FLEXlm, the seeds are s**to**red in VENDORCODE xored with this vk5 (look down from the location I'm patching - they verify if the seeds are "demo" 12345678 87654321 by direct xoring with this value. Various tu**to**rials from 6.0 era says the same).

I have an universal recipe **how to** start feeling at home with any CISC asm - spend some time in QDSP (Hexagon) asm

                                                                  Reply   Quote   Notify

---

12   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **tv84** on *September 19, 2020, 11:13:02 am* »

> **Quote from: abyrvalg on September 19, 2020, 11:00:14 am**

@tv84, now I understand why you need such big dumps, your values of interest are local variables with no fixed addresses - right?

Right. 👍🙂 Your suggestion was also on my mind. I hope we don't need it but, if we do, I will need your help. I also need **to** have a full confirmation of what is being hashed and, for that, the dump should provide the definitive answer.

I have a hard time recognizing **how** the registers of this thing work. It's almost like Blackfin! 🙂

Reply   Quote   Notify

13 Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 18, 2020, 03:46:38 pm* »

Quote from: tv84 on September 18, 2020, 02:29:07 pm

> **Quote from: abyrvalg on September 18, 2020, 01:49:30 pm**
>
>> @tv84, any ideas what **to** patch?
>> I'm going **to** prepare some patch **to** jump from ESAFW back **to** ROM Moni**to**r (i.e. with some of the psos debug commands) without reset **to** dump the data section content finally.
>
> I think I can patch the license validation ATM. Although, having some idea of **how** flexlm tests licenses, I don't know what are the consequences of activating all licenses.
>
> I would prefer 1st **to** have the dump, so that I can search for the seeds. If I can find the seeds in the dump, the keygen will be instantaneous.

Do you want the same dump we've had before or a different one?

Reply   Quote   Notify

14 Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 18, 2020, 02:54:58 pm* »

Quote from: suj on September 18, 2020, 02:45:58 pm

> My steps:
> 1. DIP sw #4 set **to** ON
> 2. break the boot process with 0x06
> 3. sword 04139614 4ef9
> 4. sword 04139618 d8a4
> 5. DIP sw #4 set **to** OFF
> 6. gu
> 7. SA restart in normal mode
> 8. Press "r" and we are in the moni**to**r now 😎
>
> Respect for you 👍🙂👍🙂👍🙂

Cool, I wake up and you all have done allot.

@suj **how** are you flipping the DIP SW without removing the Processor Card?
a long stick??? LOL

Reply   Quote   Notify

15 Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **tv84** on *September 18, 2020, 02:29:07 pm* »

Quote from: abyrvalg on September 18, 2020, 01:49:30 pm

> @tv84, any ideas what **to** patch?
> I'm going **to** prepare some patch **to** jump from ESAFW back **to** ROM Moni**to**r (i.e. with some of the psos debug commands) without reset **to** dump the data section content finally.

I think I can patch the license validation ATM. Although, having some idea of **how** flexlm tests licenses, I don't know what are the consequences of activating all licenses.

I would prefer 1st **to** have the dump, so that I can search for the seeds. If I can find the seeds in the dump, the keygen will be instantaneous.

Reply   Quote   Notify

16 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **tv84** on *September 18, 2020, 10:29:45 am* »

> **Quote from: abyrvalg on September 18, 2020, 10:13:48 am**
>
> Interesting, there is a "syscall" **to** execute a single ROM Moni**to**r command from the main app (at 04132418: trap #0E with arg=0A. All "trap #0E" functions are BootROM calls leading **to** handler at D1EC), but I see no refs **to** it.

What about patching one of the ones that we (I mean you! 🙂)know **how to** trigger, like arg=03, 04, 05 ? 🙂

                                                                    Reply   Quote   Notify

---

17 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **abyrvalg** on *September 17, 2020, 07:02:57 pm* »

More info:
"bulk" flash starts from C000000.

How to enter ROM moni**to**r before jumping **to** FW:
BootROM loads ESALOADER (from floppy) or main fw (from bulk flash) **to** DRAM then sends a 05 byte (ascii ENQ char) and waits for 06 (ascii ACK) reply with timeout. If this wait times out - jump **to** DRAM normally, otherwise - bypass jump and enter ROM moni**to**r.

This can be used **to** try patches without flashing them:
- don't insert ESALOADER floppy
- interrupt normal start by replying **to** 05 with 06
- modify firmware in RAM (with smem/sbyte/sword/slong cmds)
- jump **to** modified firmware (with gu cmd)

                                                                    Reply   Quote   Notify

---

18 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **smgvbest** on *September 17, 2020, 04:07:58 pm* »

> **Quote from: suj on September 17, 2020, 02:06:37 pm**
>
> > **Quote from: tv84 on September 17, 2020, 01:02:59 pm**
> >
> > ..Try them in the ESAFW.
>
> I tried. I changed the text on the first floppy disk (first disk of the upgrade, not loader disk). In the menu for the external mixer, I changed the text: "Presel" **to** "11974Q". I started the upgrade. After the last floppy disk was loaded, a message was displayed on the SA screen. Nothing special on the serial terminal.

Well Pooh
So the LOADER must run a cksum on the FW before continuing

That would mean either find that routine in the loader or find **how to** patch the active system I would think

                                                                    Reply   Quote   Notify

---

19 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **smgvbest** on *September 14, 2020, 10:49:40 pm* »

> **Quote from: tv84 on September 14, 2020, 09:13:22 pm**
>
> > **Quote from: smgvbest on September 14, 2020, 08:23:09 pm**
> >
> > Any recommendations on **how to** proceed?
>
> I don't know if the Bootrom is somewhat old and maps the **^C jump address** in a memory place that the ESALOADR A.05.00 knows where **to** find but the ESAFW A.14.06 doesn't (I've seen that both use different addresses, I think). Just a guess... I've tried **to** discover that **to** force the jump but... arghhh. damn language...
>
> The way **to** proceed is **to** try a patch.
>
> Please test if you can flash a patched FW (or live patch the ESAFW). You can test with a string used in any message onscreen.
>
> If you are successful, I think I can craft a special patch.

If you know the address where the ctrl+c code is then I think in the debug menu the gu address command will jump **to** that address???

Maybe we can force it there?

20 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **andrew9875** on *September 14, 2020, 10:08:55 pm* »

Quote from: smgvbest on September 14, 2020, 08:23:09 pm

> Any recommendations on **how to** proceed?

Has anyone looked at the service information for these analyzers? Maybe another vec**to**r we can explore:

DRAM and flash EPROM can be erased by flipping switches on S1 or holding down front panel but**to**ns during boot. Maybe there's some hidden features there...

Reply   Quote   Notify

21 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **tv84** on *September 14, 2020, 09:13:22 pm* »

Quote from: smgvbest on September 14, 2020, 08:23:09 pm

> Any recommendations on **how to** proceed?

I don't know if the Bootrom is somewhat old and maps the **^C jump address** in a memory place that the ESALOADR A.05.00 knows where **to** find but the ESAFW A.14.06 doesn't (I've seen that both use different addresses, I think). Just a guess... I've tried **to** discover that **to** force the jump but... arghhh. damn language...

The way **to** proceed is **to** try a patch.

Please test if you can flash a patched FW (or live patch the ESAFW). You can test with a string used in any message onscreen.

If you are successful, I think I can craft a special patch.

Reply   Quote   Notify

22 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **smgvbest** on *September 14, 2020, 08:23:09 pm* »

Quote from: tv84 on September 14, 2020, 05:17:36 pm

> **Quote from: suj on September 14, 2020, 04:20:43 pm**
>
>> EDIT
>> https://www.eevblog.com/forum/testgear/enabling-options-on-agilent-esa-series-e4402b-e4404b-e4405b-e4407b/msg3228528/#msg3228528
>> should I do according **to** this description (post #120 written by Sandra)?
>
> That method is what she has just tried and doesn't work. It dumps the ESALOADR environment. The reset crushes all the ESAFW previous state.

yeh it was worth a try but its a no-go
it looks like we need **to** find out who **to** get the moni**to**r menu from a normal boot.
You mention though that CTRL+C is disabled in the BootRom? or is it disabled in the ESAFW?
would it be hard **to** patch **to** enable that function?

the other thing is SCPI,   There's suppose **to** be a debug interface (but undocumented) via SCPI and it may be faster than the serial interface.

Any recommendations on **how to** proceed?

Reply   Quote   Notify

23 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by **tv84** on *September 11, 2020, 07:20:50 pm* »

Quote from: smgvbest on September 11, 2020, 07:07:40 pm

> Just **to** be sure we're all on same Page

How do you trigger DEBUG MENU?

For information:

DEBUG MENU is inside ESALOADR

MONI**TO**R MENU is inside BOOTROM   (called from within DEBUG MENU via ^C)

Reply   Quote   Notify

---

24 Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 11, 2020, 02:38:24 pm* »

Quote from: andrew9875 on September 11, 2020, 01:44:50 pm

> **Quote from: tv84 on September 11, 2020, 11:42:08 am**
>
>> Curious. It seems a correct dump BUT from a different memory bank (as if it was possible)...
>>
>> I have **to** take a deeper look.
>>
>> It's not the ESAFW. But I don't have here the rest of the package...
>
> Hmmm. I wonder if this is because ESALOADR is loaded and running.
>
> I think I figured **how to** access the ROM moni**to**r without ESALOADR running:
>
>   1. Boot from ESALOADR floppy, drop in**to** ROM moni**to**r menu (j, CTRL+C)
>   2. Retry test routine ('rty')
>   3. Test routine will fail/hang, then remove floppy and power cycle the unit
>   4. Boot from flash will fail and drop you back in**to** ROM moni**to**r
>
> So far the dump is at least slightly different, just need **to** wait several hours for it **to** complete.

Have your tried the (J, CTRL+C) on a normal boot
that's what we're after, if it will work

anytime loading ESALOADER you won't get ESAFW loaded off flash and executed.
the ideal is
Boot Normally
Get in**to** Moni**to**r
then Dump Memory

probably should let TV84 know your HOSTID and be sure your running 14.06 of the firmware (I know you are, this is more for anyone else who tries int he future)

Reply   Quote   Notify

---

25 Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **andrew9875** on *September 11, 2020, 01:44:50 pm* »

Quote from: tv84 on September 11, 2020, 11:42:08 am

> Curious. It seems a correct dump BUT from a different memory bank (as if it was possible)...
>
> I have **to** take a deeper look.
>
> It's not the ESAFW. But I don't have here the rest of the package...

Hmmm. I wonder if this is because ESALOADR is loaded and running.

I think I figured **how to** access the ROM moni**to**r without ESALOADR running:

  1. Boot from ESALOADR floppy, drop in**to** ROM moni**to**r menu (j, CTRL+C)
  2. Retry test routine ('rty')
  3. Test routine will fail/hang, then remove floppy and power cycle the unit
  4. Boot from flash will fail and drop you back in**to** ROM moni**to**r

So far the dump is at least slightly different, just need **to** wait several hours for it **to** complete.

Reply   Quote   Notify

---

26 Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

« Message by **smgvbest** on *September 10, 2020, 04:03:08 pm* »

Quote from: suj on September 09, 2020, 09:35:49 pm

> **How** do I enter the moni**to**r? Sandra, you wrote about a planned error. **How to** do it?

Cause a error.
I was playing with this before I had the issue om the Processor Board and i think if you put in the ESALOADER disc you can get the Moni**to**r Program that way.
of course this might be a problem for you with the FD issue your having

                                                                    Reply   **Quote**   **Notify**

---

27   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **suj** on *September 09, 2020, 09:35:49 pm* »

OK, I prepared the hardware **to** handle the serial port, set up 19200 8n1. After start, E4407B sends information.

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 5.00
@(#)LDS Rev: 3.02 - Module Incremental (Sep  9 2003)
@(#)Linked: Sep  9 2003 14:46:44

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
        End    = 0xa007fa3
```

How do I enter the moni**to**r? Sandra, you wrote about a planned error. **How to** do it?

I am ready **to** deliver information from my device with the options installed, please just keep in mind that I am not an experienced hacker 🙂
I will also point out that my SA has the A.14.01 firmware installed. Can't install the latest firmware yet, FDD can't read floppy disks reliably. It crashes on 2nd or 3rd disk when trying **to** update. I have **to** look for a new FDD.

EDIT

I'm now motivated **to** solve the FDD problem in my SA. I ordered 2 used SLIM FDD from the local auction site. One type NEC FD3238T and the other Teac FD-05HG. The FDD Teac FD-05HF was originally installed in my E4407B, but I haven't found one. Hope one of them will work well, both have a 26 pin connec**to**r. If they work, I will update the firmware **to** version A.14.06.

                                                                    Reply   **Quote**   **Notify**

---

28   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 09, 2020, 04:05:32 pm* »

Guess what I just found.

This is the moni**to**r program I was after.
to get it i caused an error.   the error was planned, getting the moni**to**r program was not
question will be **how to** get this when loading normally.

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 3.10
@(#)LDS Rev: 3.02 - Module Incremental (Feb 18 1999)
@(#)Linked: Feb 18 1999 11:46:22

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
```

```
Non Destructive SRAM Test ...
Main Firmware DRAM:    Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
    ROM Checksum Failure.  Bad Checksum.  01, 0
Self-tests complete.SRAM selftest results:
```

Serial is at 19.2Kb so dumping memory will be slow but may be doable soon (I hope)
and if you notice the menu you can dump and write memory 👍🙂

Reply	Quote	Notify

29   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 07, 2020, 05:48:07 pm* »

I'm trying **to** figure out **how to** read out the FLASH SIMM without de-soldering the Flash ICs
I've created a map between the LH28F320STKD -> SIMM -> T56 Programmer
There's a few signals that need investigation, **show**n in RED.

mainly the LCS_FLASH (CS Selects), Program Voltage ,RYBY (why are there 6 of these, 3 makes sense) , PA0 (possible tried low) ,PA1 (should be straight thru), byte# (likely tied high)
I'll have **to** ohm out the simm **to** figure out

Ill still have **to** de-solder U74 from the processor board (no way around that)

has anyone ever use JTAG on a 68040?
I dont' see a def for it in OCD
if all you can do is a boundary scan can you access memory or do you need debug for that?

Reply	Quote	Notify

30   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **tv84** on *September 04, 2020, 09:10:49 am* »

> **Quote from: smgvbest on September 03, 2020, 09:15:37 pm**
>
> **how** did you manage **to** get the load address?

Educated trial & error... 🔛🙂

I would like **to** know if there is any way **to** manually upload a license.dat file **to** the instrument? (If this is not possible we can't do an universal license file.)

Also, can anyone provide a printscreen of the license input menu?

Edit: Now that you asked... 🔛🙂 🔛🙂 🔛🙂 🔛🙂

> **Quote from: smgvbest on August 31, 2020, 04:12:44 pm**
>
> Bootrom Checksum ...
> Bootrom DRAM: Testing 69632 bytes at **0x04000000**
> Non Destructive SRAM Test ...
> Main Firmware DRAM: Testing 33484800 bytes at **0x04011000**
> Main FW Checksum ...

Reply	Quote	Notify

31   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **smgvbest** on *September 03, 2020, 09:15:37 pm* »

> **Quote from: tv84 on September 03, 2020, 08:46:24 pm**
>
> Those that want **to** play in IDA with @smgvbest's ESAFW can use these settings:
>
> Proc: Mo**to**rola Coldfire
> Load address: 0x04011000

Is the Mo**to**rla Coldfire same as a M68040?

the Mo**to**rola 68LC040 is the actual processor on the board is why I ask

how did you manage **to** get the load address?

| | **Reply** | **Quote** | **Notify** |

---

32   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **tv84** on *September 03, 2020, 02:41:58 pm* »

Quote from: smgvbest on September 03, 2020, 11:59:58 am

If this does not work the other way I could brute force this is I could remove all of the FLASH memory and read them out with the Xgpro (formerly TL866) reader/programmer.
I have a spare processor card I'm willing **to** experiment on.

This seems the best option. **How** many flash chips are there? Isn't just one?

| | **Reply** | **Quote** | **Notify** |

---

33   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **analogRF** on *September 03, 2020, 10:37:54 am* »

Quote from: tv84 on September 03, 2020, 10:31:32 am

> **Quote from: analogRF on September 03, 2020, 10:28:48 am**
>
> > Another way would be **to** figure out **how to** combine the 9 floppy disks **to** create a single file firmware and then "explore" it 😀
>
> Where are those 9 disks?

on keysight website
https://www.keysight.com/main/software.jspx?
cc=CA&lc=eng&ckey=1000001085:epsg:sud&nid=-32406.536879915.02&id=1000001085:epsg:sud&cmpid=92448

EDIT: i dont have the instrument so I have never gone through the process of making the firmware update. I just know that it creates 9 floppy disks

| | **Reply** | **Quote** | **Notify** |

---

34   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **tv84** on *September 03, 2020, 10:31:32 am* »

Quote from: analogRF on September 03, 2020, 10:28:48 am

> Another way would be **to** figure out **how to** combine the 9 floppy disks **to** create a single file firmware and then "explore" it 😀

Where are those 9 disks?

| | **Reply** | **Quote** | **Notify** |

---

35   Test Equipment / Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« Message by **analogRF** on *September 03, 2020, 10:28:48 am* »

Quote from: xymox on September 03, 2020, 05:43:27 am

Ive done jtag in a bunch of things.. Its not normally what is in your pic ? Maybe that is something else ? OR I am just stupid,, I CAN be that.. Normally its a 4 pin header. +5, tx, rx, gnd.. With ther TTL or RS232 voltages. I will look more at the board shortly..

TX,RX,GND is not a JTAG, it's UART . you dont even need the Vcc necessarily.

this thing has a JTAG interface but i dont think it will be of much help. The content of bootrom is not what we need.
you only need the dump of flash memory **to** access the file system of the main OS, nothing else really. Another way would be **to** figure out **how to** combine the 9 floppy disks **to** create a single file firmware and then "explore" it 😀

| | **Reply** | **Quote** | **Notify** |

---

36 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by *tv84* on *September 03, 2020, 10:22:20 am* »

Quote from: smgvbest on September 03, 2020, 12:41:34 am

> The first item needed is a full dump of the memory.   a dump of one with licensed options would really help.   mine has no licensed options
> flexlm 6.01 which appears **to** be in the update file which I extracted strings from has been hacked and there's articles on **how to** find the different key values.
>
> the part at the moment is **how to** get that dump,   flash and sdram from a running system

---

I don't think flexLM is in the update file. It should be already inside the machine. That's why a flash dump would be great.

The FlexLM version should be no problem. Regarding the places where **to** find the seeds it's not so simple as the several guides don't cover this lang/processor.

	Reply	Quote	Notify

37 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by *smgvbest* on *September 03, 2020, 12:41:34 am* »

The first item needed is a full dump of the memory.   a dump of one with licensed options would really help.   mine has no licensed options
flexlm 6.01 which appears **to** be in the update file which I extracted strings from has been hacked and there's articles on **how to** find the different key values.

the part at the moment is **how to** get that dump,   flash and sdram from a running system
i figured out the JTAG pins and where you can pick them up but JTAG is not something I'm good with

if all you have is a boundary scan ability can you get a dump of memory?
[attach=1]

anyone who can help with that and setting up OCD I'll do it on my ESA
I just need the help

the processor is a 68LC040 I believe (its the LC part i'm not 100% sure of off **to**p of the head)

	Reply	Quote	Notify

38 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by *analogRF* on *August 28, 2020, 12:57:32 am* »

---

all you need **to** do is **to** attach two small grabbers **to** pin9 and pin10 of the MAX232 chip (TTL level) and you are good **to** go. Any cheap UART-USB converter will do the job. I prefer my BUSPirate. That's **how** I have always done this in numerous instruments.

But which RS232 connec**to**r is this? Is it the one at the back of instrument? or is it something just on board for debugging?

Because if it is the one at the back of instrument, you won't get any boot log on that or access **to** the OS

	Reply	Quote	Notify

39 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by *tv84* on *May 20, 2020, 09:51:05 pm* »

Quote from: PA0PBZ on November 11, 2019, 09:17:43 pm

> The method I used **to** get around the FlexLM stuff in the other instruments is always returning "ok" on an entered license but you have **to** patch the FlexLM
> daemon. If you can't get **to** the file that is going **to** be difficult so I'm looking at the install.o file **to** see **how** it works and if there is a way **to** install a patched
> file, that's basically it 🙂

Have you succeeded? Do you have JTAG access?

	Reply	Quote	Notify

40 **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
« Message by *PA0PBZ* on *November 11, 2019, 09:17:43 pm* »

I'm trying **to** find a way in**to** the ESA **to** be able **to** patch the FlexLM part. It looks like the code disassembles fine as a Coldfire processor but you could be right that it is a 68LC040. It looks like it's not that different and it disassembles fine. The method I used **to** get around the FlexLM stuff in the other instruments is always returning "ok" on an entered license but you have **to** patch the

FlexLM daemon. If you can't get **to** the file that is going **to** be difficult so I'm looking at the install.o file **to** see **how** it works and if there is a way **to** install a patched file, that's basically it 😊

<div align="right">

Reply   **Quote**   **Notify**

</div>

41   **Test Equipment** / **Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B**
      « Message by **mbielman** on *November 11, 2019, 08:59:44 pm* »

Not sure what you are trying **to** convey here. The ESA instruments use the MC68LC040 (integer only version) and as far as I know do not have a "traditional" OS at all, unlike the newer units.

If there is a way **to** interrogate the system, I would love **to** know **how**!

<div align="right">

Reply   **Quote**   **Notify**

</div>

Pages: [**1**]

Jump to: `=> Please select a destination ▾` `Go!`

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