

# Hacking the Farm: Breaking Badly Into Agricultural Devices.

DEF CON 30

---

*SICK.CODES*

---

# Prime focus areas

- Food security
- ICS
  - Food & Agriculture
- Supply chain wake up call  
*(hopefully)*

---

# Main take aways

- I should do this to my \_\_\_\_\_

---

This talk is suitable for

- People who eat food





[HOME](#) > [NEWS](#) > [OUTAGES](#)

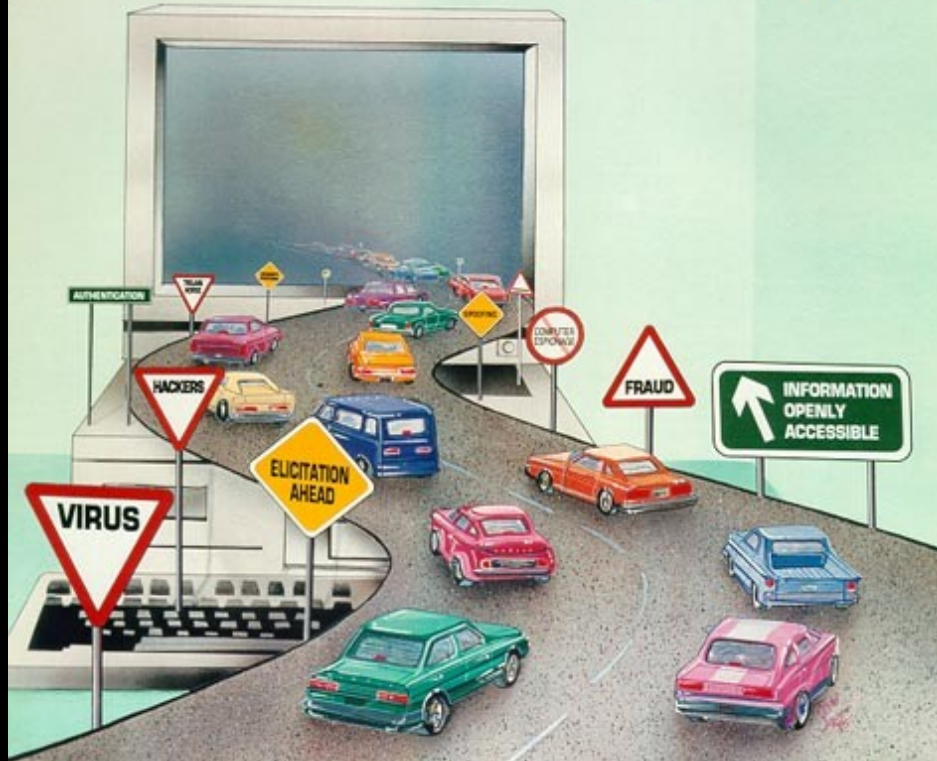
# OVH fire: while police investigate the cause, OVHcloud promises free backups in future

"I believe this incident will change the standards of the industry" says founder Octave Klaba

March 17, 2021 By: [Peter Judge](#)  [Comment](#)



Before hitting the  
Information Superhighway...



Consider the  
**RISKS!**

YOU WOULDN'T  
UPLOAD THE  
SUPPLY CHAIN

YOU WOULDN'T  
UPLOAD THE  
SUPPLY CHAIN  
...OR WOULD YOU



Login

Contacted by a hacker?

Contact Us

# hackerone

SOLUTIONS ▾

PRODUCTS ▾

PARTNERS ▾

COMPANY ▾

HACKERS ▾

RESOURCES



## John Deere

<http://deere.com>

Reports resolved  
94

Assets in scope  
15

Submit report

Vulnerability Disclosure  
Program  
Launched on Aug 2021

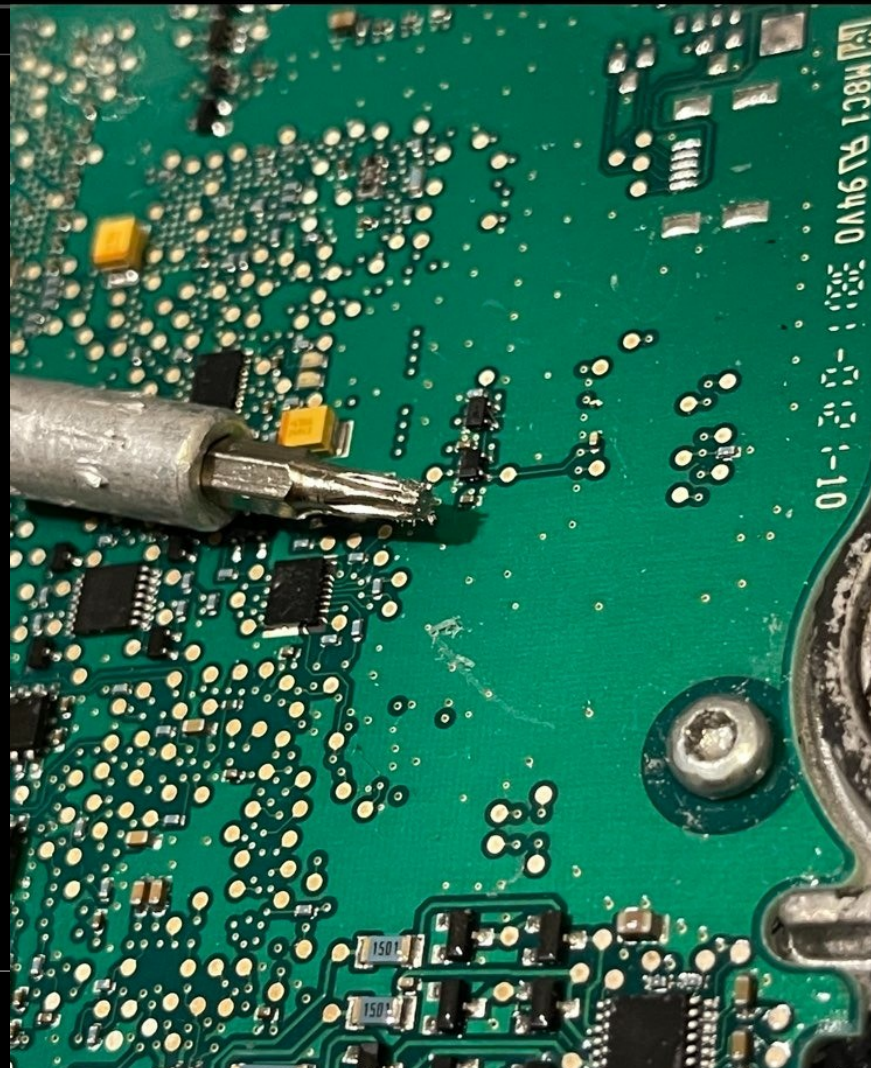
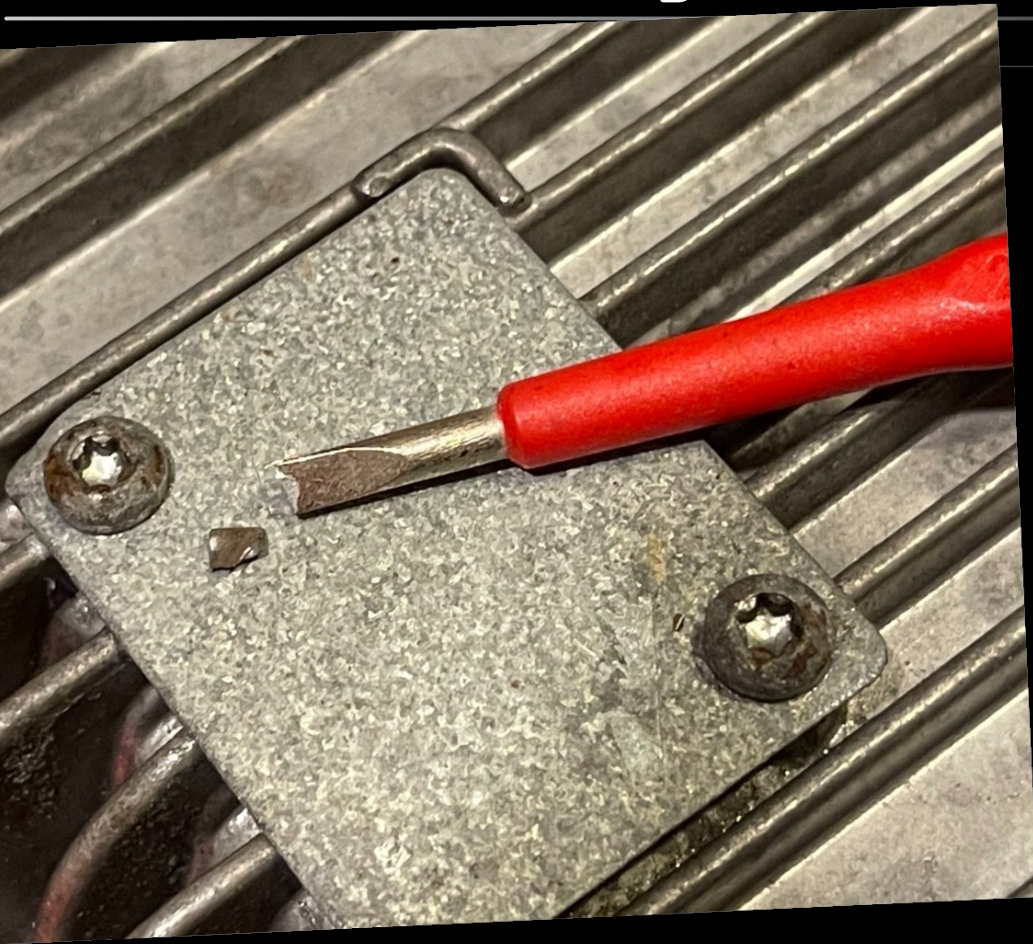
Managed by HackerOne

---

# Reminder

- Today is a good day
- Wow that looks easy
- I should do this to my \_\_\_\_\_
- ~~I can drive a tractor now!~~

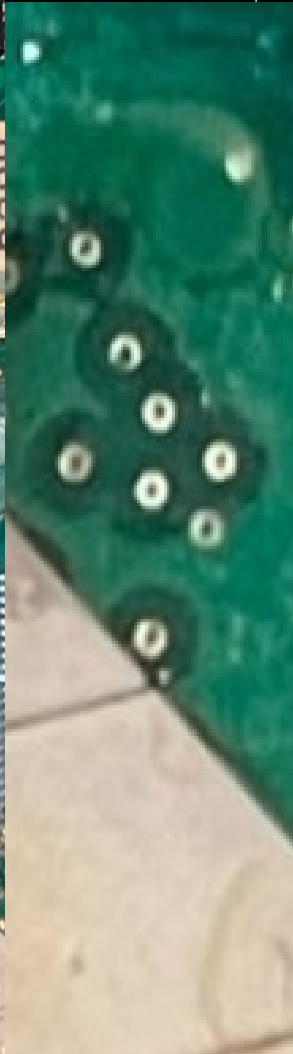
# Never give up



Never



Never g



# So I got another one



I bought yet another MTG

<https://www.elektroda.com/rtvforum/topic3256200-210.html>

NAND Lite! v1.0b1024.84L

Plik Language Pomoc

Co nowego Programator Zawartość Transfer Wsady

Odczyt pamięci

C:\Users\Test2\Desktop\29F8G08ABABA ORIG OK.bin

Zapisz do pliku...

Programowanie pamięci

Wczytaj plik...

Polecenia

Skanuj pamięć Odczytaj pamięć Zapisz do pamięci Kasuj całą pamięć Weryfikuj Anuluj

Prepare file D5500

<== Not tested on TV

☒ Wysyłaj informacje statystyczne o działaniu aplikacji NAND Lite!

Target: 1/1 LUN: 0/1 Block: 1/2048 Page: 96/128 File: 967 680/1 132 462 080

weryfikacja zawartości pamięci

ID : 2C 38 00 26 85 00 00 00  
Manufacturer : MICRON  
Model : MT29F8G08ABABWP  
Konfiguracja:  
Target count : 1  
LUN count : 1  
Block per LUN : 2048  
Page per Block : 128  
Page size : 4096+224  
Rozmiar całkowity : 1 132 462 080 bajtów  
Error verify page: T:1 L:0 B:0 P:0 Count bit:5380  
Error verify page: T:1 L:0 B:0 P:1 Count bit:6172  
Error verify page: T:1 L:0 B:0 P:2 Count bit:3225  
Error verify page: T:1 L:0 B:0 P:3 Count bit:4967  
Error verify page: T:1 L:0 B:0 P:4 Count bit:10833  
Error verify page: T:1 L:0 B:0 P:5 Count bit:5413  
Error verify page: T:1 L:0 B:0 P:6 Count bit:6116

Never give up



Feat. (but not limited to)

OVH

AgCo

John Deere

Case, New Holland

Samsung

Red Hat

Wind River

CISA

Yocto

John Deere

John Deere

Molex

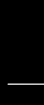
---

Micron



# Disclaimer

- None of research was paid for
  - All research was done in good faith
  - Nothing today represents our employers, past employers, or future employers
  - None of us are under gag orders
  - All content in the slides is CC0
  - All trademarks, logos and brand names are the property of their respective owners.
- 



Sick Codes – good faith hackerman

<https://github.com/sickcodes>

<https://twitter.com/sickcodes>

<https://linkedin.com/in/sickcodes>

<https://sick.codes>



**sickcodes** Follow



Contractor (Always available!) | Secur...

Australiasia



<https://sick.codes>

@sickcodes

**Sponsors**



**Sponsoring**



Overview


Repositories 195

Projects

Packages

Stars 218

Sponsoring 4




 **Docker-OSX** Public


Run macOS VM in a Docker! Run near native OSX-KVM in Docker! X11 Forwarding! CI/CD for OS X Security Research! Docker mac Containers.

 Shell  23.4k  1.1k


 **osx-serial-generator** Public


Mac Serial Generator - Generate complete sets of Serial Numbers for OSX-KVM, Docker-OSX and of course, OpenCore.

 Shell  1.3k  81

 **dock-droid** Public

Docker Android - Run QEMU Android in a Docker! X11 Forwarding! CI/CD for Android!

 Dockerfile  292  24

 **Docker-eyeOS** Public

Run iPhone (xnu-arm64) in a Docker container! Supports KVM iOS kernel debugging (GDB)! Run xnu-qemu-arm64 in Docker! Works on ANY device.

 Shell  561  54

Want to do business?

Hardware/IoT/Firmware Embedded.

**info@sick.codes**

**sick.codes/contact**

---



Home Acc

**Automated  
Security  
Research LLC**

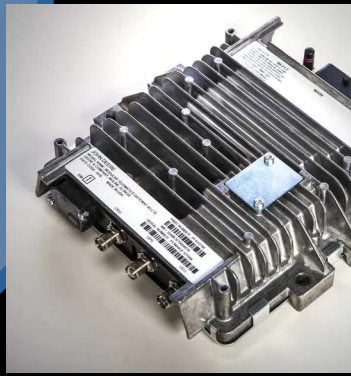
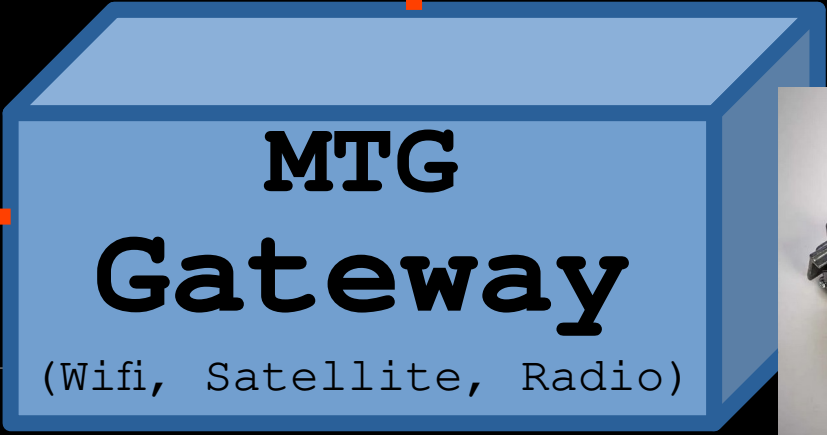
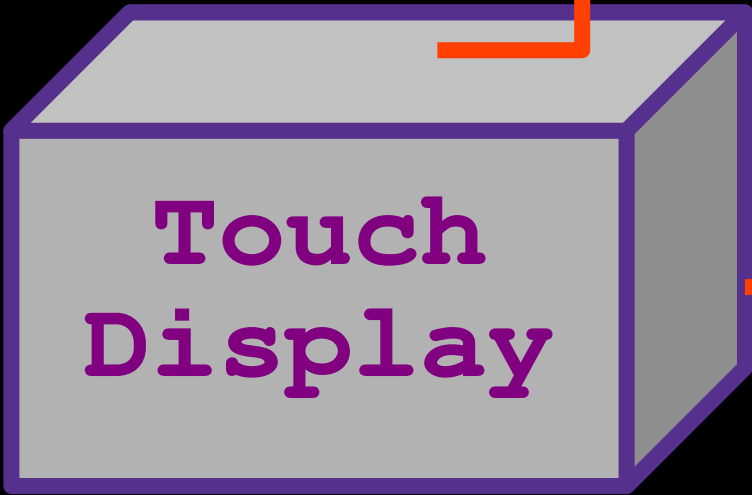
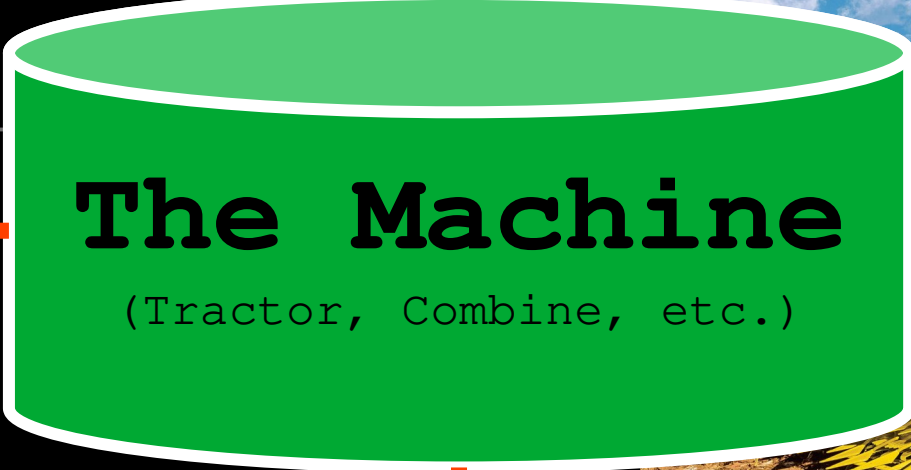
Let's talk?

chainsaw boi



gps controlled chainsaw boi

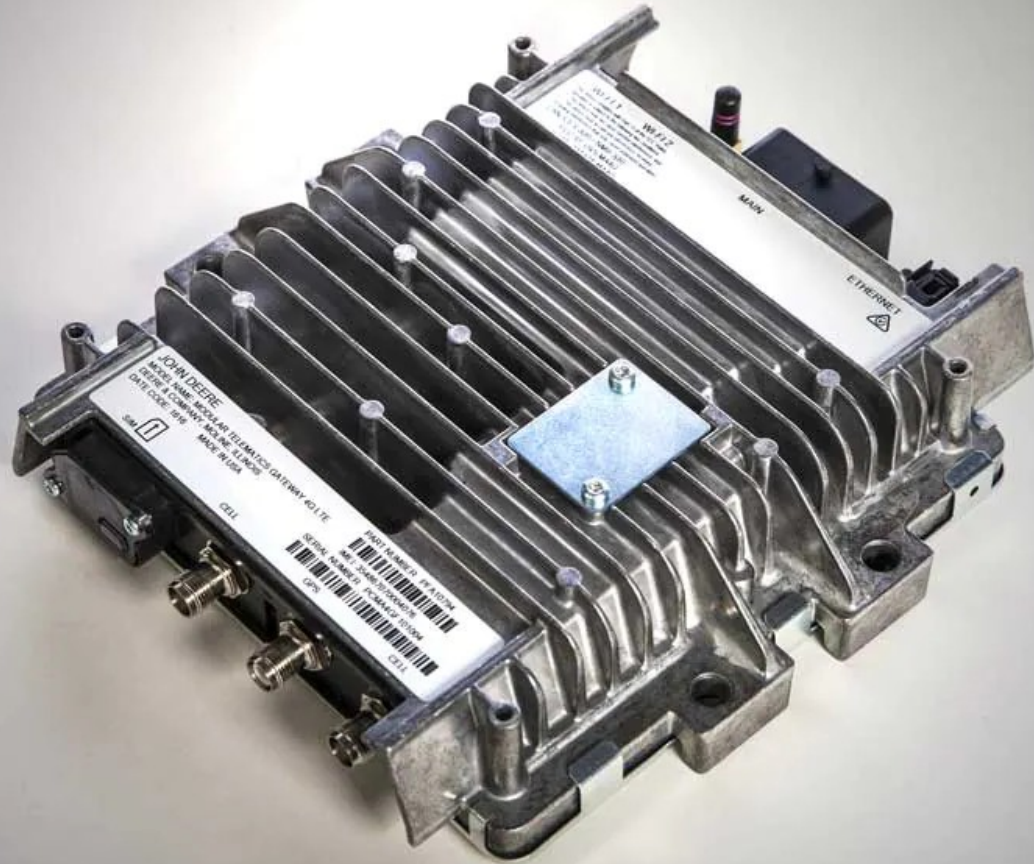




# The Gateway

All 3 parts  
can control the  
other

[https://  
www.deere.com/en/  
electronics/news-  
room/news-articles/  
mtg4g-lte-telematics/](https://www.deere.com/en/electronics/news-room/news-articles/mtg4g-lte-telematics/)



# Go hard or go home



# Brown Box



[https://www2.1jworld.com/news/2008/apr/26/new\\_technology\\_makes\\_farming\\_more\\_profitable\\_produ/](https://www2.1jworld.com/news/2008/apr/26/new_technology_makes_farming_more_profitable_produ/)



**GREENSTAR™**  
MOBILE PROCESSOR

**JOHN DEERE**  
DEERE & COMPANY MOLINE, IL  
GREENSTAR MOBILE PROCESSOR  
PART NUMBER PF80332  
SERIAL NUMBER 113273  
MANUFACTURER PIC  
DATE CODE 0110  
MADE IN USA  
PCGV02C113273

ISO 2.5  
OR  
DEERE 4/5

**32 MB KEYCARD**

- ☒ AUTOTRAC  
☐ FIELD DOC™ 8520  
☐ PARALLEL TRACKING  
☐ MAP BASED PRESCRIPTIONS  
☐ HARVEST DOC™  
☐  
☐

**JOHN DEERE**

Component Serial Number

PCPCB32110631



DEERE & COMPANY MOLINE, ILLINOIS  
MADE IN USA

677053K



PAT. 5070032, 5172338, 5268318  
5279148, 5418752, 5602987

MADE IN CHINA (C) 2002 SANDISK



CERTIFIED BY  
SANDISK



744885D



SDP001

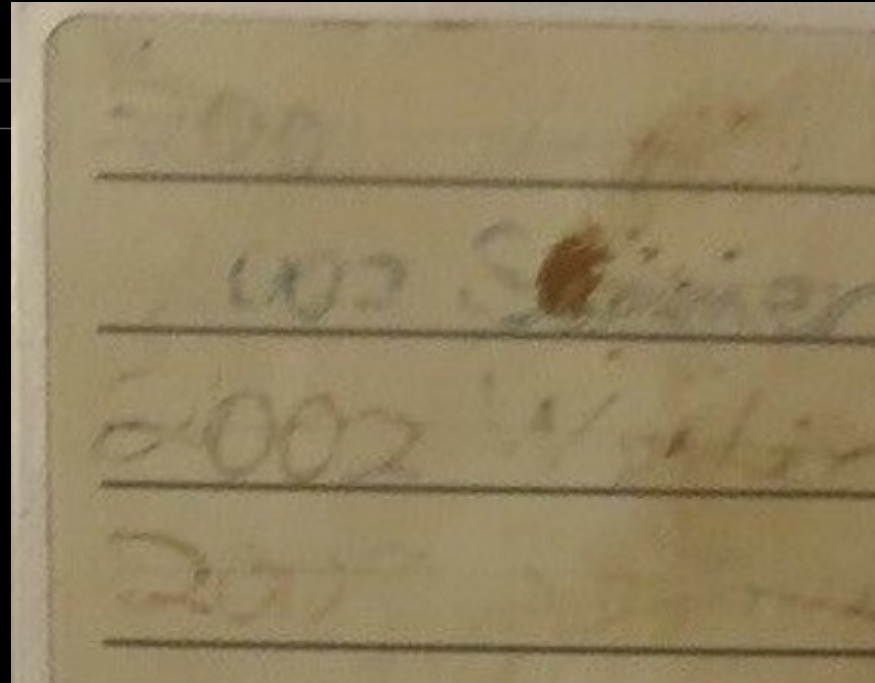
MADE IN USA

PAT. 5070032

5279148

(C) 2002

- Early 2000's
- Still in use
- Lifetime unlocks



**John Deere Brow**

Location:

Auction: Mar 30, 2022

<https://www.bigiron.com>

1800

Rare



1800

Rare



US \$775

## John Deere 1800 Green Star 2 Monitor

ID#

Location:

Auction: Aug 10, 2022

Closing: **11d 21h 40m**

9 Bids

*Last minute bids extend item close by 3 mins*

# 2600



GreenStar™ 2 2600 computer display on the John Deere 9770 STS. Credits:  
Rebecca Barocco, UF/IFAS

# 2600



## Windows® Embedded CE



# 2600



**SOLD! US \$5,600**

## John Deere 2600 Display

ID#

Location:

Auction: Jul 13, 2022

63 Bids

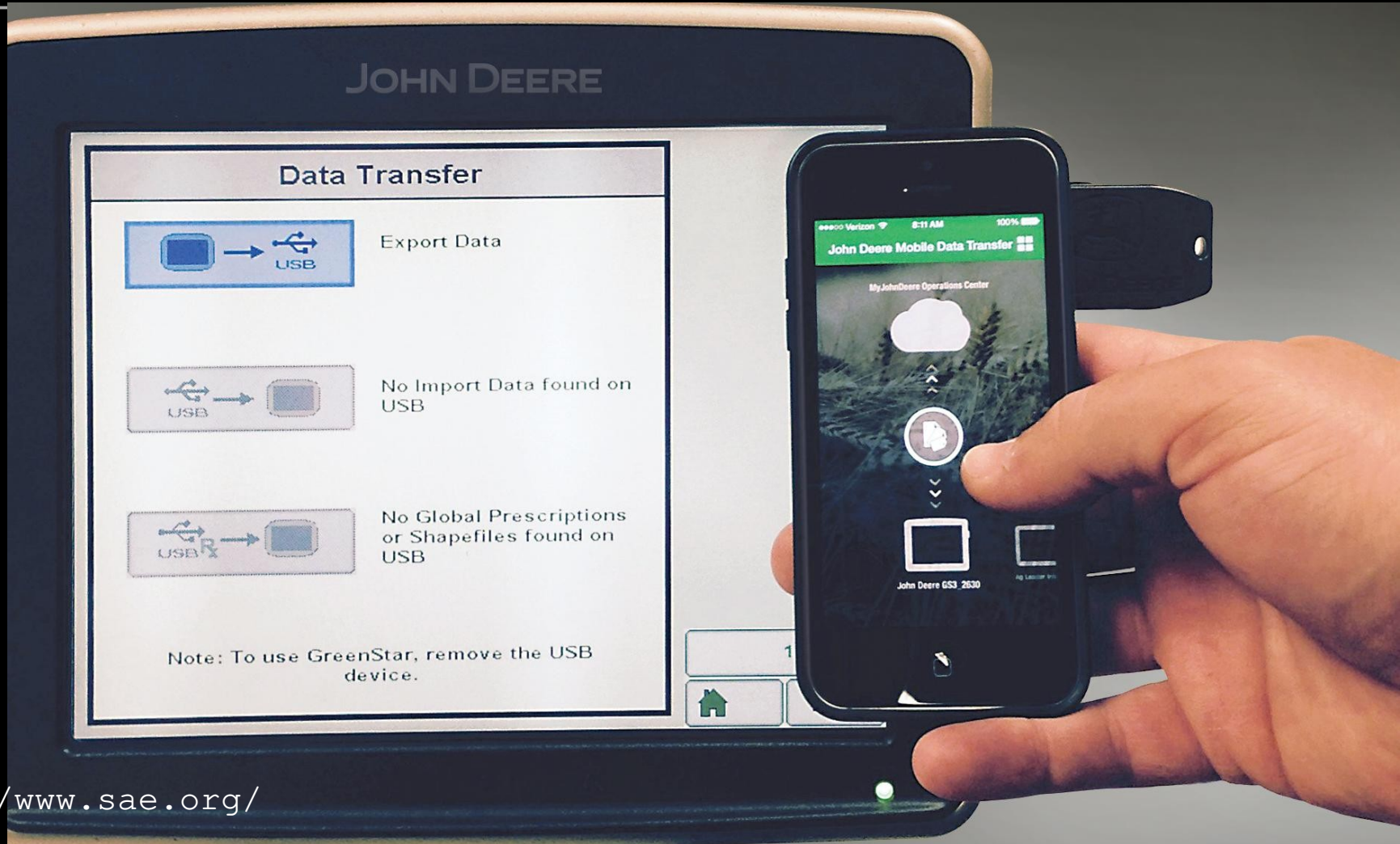
[https://www.bigiron.com/Search?  
historical=true&search=2600&searchMode=All&tab=&page=2&i  
temsPerPage=20&filter=Sold](https://www.bigiron.com/Search?historical=true&search=2600&searchMode=All&tab=&page=2&itemsPerPage=20&filter=Sold)

# 2630 "The Workhorse"



- <https://www.youtube.com/watch?v=wFv-flTic2M>

# 2630 "The Workhorse"



- <https://www.sae.org/>

# 2630 "The Workhorse"



Windows®  
Embedded CE *btw*

Note: To use GreenStar, remove the USB device.



- <https://www.sae.org/>

# 2630 "The Workhorse"

>\$8,000

>EOL

1 to 20 of 661 item(s)

1 2 3 4 5 ... 34 Next Page →



## John Deere 2630 GreenStar 3 Display

Location: Ashland, NE

Auction: Jul 27, 2022

37 Bids



## John Deere 2630 GreenStar 3 Display

Location:

Auction: Jul 27, 2022

26 Bids

# Lifecycle

	<b>Born</b>	<b>Support end date</b>	<b>Support end date Pro</b>	<b>EOL</b>
<b>Windows Embedded CE 6.0</b>	30 <sup>th</sup> Nov 2006	9 <sup>th</sup> April 2013	10 <sup>th</sup> April 2018	<b>28<sup>th</sup> Feb 2022</b>
<b>Windows Embedded Compact 7</b>	15 <sup>th</sup> Mar 2011	12 <sup>th</sup> Apr 2016	13 <sup>th</sup> Apr 2021	28 <sup>th</sup> Feb 2026
<b>Windows Embedded Compact 2013</b>	11 <sup>th</sup> Aug 2013	9 <sup>th</sup> Oct 2018	10 <sup>th</sup> Oct 2023	31 <sup>st</sup> May 2028

# Credit due:

---

- WinCE 6.0 keeps the food chain rolling

# Credit due:

---

- Still works perfectly though.
- Farms:
  - Put seeds in ground
  - Wait for seeds to grow
  - Pick result
  - Sell result
  - Buy more seeds

# Infinite money glitch IRL

Farms:

- Put seeds in ground
- Wait for seeds to grow
- Pick crop
- Sell crop
- Buy more seeds



## John Deere Display Software License Agreement



JOHN DEERE

connection with your purchase of the Display. Either method of notification used by Licensor shall be effective upon dispatch. You agree to notify Licensor of any change in your address in the manner set forth above.

21. **Third Party Software Notifications and Licenses.** The copyrights for certain portions of the Software may be owned or licensed by other third parties ("**Third Party Software**") and used and distributed under license. The Third Party Software Appendix (viewable at this [link](#)) includes the acknowledgements, notices and licenses for the Third Party Software. The Third Party Software is licensed according to the applicable Third Party Software license notwithstanding anything to the contrary in this License Agreement. The Third Party Software contains copyrighted software that is licensed under the GPL/LGPL or other copyleft licenses. A copy of those licenses are included in the Third Party Software Appendix. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of the Software by sending a money order or check for \$5 to:

Deere Open Source Compliance Team  
P.O. Box 1202  
Moline, IL 61266-1202  
USA

Please write "source for John Deere Generation 4-Series Display Unit Software" and [blank] number of the software

# The 4240 & 4640



# The 4240 & 4640



## John Deere 6000 Gen 4 4240 Universal Display

ID#

Location: Parlin, NJ

Auction: Jun 22, 2022

62 Bids

---

Farmers prefer the old  
equipment

- **Reliability/Productivity**
- **Proven**
- **Familiar**
- **Less device restrictions**

# Why am I hacking the 4240?

- Choosing the device with most **longevity**
- **2<sup>nd</sup> Hand** fleet market

- Agricultural tech adoption is **unique**
- Equipment lasts for a **LONG** time

# Ultra compatibility

---

- Brown Box **works** in brand new combine
- ISOBus VT: it's in the name
- CAN, RS232, Analog, Digital, GPIO, WiFi
- GPS, RTCM, RTK Radio, NTRIP, USB, TCP, HSAL2...



**Wind River works closely with Arm®** to ensure that Wind River OSes, tools, and simulation offerings are optimized for use by Arm licensees. With Arm and Wind River, software developers and architects can utilize the full potential of Arm-based SoC devices.

[Learn More »](#)



**A broad range of Intel®** products and solutions are enabled for use with Wind River Studio, Wind River Linux, and VxWorks, providing compute platforms for critical workload consolidation and software-defined infrastructure.

[Learn More »](#)








**Wind River partners with NXP** to enable optimized VxWorks and Wind River Linux OSes, compilation tools, and Wind River Simics® simulation support for the NXP QorIQ, i.MX, and S32 families of Arm and Power Architecture-based MPUs.

[Learn More »](#)



AN INTEL COMPANY

# Wind River in Aerospace and Defense

Air	Commercial Aviation	Land	Sea	Space
				
<p>Apache Helicopter AWACS Airbus A330M Airbus A400M B-1B B-2 B-52 Boeing 767 Tanker Boeing C-130 AMP EC-725 Helicopter F-15 F-16 F-18 F-22 F-35 (JSF) Global Hawk UAV Jaguar nEUROn SH 60 Helicopter X-47B UCAS-D</p>	<p>Airbus A318 Airbus A319 Airbus A320 Airbus A340 Airbus A380 ATIDS Boeing 777 Boeing 787 EC-225 Helicopter GlobalStar 2100 VICTORIA WAAS</p>	<p>Abrams Tank Challenger Tank CHALS-X CIBADS II Fuchs Spürpanzer GIG-E Program Hellfire Missile JCAD JTRS MEADS Missile Patriot Missile PDCUE Sentinel Missile Stinger Missile TDOA System THAAD Missile TRC 4000</p>	<p>AEGIS AN/AQS20/X Sonar AN/SQQ-89 ASW Astute Class Sub. Harpoon Missile Mark 48 GMVLS MK41 5 inch gun NCSSS NAVMACS Phalanx – CIWS SGS SSDS Tomahawk Missile Trident Missile Type 45 Destroyer</p>	<p>A2100 Satellite EGNOS HOPE-X Space Plane Mars Rovers Mars Odyssey Mars Pathfinder Mars Recon Orbiter MTSAT-2 Satellite MUBLCOMM Satellite NASA Space Shuttle NPOESS ORBCOMM Phoenix Mars Lander PROBA Satellite SBIRS SORCE Satellite X-38 Space Lifeboat</p>

JOHN DEERE

## Guidance

08:57



SF3



Location  
North 75  
Field



S

181°



Counters A  
0.46 ac



ac

Counters A  
0.46 ac



ac

Next Track  
Track 1

Swap



Guidance

Track 1

See Track

Track Spacing

Shift Track



6.0 in

Shift Increment



SETUP



WORK

OFF



AUTO TRAC

ON



GUIDANCE



QUICK LINE



SWAP TRACK



ISOCON VT



DISPLAY



HELP



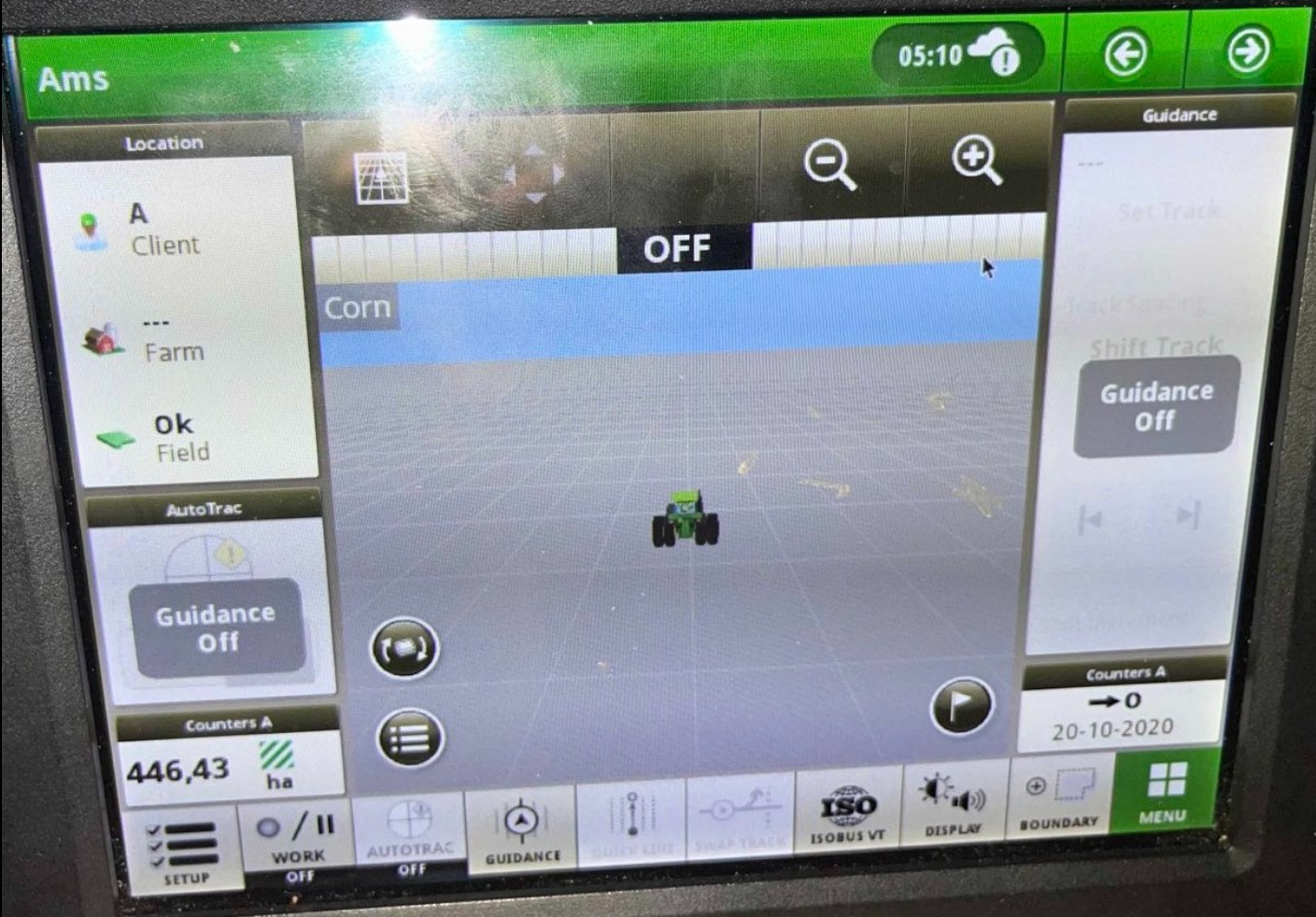
MENU

# displaysimulator.deere.com

The image displays the John Deere 4600 CommandCenter simulator interface, which is divided into several functional areas:

- Navigation:** Located on the left, it includes a speedometer showing 0 mph and directional controls.
- Additional Controls:** Below navigation, it features crop input settings for Yield (bu/ac) set to 200 and Moisture (%) set to 15, each with minus and plus adjustment buttons.
- Operations:** A central panel titled "Operations" with a "Select a scenario:" dropdown menu set to "Import Data" and an "Upload Files" button. It contains a list of files: USB\_example.zip, GS3\_2630, Profile1, Profile2, and Rx. Below the list, it provides instructions for uploading files and using USB drive options.
- ISOBUS Controllers:** A pop-up window titled "ISOBUS Controllers" showing a "StarFire - Vehicle Navigation" status for John Deere 12344. It indicates a "Virtual Terminal disconnected" error on the Implement Bus and includes a "Troubleshoot" button.
- Harvesting:** The main display area shows a map of the "Wheat (White)" field. It includes a "Location" panel with "Deere Client", "Simulator Farm", and "South 40 Field". The "Guidance" panel shows "40.000ft Track Spacing" and "Shift Track" controls. The "Counters A" panel displays "15.0 bu/ac" and "0.0 ac". The "Grain Handling" panel shows "Wheat" and "Feature unavailable or not installed".
- Primary Display:** A large digital display on the right showing speed (1200 RPM, 0.0 MPH) and various icons.
- 4600 CommandCenter:** The main interface is labeled "4600 CommandCenter" and includes a "Harvesting" section with a "Set Track" button and "Shift Track" controls.

JOHN DEERE



Menu



## Section Control | Section Control



### Section Control

Demo Off



Demo

Time Remaining: 15 of 15 Hrs

ON

OFF



Enter Activation Code

# Dollar bills

## AUTO TRAC PRICES

updated 7/26/17

### GS3 AUTOTRAC PRICES

#### SF1 HAS 9" ACCURACY

<u>SF1 WITH GS 3 2630</u>	<u>PRICE</u>
AUTOTRAC ACTIVATION	\$ 3,500.00
GS3 DISPLAY	\$ 5,895.00
SF1 SF6000 RECEIVER	\$ 3,895.00
<b>TOTAL</b>	<b>\$ 13,290.00</b>

### USED AUTOTRAC PRICES

<u>SF1 WITH GS2 2600</u>	<u>PRICE</u>
AUTOTRAC ACTIVATION	\$ 3,500.00
USED GS2 DISPLAY	\$ 1,500.00
USED SF1 SF3000 RECEIVER	\$ 2,500.00
<b>TOTAL</b>	<b>\$ 7,500.00</b>

### Gen IV Display Prices

#### Gen IV 4600 Activations

AutoTrac Activation	\$ 1,000.00
Premium Activation (AT, Swath, Doc)	\$ 3,000.00

#### SF3 HAS 1.2" ACCURACY

<u>GS3 2630 SF3 KIT</u>	<u>PRICE</u>
AUTOTRAC ACTIVATION	\$ 3,500.00
GS3 DISPLAY	\$ 5,895.00
SF3 SF6000 RECEIVER	\$ 7,895.00
<b>TOTAL</b>	<b>\$ 17,290.00</b>

#### RTK HAS SUB INCH ACCURACY

<u>GS 3 2630 RTK KIT</u>	<u>PRICE</u>
AUTOTRAC ACTIVATION	\$ 3,500.00
GS3 DISPLAY	\$ 5,895.00
SF3 SF6000 RECEIVER	\$ 7,895.00
RTK ACTIVATION	\$ 3,500.00
RTK RADIO BUNDLE	\$ 1,795.00
<b>TOTAL</b>	<b>\$ 22,585.00</b>

**\*RTK Subscription is Required see an AMS Specialist for Details**

**\*For RTK Other Hardware is Required see an AMS Specialist for Details**

**Have A Farm Plan Account??? Check Out Their Special Financing Options for AMS Equipment**

#### Gen IV 4640 Prices

4640 Universal Display	\$ 3,995.00
1 Yr AutoTrac Subscription	\$ 850.00
1 Yr Precision Ag Core Subscription (AT, Swath, Doc)	\$ 1,700.00
5 Yr AutoTrac Subscription	\$ 4,000.00
5 Yr Precision Ag Core Subscription (AT, Swath, Doc)	\$ 8,000.00

### Other Items and Upgrades to GS2 and GS3 Equipment

<u>GS2 Upgrades</u>	<u>PRICE</u>
SWATH CONTROL PRO	\$ 3,000.00
AUTOTRAC ACTIVATION	\$ 3,500.00
ROWSENSE ACTIVATION	\$ 3,000.00
RTK ACTIVATION	\$ 3,500.00

<u>GS3 Upgrades</u>	<u>PRICE</u>
Machine Sync Activation	\$ 1,500.00
SWATH PRO ACTIVATION	\$ 3,000.00
AUTOTRAC ACTIVATION	\$ 3,500.00
AUTOTRAC ROWSENSE	\$ 3,000.00

<u>Misc</u>	<u>PRICE</u>
RATE CONTROLLER 2000	\$ 2,350.00
ATU 200	\$ 1,395.00
SF1 TO SF2 RECEIVER UPGR	\$ 4,000.00
RTK RADIO BUNDLE	\$ 1,795.00

# Dollar bills

## **RTK HAS SUB INCH ACCURACY**

### **GS 3 2630 RTK KIT**

### **PRICE**

AUTOTRAC ACTIVATION	\$	3,500.00
GS3 DISPLAY	\$	5,895.00
SF3 SF6000 RECEIVER	\$	7,895.00
RTK ACTIVATION	\$	3,500.00
RTK RADIO BUNDLE	\$	1,795.00
<b>TOTAL</b>	<b>\$</b>	<b>22,585.00</b>

---

### **Gen IV 4640 Prices**

4640 Universal Display with Documentation and Autotrac	\$	8,495.00
Premium 3.0 Subscription - 1 Year (Swath, RowSense, Data Share)	\$	850.00
Automation 3.0 Subscription - 1 Year (Prem 3.0 +Turn Automation, Imp Guide, Machine Sync)	\$	1,350.00

### **Gen IV 4240 Prices**

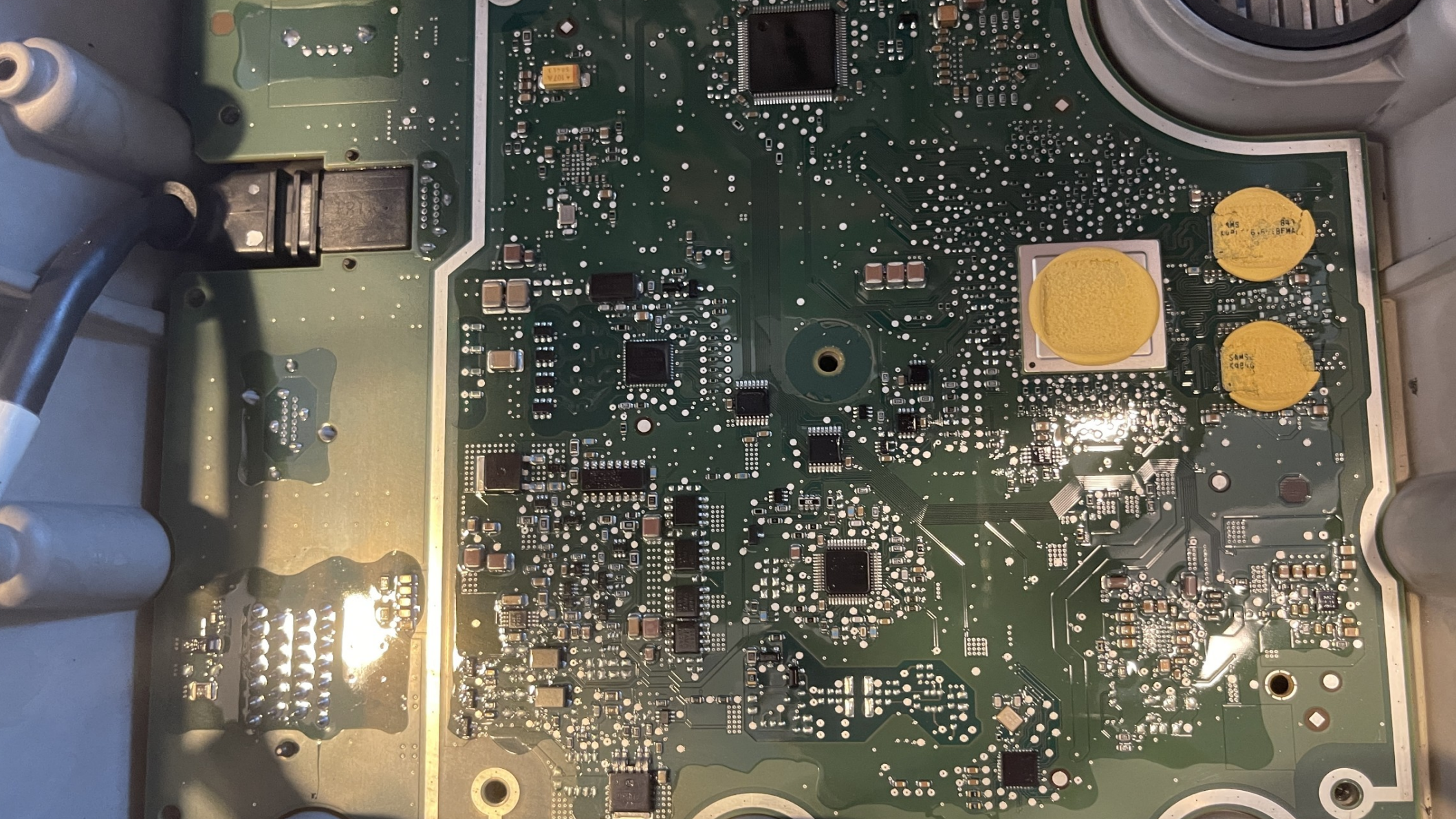
4240 Display with Documentation and AutoTrac	\$	5,495.00
Subscription - 1 Year (Swath, Data Sync)	\$	600.00

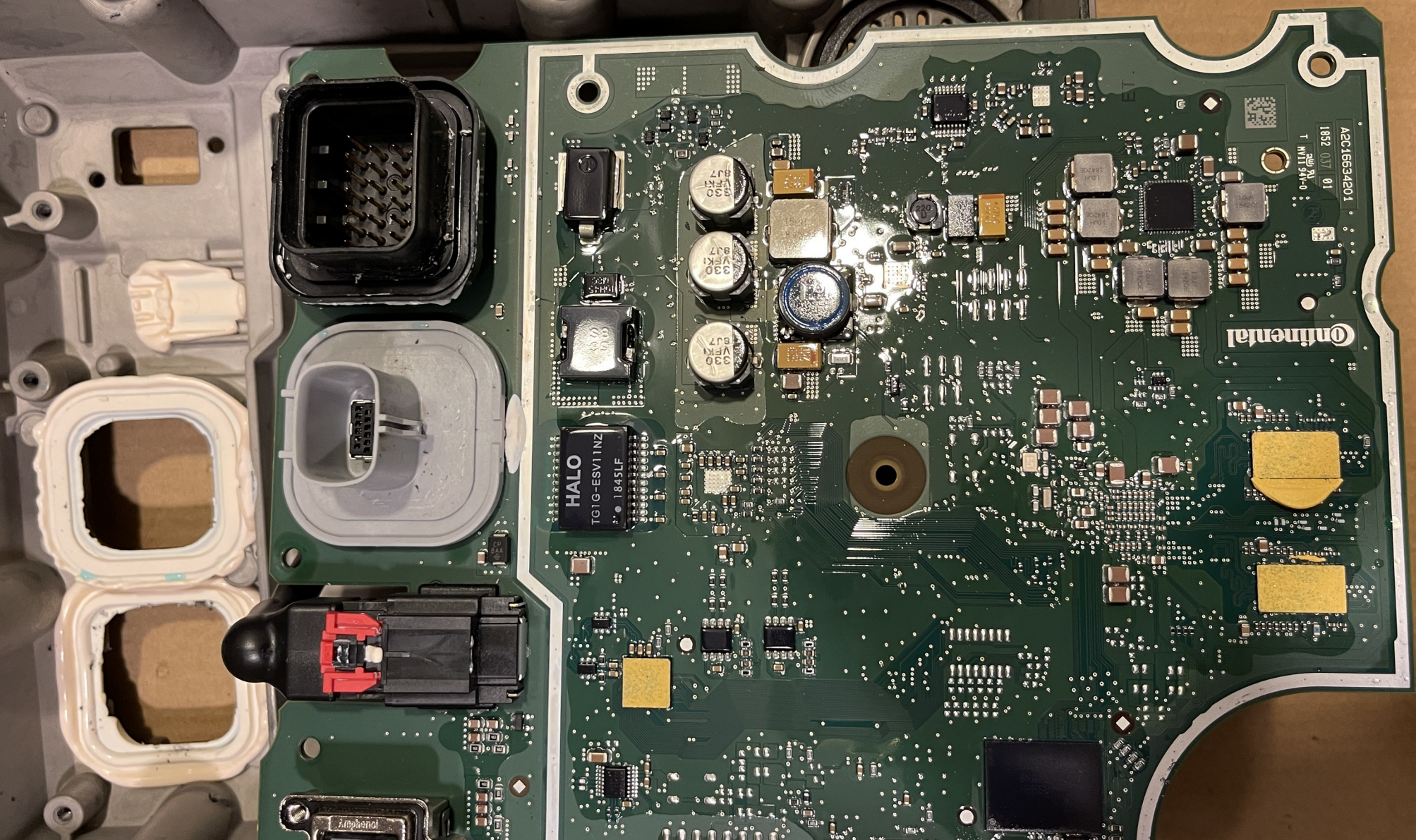
## Gen IV Display Prices

### Gen IV 4600 Activations

AutoTrac Activation	\$ 1,000.00
Premium 3.0 (AT, Swath, Doc, RowSense, Data Share)	\$ 3,750.00
Premium 1.0 to 3.0 Upgrade	\$ 750.00
Premium 2.0 to 3.0 Upgrade	\$ 250.00
Automation 3.0 (Prem 3.0 + Turn Automation, Imp Guide, Machine Sync)	\$ 5,250.00
AutoTrac to Automation 3.0 Upgrade	\$ 4,250.00
Premium 1.0 to Automation 3.0 Upgrade	\$ 2,250.00
Premium 2.0 to Automation 3.0 Upgrade	\$ 1,750.00
Premium 3.0 to Automation 3.0 Upgrade	\$ 1,500.00
Automation 3.0 to Automation 3.0 Upgrade	\$ 500.00







A2C1663420.1

1052 03/01

T M113N-0

Continental

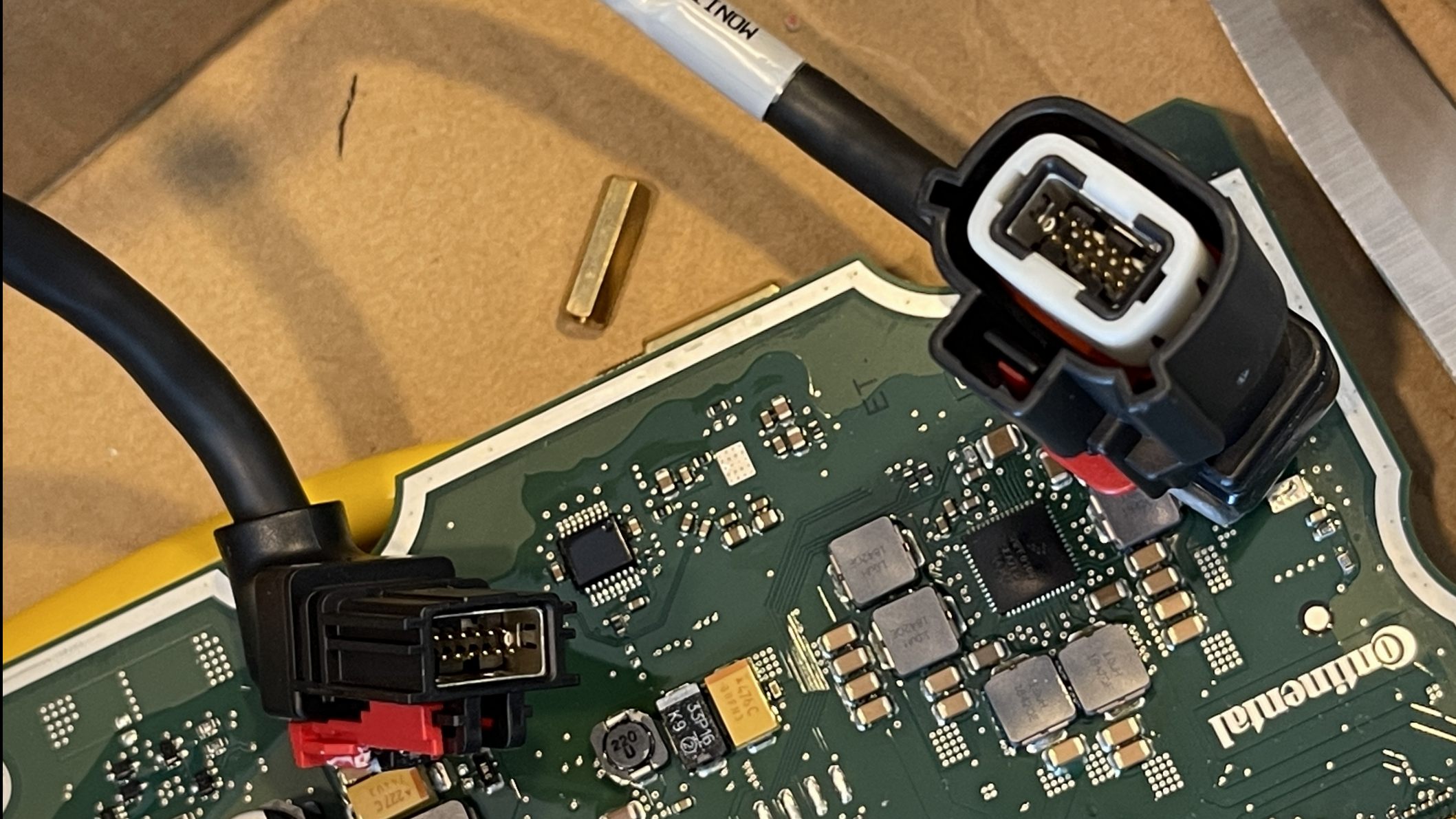
HALO  
TG1G-ESV11NZ  
1845LF

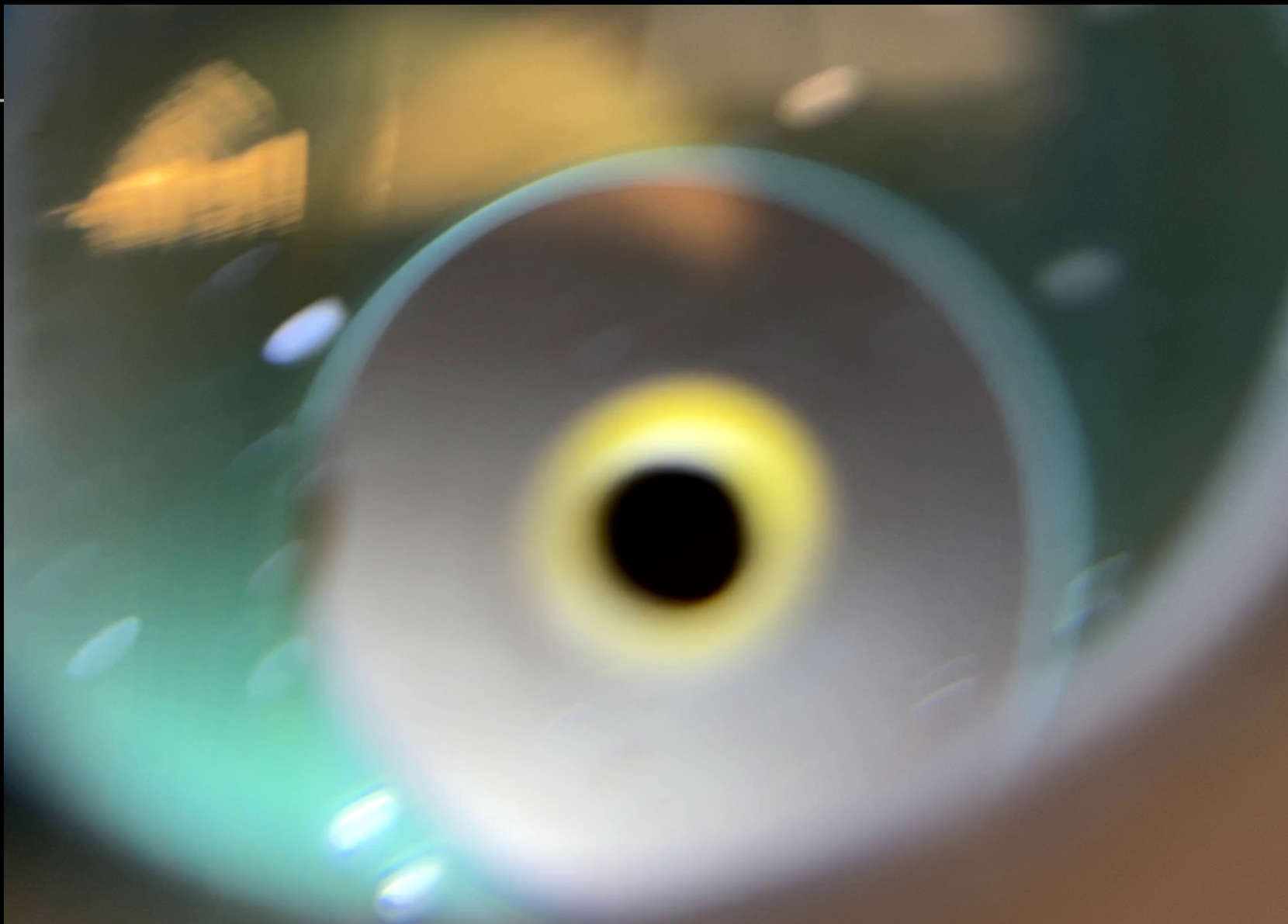
330  
VFK1  
8J7

330  
VFK1  
8J7

330  
VFK1  
8J7



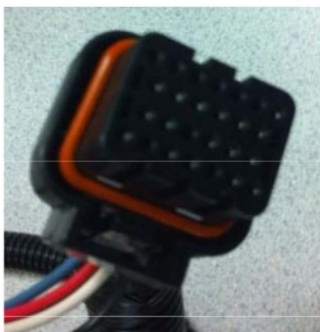




## Pinout Information

Continuation of PF90687

4



Pin Number	Circuit Code	Function
1	922C	Switched Power
2	n/a	n/a
3	209B	Implement Status Signal
4	n/a	n/a
5	n/a	n/a
6	925B	CCD +
7	924B	CCD -
8	182	Unswitched Power
9	998	Audio Mute
10	n/a	n/a
11	211B	Radar Ground Speed Signal

## Pinout Information

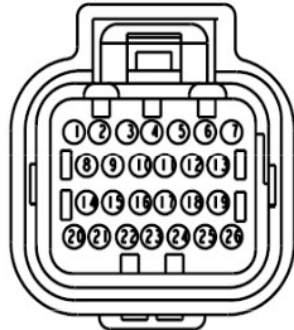
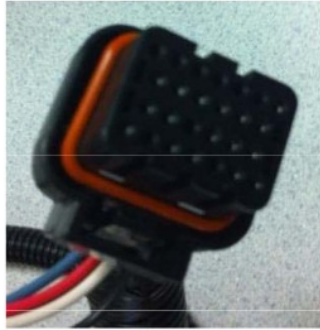
Continuation of PF90687

Pin Number	Circuit Code	Function
12	915	Vehicle CAN Bus - Lo
13	914	Vehicle CAN Bus - Hi
14	070C	Ground
15	n/a	n/a
16	n/a	n/a
17	n/a	n/a
18	904C	Implement CAN Bus - Hi
19	905C	Implement CAN Bus - Lo
20	n/a	n/a
21	n/a	n/a
22	n/a	n/a
23	n/a	n/a
24	n/a	n/a
25	n/a	n/a
26	n/a	n/a

## Pinout Information

Continuation of PF90687

4

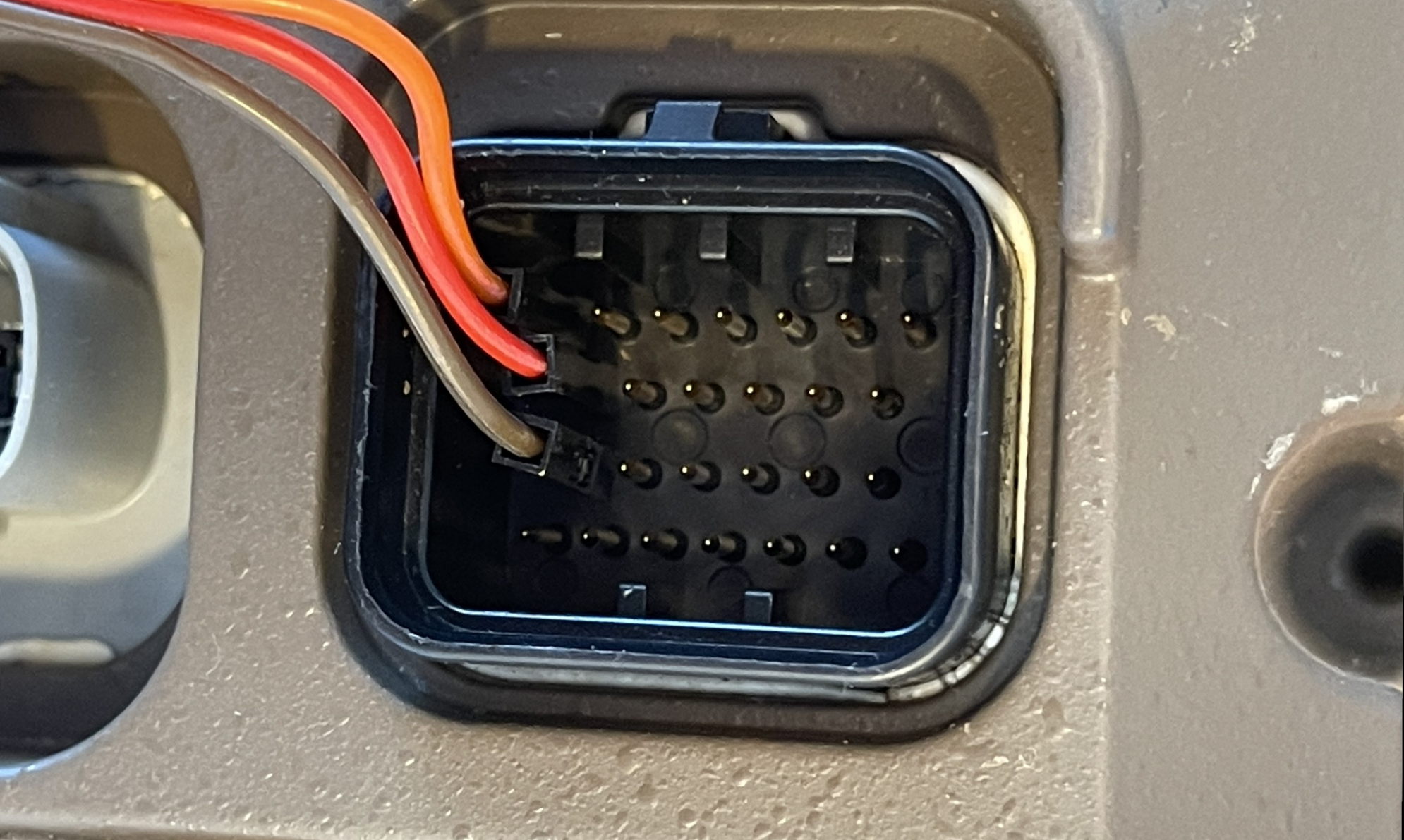


Pin Number	Circuit Code	Function
1	922C	Switched Power
2	n/a	n/a
3	209B	Implement Status Signal
4	n/a	n/a
5	n/a	n/a
6	925B	CCD +
7	924B	CCD -
8	182	Unswitched Power
9	998	Audio Mute
10	n/a	n/a
11	211B	Radar Ground Speed Signal

## Pinout Information

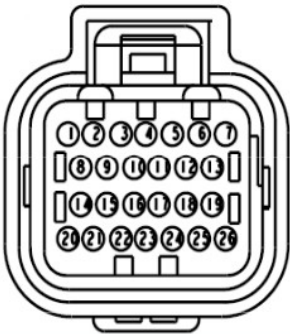
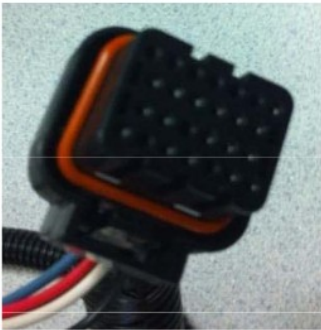
Continuation of PF90687

Pin Number	Circuit Code	Function
12	915	Vehicle CAN Bus - Lo
13	914	Vehicle CAN Bus - Hi
14	070C	Ground
15	n/a	n/a
16	n/a	n/a
17	n/a	n/a
18	904C	Implement CAN Bus - Hi
19	905C	Implement CAN Bus - Lo
20	n/a	n/a
21	n/a	n/a
22	n/a	n/a
23	n/a	n/a
24	n/a	n/a
25	n/a	n/a
26	n/a	n/a



**Pinout Information**  
*Continuation of PF90687*

4

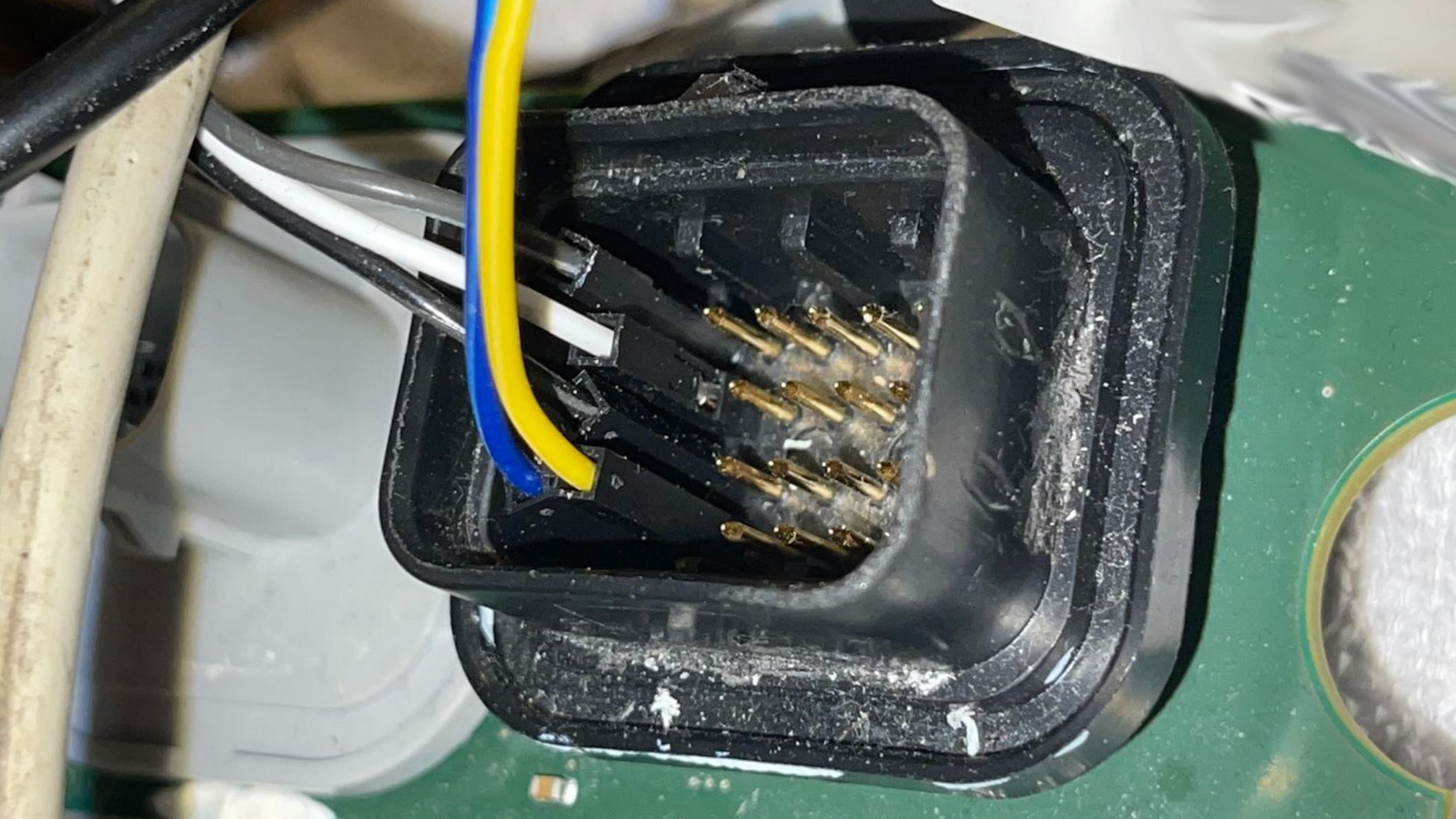


Pin Number	Circuit Code	Function
1	922C	Switched Power
2	n/a	n/a
3	209B	Implement Status Signal
4	n/a	n/a
5	n/a	n/a
6	925B	CCD +

20	n/a	n/a
21	n/a	n/a

**Pinout Information**  
*Continuation of PF90687*

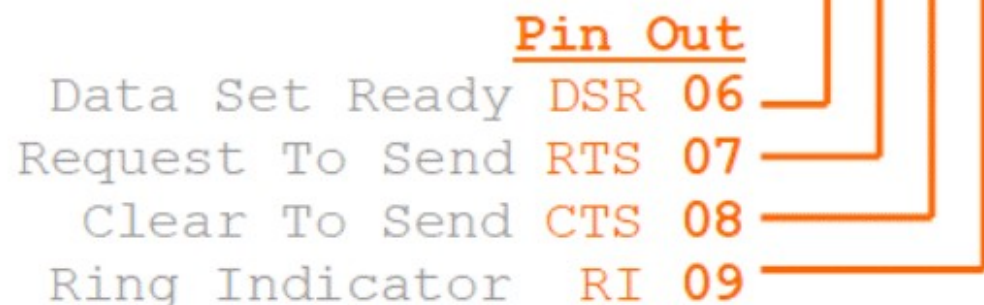
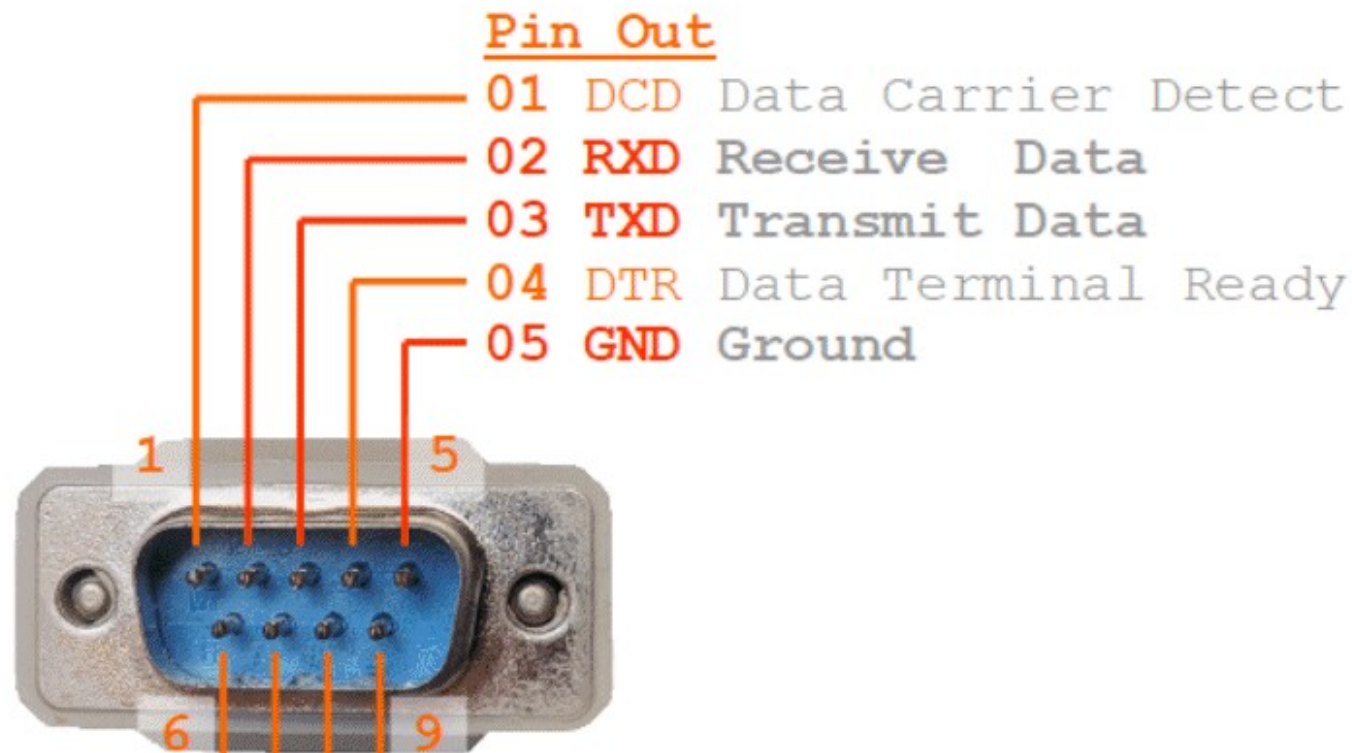
Pin Number	Circuit Code	Function
12	915	Vehicle CAN Bus - Lo
13	914	Vehicle CAN Bus - Hi
14	070C	Ground
15	n/a	n/a
16	n/a	n/a
17	n/a	n/a
18	904C	Implement CAN Bus - Hi
19	905C	Implement CAN Bus - Lo
20	n/a	n/a
21	n/a	n/a
22	n/a	n/a



# RS232 Pin Out

Connector:

D-Sub Male 9 pins



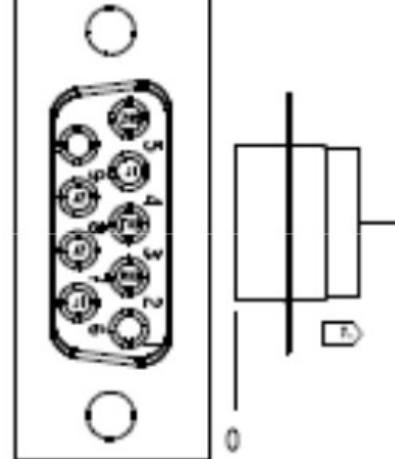
Copyright ©

[www.cable-tester.com](http://www.cable-tester.com)

- RS232



3



Pin Number	Circuit Code	Function
1	911B	n/a
2	907	RS232 Com Bus 1 - TXD
3	909	RS232 Com Bus 1 - RXD
4	911C	n/a
5	070A	Ground

# JOHN DEERE

## SR INSTALLATION of PCGUMUA005528 - 1.1

English: Your system has entered System Recovery. Please contact your John Deere Dealer to attempt data recovery and software reinstallation. Dealers please refer to latest machine or display technical manual for more information.

Español: Su sistema ha entrado en modo de Recuperación. Por favor comuníquese con el concesionario John Deere para intentar la recuperación de datos y la reinstalación del software. Los concesionarios deben consultar el manual técnico más reciente de la máquina o de la pantalla.

Français: Votre système a démarré une récupération du système. Veuillez contacter votre concessionnaire John Deere pour tenter une récupération de données et une réinstallation du logiciel. Concessionnaires : veuillez vous reporter au manuel technique le plus récent de la machine ou de la console pour plus d'informations.

Deutsch: Ihr System befindet sich im Systemwiederherstellungsmodus. Bitte wenden Sie sich an Ihren John Deere-Händler, um eine Datenwiederherstellung und Neuinstallation der Software zu versuchen. Händler sollten das neueste technische Handbuch der Maschine oder des Displays heranziehen, um weitere Informationen zu erhalten.

Português: Seu sistema iniciou a Recuperação do Sistema. Entre em contato com o seu distribuidor John Deere para tentar efetuar a recuperação dos dados e a reinstalação do software. Distribuidor, consulte o manual técnico do monitor ou da máquina mais recente para obter mais informações.

Italiano: Il sistema in uso è entrato in fase Recupero sistema. Rivolgersi al concessionario John Deere di zona per procedere al recupero dei dati ed alla reinstallazione del software. Per ulteriori informazioni i concessionari possono consultare il manuale tecnico della macchina o del display più recente.

Welcome to minicom 2.8

I OPTIONS: I18n

Compiled on Jan 9 2021, 12:42:45.

Port /dev/ttyUSB0, 06:52:12

Press CTRL-A Z for help on special keys

my\_load:667: do

HOTPLUG: mounted sda1 at /tmp/mnt/usbLYU3Gf

/dev/mmcblk0p2: recovering journal

/dev/mmcblk0p2: clean, 17026/130048 files, 243487/520192 blocks

SetupNormalPartitions IN\_PROGRESS 36

fsck from util-linux 2.26.2

SetupUserDataAccess SUCCESS 100



# 10 Reboots = Dealer lock...

- Ok let's desolder the eMMC
- Reduce the bootcount, increase max to 9999





bootcount.cfg

user

58 bytes -rw-r--r--



zImage-4.1.21-r



zImage

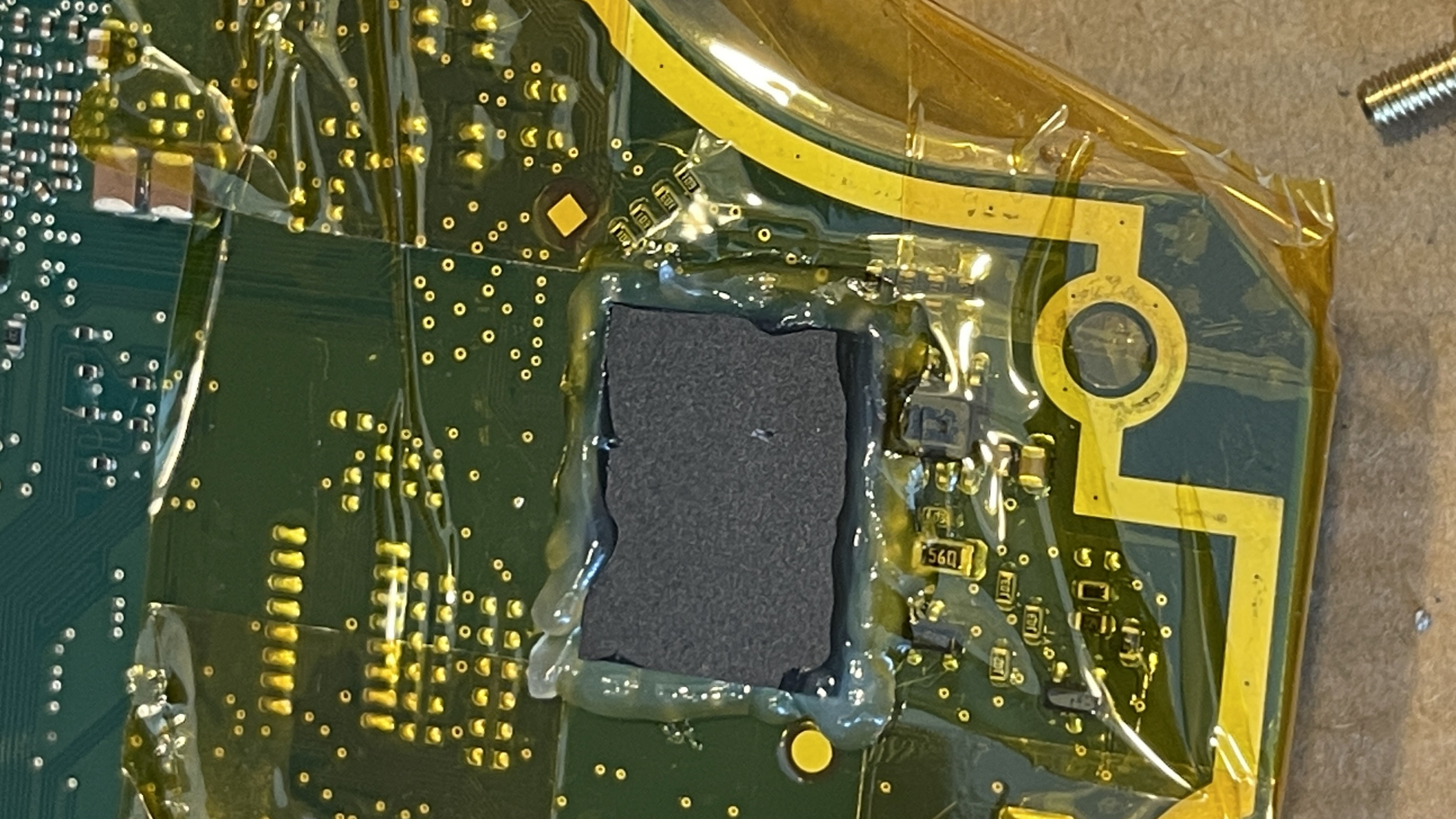
user

4.5 MiB -rw-r--r--

```
[user@hostname 0]$  
[user@hostname 0]$ cat bootcount  
BOOT_MODE=NORMAL  
MAX_BOOT_COUNT=10  
RECOVERY_BOOT_COUNT=6  
  
[user@hostname 0]$
```

# "The Magic Check File"

```
474
475 #*****
    *****
476 # DESCRIPTION
477 #     Spawns login prompt on serial port, does not return.
478 #*****
    *****
479 SpawnSerialLogin()
480 {
481     while true; do
482         setsid /sbin/agetty -c -L 115200 ttyS_debug vt100
483     done
484 }
485
486 #*****
```



Size 16 GB (15,535,702,016 bytes)

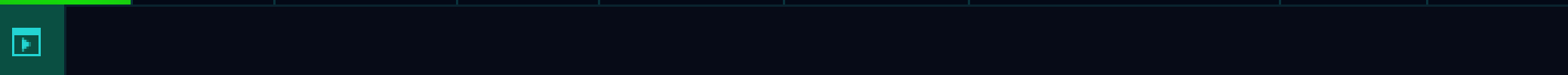
Auto-clear ☒

Backing File /run/media/user/970EVO-1TB/master/4240.img

Partitioning Master Boot Record

## Volumes

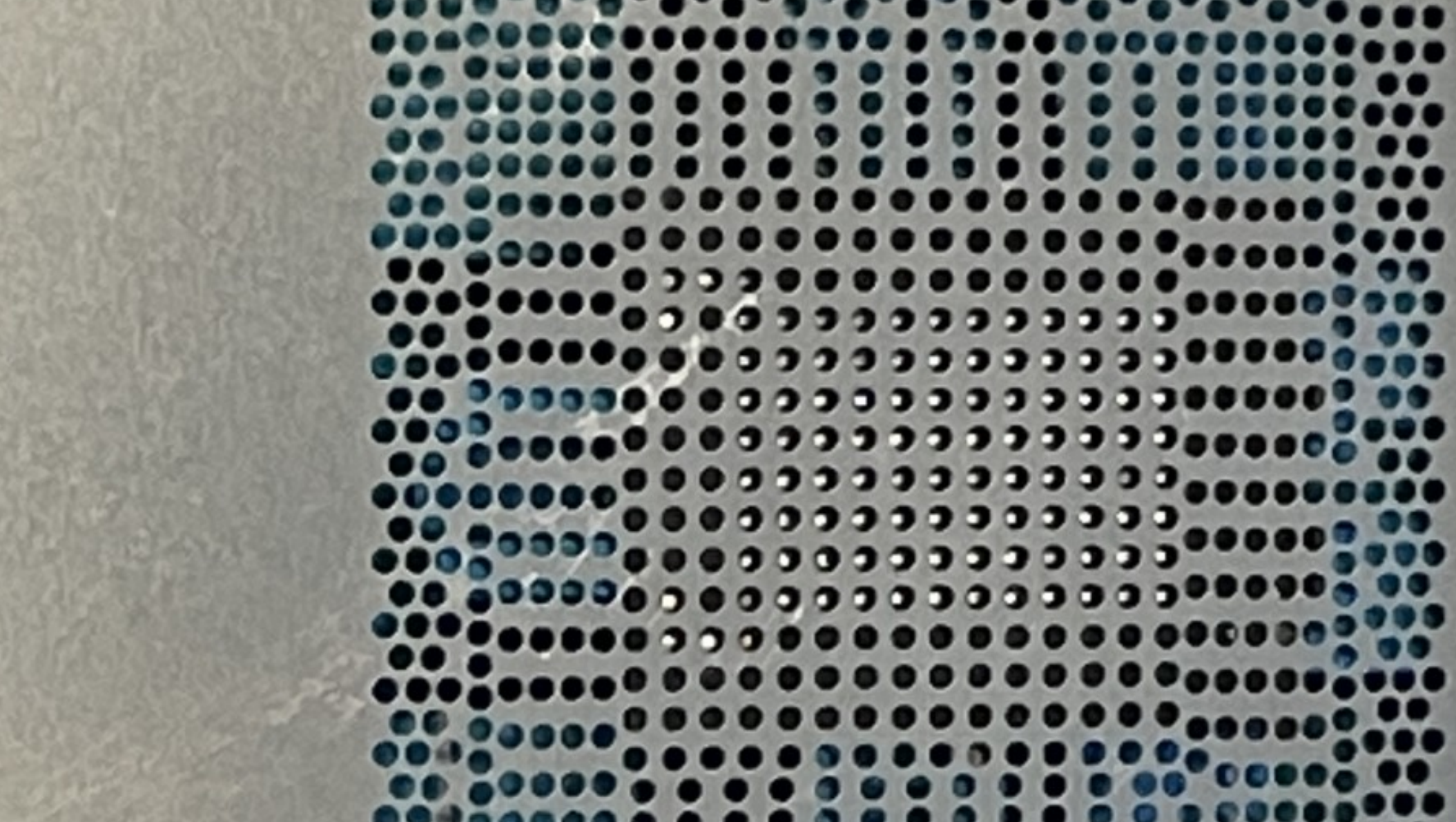
Free Space 17 MB	Filesystem Partition 1 17 MB Ext2	Filesystem Partition 2 2.1 GB Ext4	Filesystem Partition 3 34 MB Ext4	Extended Partition Partition 4 13 GB				
				Filesystem Partition 5 2.1 GB Ext4	Filesystem Partition 6 2.1 GB Ext4	Filesystem Partition 7 8.5 GB Ext4	Filesystem Partition 8 268 MB Ext2	Filesystem Partition 9 268 MB Ext2

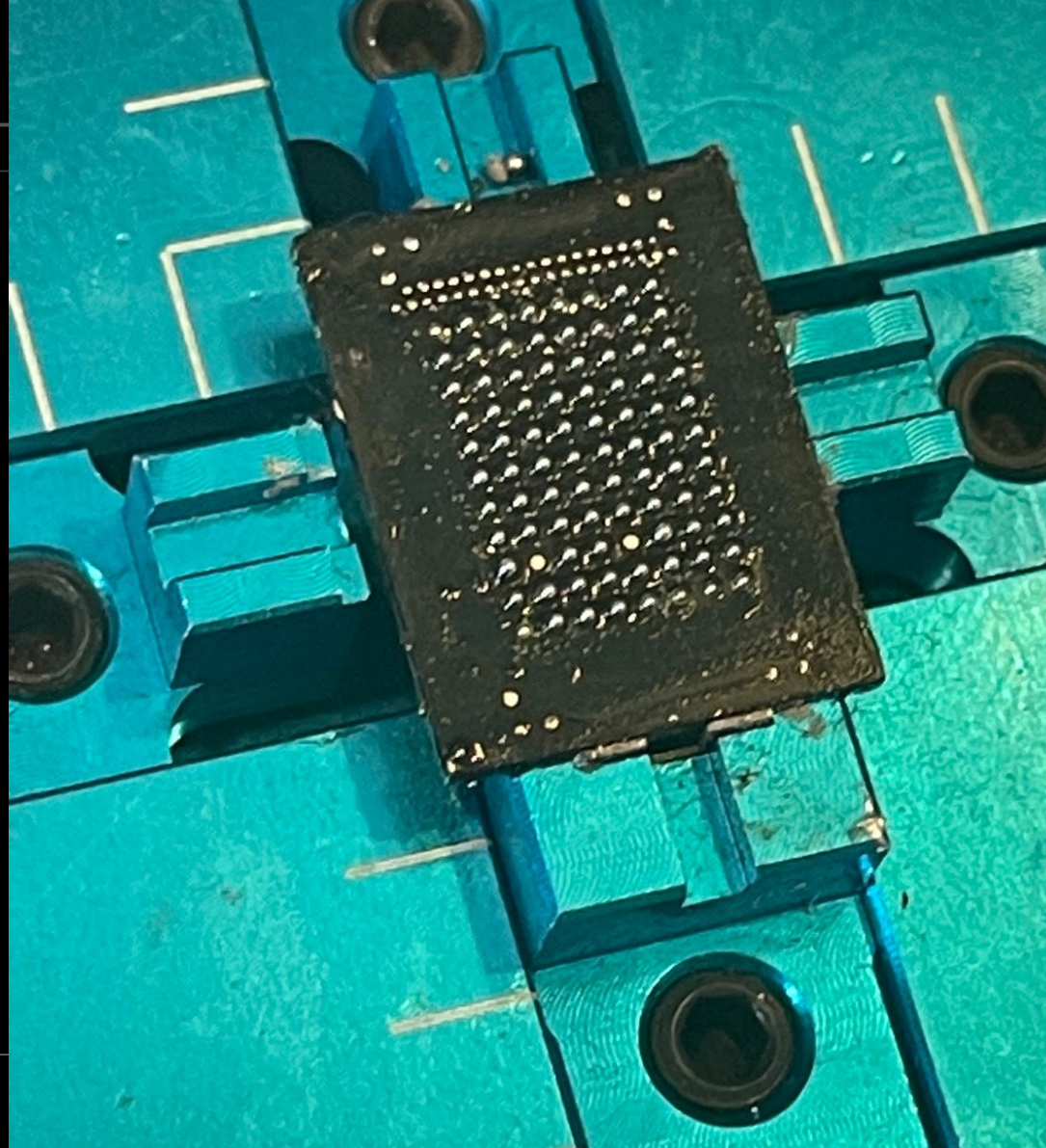
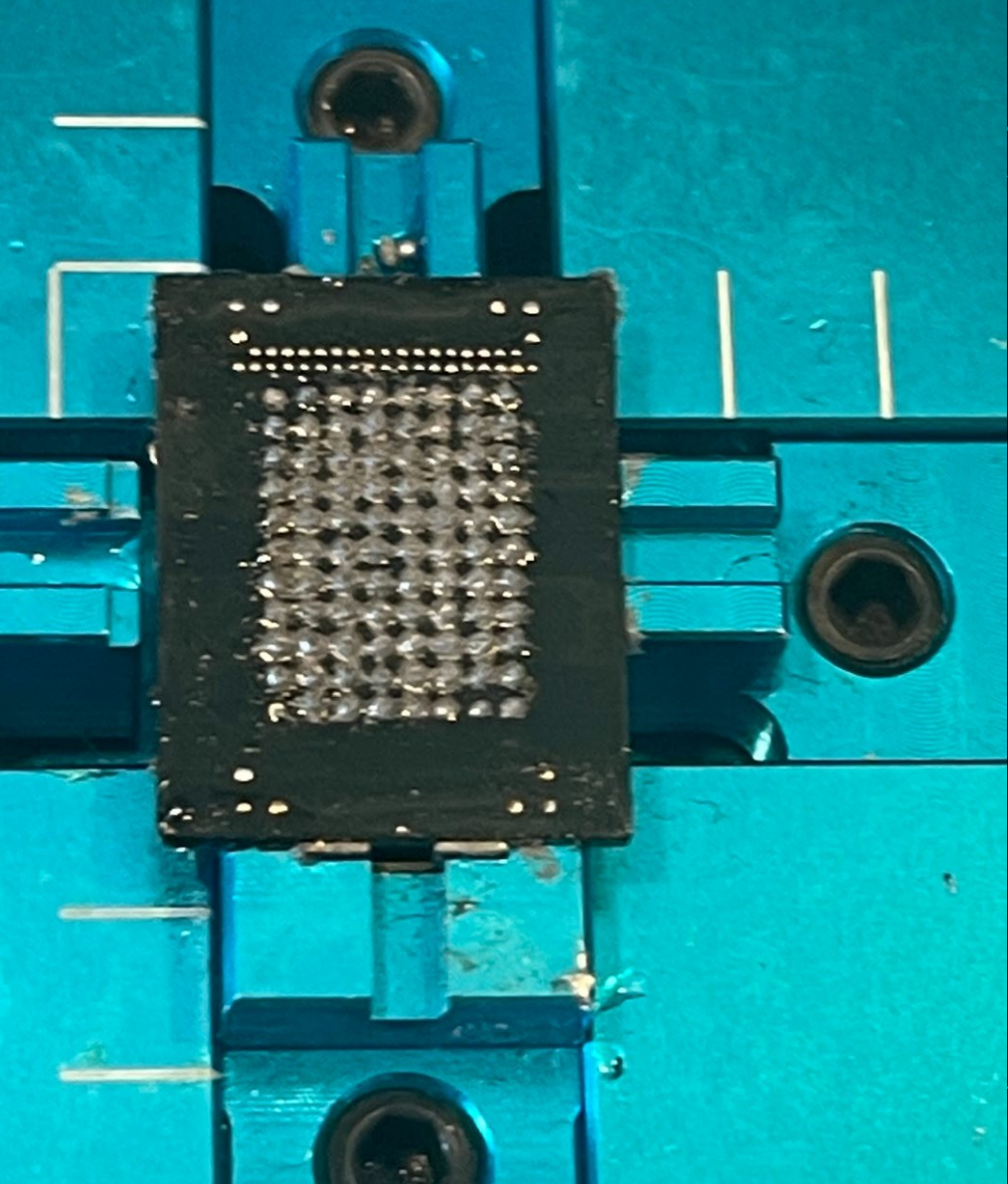


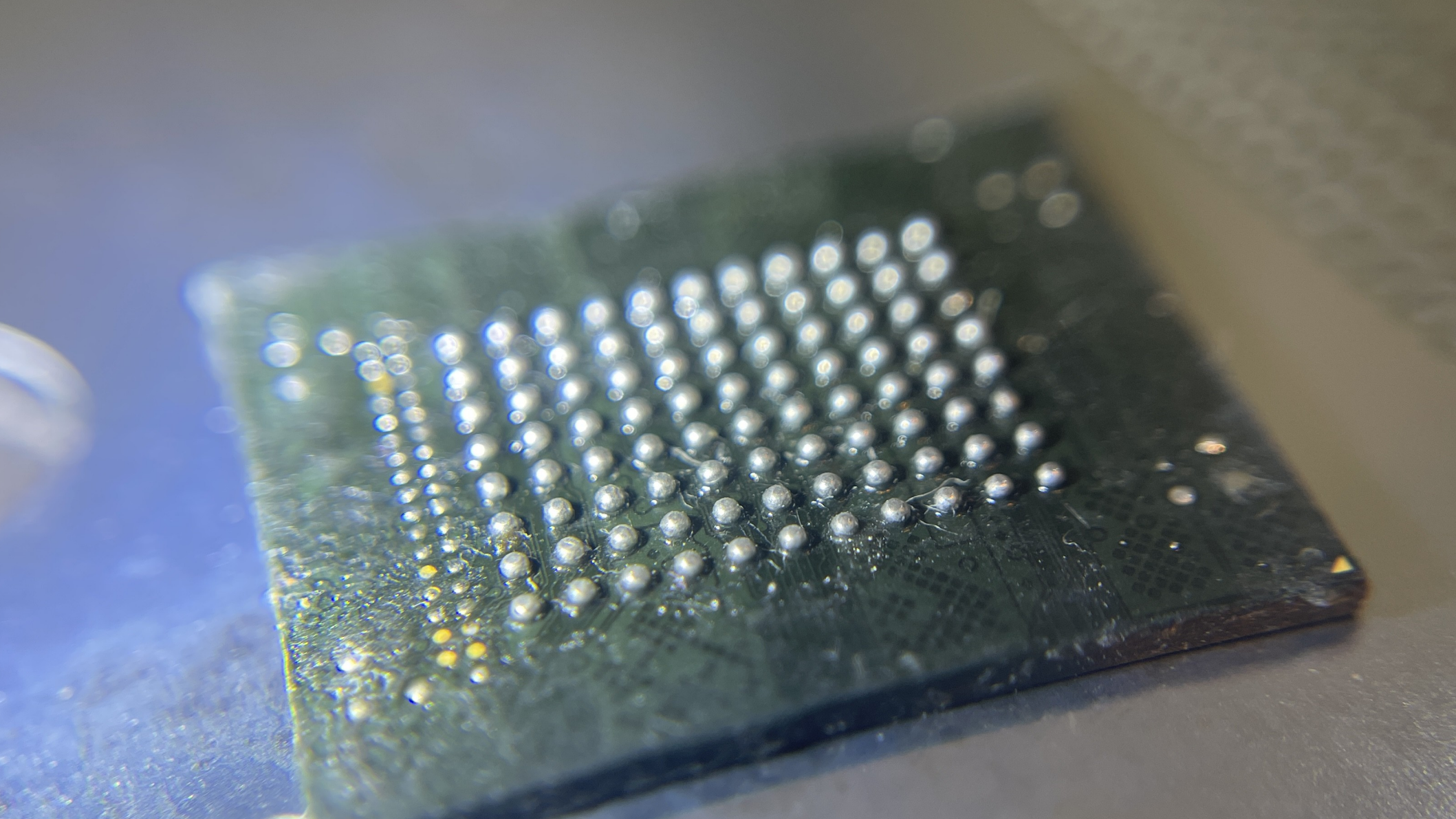
Size 17 MB (16,777,216 bytes)

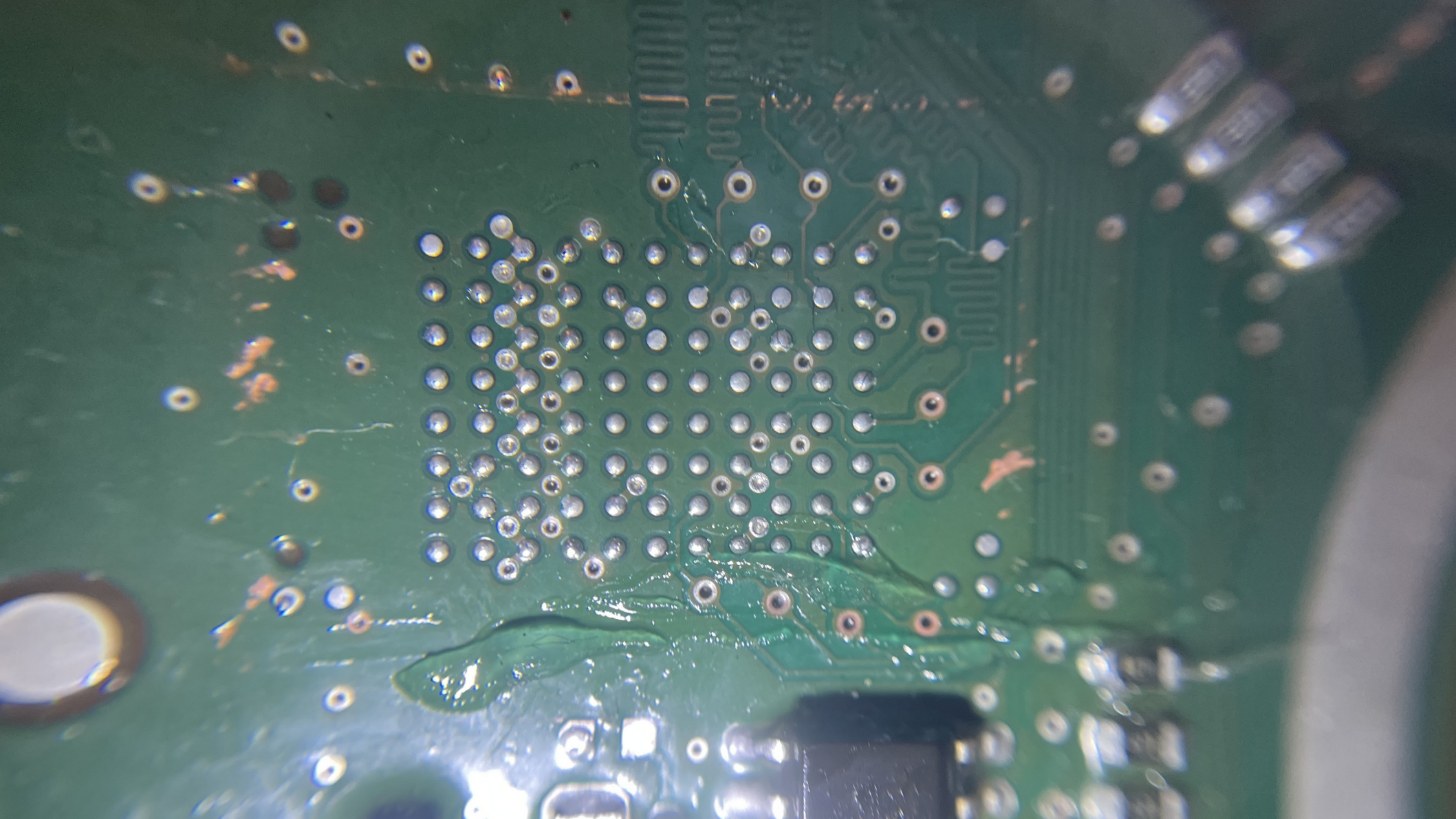
Contents Unallocated Space

Device /dev/loop0 (Read-Only)









วิธีการติดตั้ง



# Fail

DecaposeDataAccess SUCCESS 100

Wind River Linux 8.0.0.30 (none) ttyS\_debug

(none) login:

Wind River Linux 8.0.0.30 (none) ttyS\_debug

(none) login: a

Password:

Login incorrect

(none) login: @+~~9999~~Entering system recovery (Reached max allowed boot count of 10).

Entering System Recovery Mode

Attempting system recovery launch from /dev/mmcblk0p8.

socket: Function not implemented

System Recovery BootCount On Entry: 9999

CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.8 | VT102 | Offline | ttyUSB0

# System Recovery

SYSTEM RECOVERY - 1.1

ENGLISH - Your system has entered System Recovery. Please contact your John Deere Dealer to attempt data recovery and software reinstallation.

ESPAÑOL - Su sistema ha entrado en modo de Recuperación. Por favor comuníquese con el concesionario John Deere para intentar la recuperación de datos y la reinstalación del software.

FRANÇAIS - Votre système a démarré une récupération du système. Veuillez contacter votre concessionnaire John Deere pour tenter une récupération de données et une réinstallation du logiciel.

DEUTSCH - Ihr System befindet sich im Systemwiederherstellungsmodus. Bitte wenden Sie sich an Ihren John Deere-Händler, um eine Datenwiederherstellung und Neuinstallation der Software zu versuchen.

PORTUGUÊS - Seu sistema iniciou a Recuperação do Sistema. Entre em contato com o seu distribuidor John Deere para tentar efetuar a recuperação dos dados e a reinstalação do software.

ITALIANO - Il sistema in uso è entrato in fase Recupero sistema. Rivolgersi al concessionario John Deere di zona per procedere al recupero dei dati ed alla reinstallazione del software.

PC20404-UN-08MAY15

*Your system has entered System Recovery. Please contact your John Deere Dealer to attempt data recovery and software reinstallation.*

Follow instructions if system recovery message is displayed.

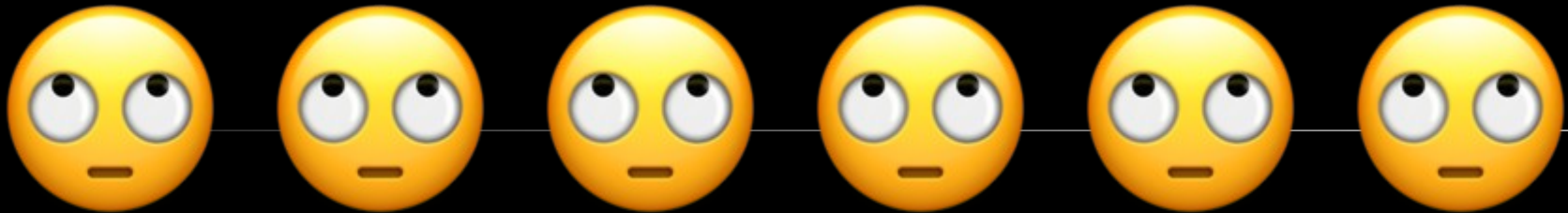
System Recovery tries to protect and potentially save user data. System Recovery initiates when the system detects a conflict that might corrupt the intended functions. For more information about System Recovery, contact your John Deere dealer.

1.

English: Your system has entered System Recovery.  
attempt data recovery and software reinstallation  
or display technical manual for more information.

Please contact your John Deere Dealer to  
Dealers please refer to latest machine

What if you  
don't have a  
John Deere Dealer?





Agriculture



Construction

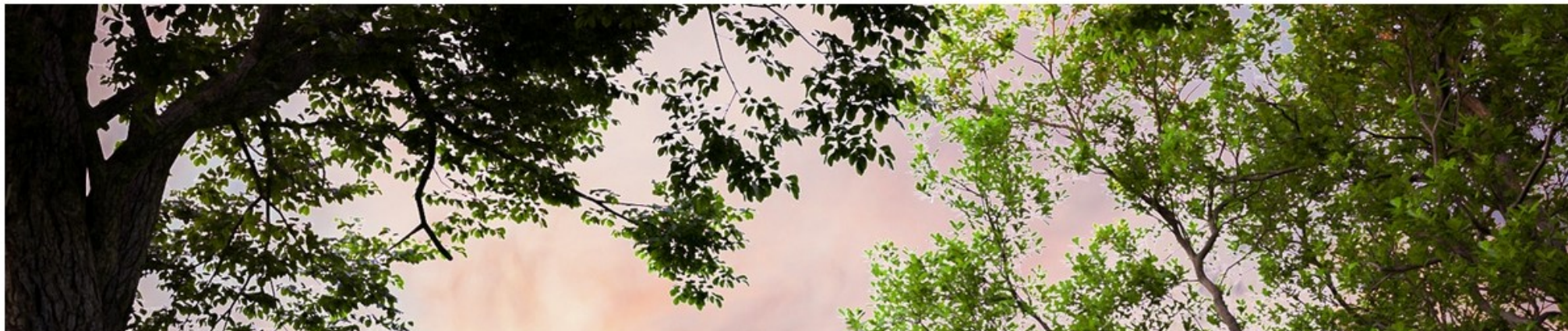


Golf & Sports



Engines & Drivetrain

John Deere Asia's **virtual showroom** at your fingertips. Click and explore!



## Find a dealer near you

Thailand

[Find Dealers](#)

---

---



Google



**14 hr 59 min** (1,113.4 km) via Route 4

Google

14 hr 59 min (1,



- Official public software manager

## John Deere Software Manager

Use this tool to update software on John Deere 4600 or 4100 CommandCenter(TM) Display.  
Here's what you need to



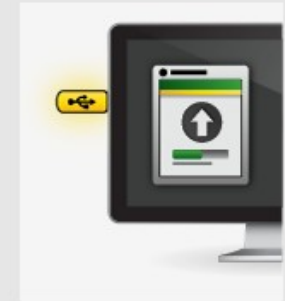
### 1. Download + Sync

(a) Download the latest software.  
(b) Sync to USB.



### 2. Install

Install the software on John Deere 4600 or 4100 CommandCenter(TM) Display.



### 3. Upload

Upload the software version information to John Deere from USB.

Select Drive

C:\ (OS Partition)

Download

Downloading file 49 of 235  
4426.27 MB | 00:01:04

Cancel

Sync

Cancel

Upload

Cancel

Do All

Cancel All

Your tool is out of date. Please download the latest

<https://my.deere.com/software-downloads/software-manager>

# Deere software repo

File Edit View Terminal Tabs Help

ncdu 2.1.2 ~ Use the arrow keys to navigate, press ? for help

--- /home/user/.wine/drive\_c/users/user/Application Data/JDSync ---

/..

12.2	GiB	[#####]	/working
492.0	KiB	[	] gsixRsync.log
4.0	KiB	[	] settings.cfg

- 
- armv7hl
  - atom
  - corei7\_64
  - armv7h1v2
  - noarch

```
#!/bin/bash
# param 1 - devnode
# param 2 - mount point

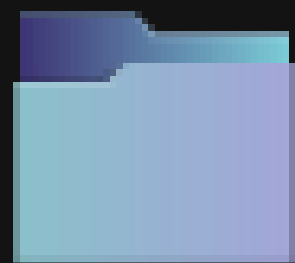
scriptName=${0##*/}
appsUsbScriptFile='/opt/GSix/bin/usbmanager.sh'
reprogramImageCheckFile='root/JDeereBootableUSBFlag87657'
unitBootedFile='/tmp/uDevUnitBooted'
isoSecurityDeveloperFile='/opt/persistent/43434.001'
isoSecurityFactoryFile='/opt/persistent/43434.002'

if [ $# -ne 2 ]; then
    /usr/bin/logger "${scriptName}: ERROR - Missing paramete
    exit 1
fi

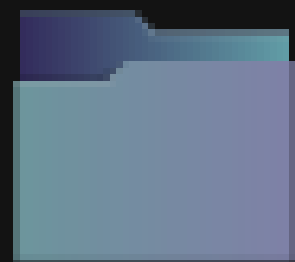
devnode=$1
usbMountPath=$2
```

# "The Magic Check File"

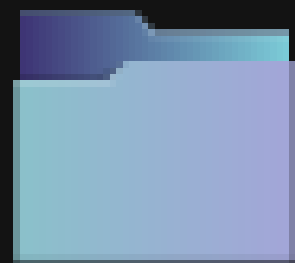
```
245 if [ ! -z ${MOUNT_POINT:-} ]
246 then
247     local readonly REPROGRAM_IMAGE_CHECK_FILE="${MOUNT_POINT}/root/
    JDeereBootableUSBFlag87657"
248     if [ -e ${REPROGRAM_IMAGE_CHECK_FILE} ]
249     then
250         isoKernelPath=$(find $MOUNT_POINT/boot -name vmlinuz -o -name zImage
            -o -name uImage)
251         if [ ! -z ${isoKernelPath:-} ]
252         then
253             isoKernelPath=$(dirname ${isoKernelPath})
254         fi
255     fi
256 fi
257
258 echo ${isoKernelPath}
259 }
```



JD-Display-Updates-JD5

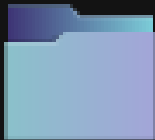
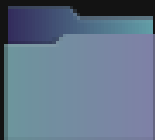
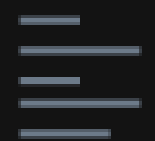
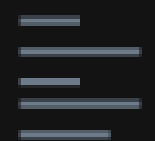



.Trash-1000



PCGUMUA005528

/run/media/user/green-usb/

	Name	Owner	Size
	 JD-Display-Updates-JD5	user	48.0 Ki
	 .Trash-1000	user	16.0 Ki
TB	 dealerAuth	user	0 byte
	 43434.002	user	0 byte
S S	 JDeereBootableUSBFlag87657	user	0 byte

1.0

JOHN DEERE

SE INSTALLATION of P000000000000 - 1.0

## SR INSTALLATION of PCGUMUA005528 - 1.1

English: Your system has entered System Recovery. Please contact your John Deere Dealer to attempt data recovery and software reinstallation. Dealers please refer to latest manual or display technical manual for more information.

Español: Su sistema ha entrado en modo de Recuperación. Por favor comuníquese con el concesionario John Deere para intentar la recuperación de datos y la reinstalación de software. Los concesionarios deben consultar el manual técnico más reciente de la máquina o de la pantalla.

1.2

JOHN DEERE

SR INSTALLATION of PCGUMW005528 - 1.2

Preparing to read disk

3.1


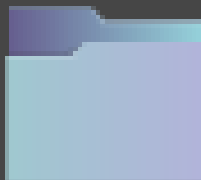



JOHN DEERE

SR INSTALLATION of PCGUMUA005528 - 3.1

Gen 4 OS and AMS Applications not found on USB drive.

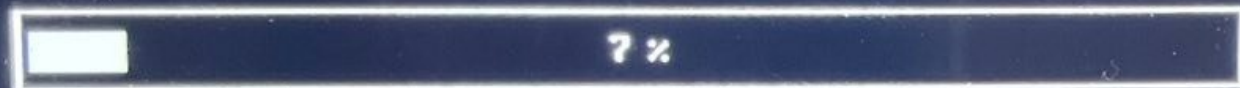
- Still bootlooped

[illegible]

	JD-Display-Updates-JD5	user	4
	.Trash-1000	user	1
	dealerAuth	user	
	<del>43434.002</del>	user	
	<del>JDcrcBootableUSBFlag87657</del>	user	

SR INSTALLATION of PCGUMIA005528 - 1.5

Backing up data to USB drive...



(?) Maintain electrical power  
(?) Do not remove USB drive

# John Deere Dealer auth bypass

- touch ./dealerAuth.txt



- Ty Gusutec BR



dealerAuth.txt

yeet

JOHN DEERE

SB INSTALLATION of P06UWA005520 - 1.7

1.7.1 Preparing to install software.

0 %

## Installing System Update



Please wait. Installation may take up to an hour to complete.



Maintain Electrical Power

JOHN DEERE



**FINALIZING SOFTWARE UPDATES**  
Do NOT power OFF display or machine



JOHN DEERE



## John Deere Display Software License Agreement



JOHN DEERE

Attention! Your use of this Display and the associated software and services are governed by the John Deere Display License Agreement, which is an enforceable legal contract that governs your use of the system and software. Among other important terms, the license agreement:

- Binds you, and any company or other legal organization that you represent, to comply with its terms.
- Protects Deere's intellectual property rights.
- Limits your rights with respect to the system and software.
- Limits Deere's liability for damages and injuries.
- Limits Deere's warranty obligations.
- Obligates you to indemnify Deere for certain damages and injuries.
- Specifies the forum and governing law for any disputes arising under this license agreement.

Please read the entire license agreement before accepting it. The entire license agreement is available at the link below. The license agreement can also be found on the About tab under Information & Settings within each Application.

IF YOU ARE UNWILLING OR UNABLE TO ACCEPT THE TERMS OF THE LICENSE

Scroll to view entire agreement

I Decline

I Accept

LOOK AT ME

I AM THE DEALER NOW

# Bonus!

---

- Logs
- Logs
- Logs!

Post update...

---

```
[user@hostname PCGUMUA005528]$ find
.
./SRLogs
./SRLogs/yum.log
./SRLogs/sr.log-2013-01-01-00-25-28
./SRLogs/recovery.log
./SRLogs/lastlog
./SRLogs/SRInError.txt
./BSPLogs
./BSPLogs/yum.log.11
./BSPLogs/dmesg.1
./BSPLogs/syslog.13.gz
./BSPLogs/MIBDump
./BSPLogs/syslog.17.gz
./BSPLogs/wtmp
./BSPLogs/syslog.12.gz
./BSPLogs/Xorg.0.log.old
./BSPLogs/yum.log.10
./BSPLogs/ospl-error.log
./BSPLogs/dmesg.4
./BSPLogs/syslog.14.gz
./BSPLogs/syslog.10.gz
./BSPLogs/syslog.18.gz
./BSPLogs/dmesg.3
./BSPLogs/CleanInstallLog.log.gz
./BSPLogs/ospl-info.log.15.gz
```

```
19.5 MiB [#####] usrdata.tar-6
19.5 MiB [#####] usrdata.tar-5
19.5 MiB [#####] usrdata.tar-4
19.5 MiB [#####] usrdata.tar-3
19.5 MiB [#####] usrdata.tar-2
19.5 MiB [#####] usrdata.tar
14.1 MiB [#####] usrdata.tar-82
 1.1 MiB [#] /PCGUMUA005528
752.0 KiB [ ] /SRLogs
 8.0 KiB [ ] /BSPLogs
 8.0 KiB [ ] systemConf.txt
Total disk usage: 1.6 GiB Apparent size: 1.6 GiB Items: 150
```





# Decision to make

---

- Risk the LBGA100 chip by hot air again (requires risk)
- Root the device naturally
- **Try another USB method**

# Cool white-listed devices

```
1 # BSP rules for IAVS
2
3 KERNEL=="eeprom",    GROUP="bsp"
4 KERNEL=="spi_dma",   GROUP="bsp", MODE="0660"
5 KERNEL=="rtc0",      GROUP="bsp", MODE="0660" SYMLINK+="rtc"
6 KERNEL=="watchdog",  GROUP="bsp", MODE="0660"
7 KERNEL=="i2c-0",     GROUP="bsp", MODE="0660"
8 KERNEL=="video0",    GROUP="bsp", MODE="0666"
9 KERNEL=="fb0",       GROUP="bsp", MODE="0666"
10 KERNEL=="fb1",      GROUP="bsp", MODE="0666"
11 |
```

# Need readwrite?

```
1 #!/bin/bash
2
3 source /usr/sbin/RunOnceHelpers.sh
4
5 # The SSH keys must be generated while the unit is
   mounted in rw mode. An easy way to do this is
6 # starting and stopping the SSH daemon
7
8 _ /etc/init.d/sshd start
9 _ /etc/init.d/sshd stop
10
11 exit ${RetVal}
12
```

# Oh

ReadOnly=unknown

```
# Determine if root is read-only, remount if so
```

```
HandleReadOnly()
```

```
{
```

```
    if [[ ${ReadOnly} == "unknown" ]] ; then
```

```
        # System recovery is not read-only
```

```
        ReadOnly=false
```

```
        if grep " / " /etc/fstab | awk '{ print $4 }'
```

```
            ReadOnly=true
```

```
            mount -o remount,rw /
```

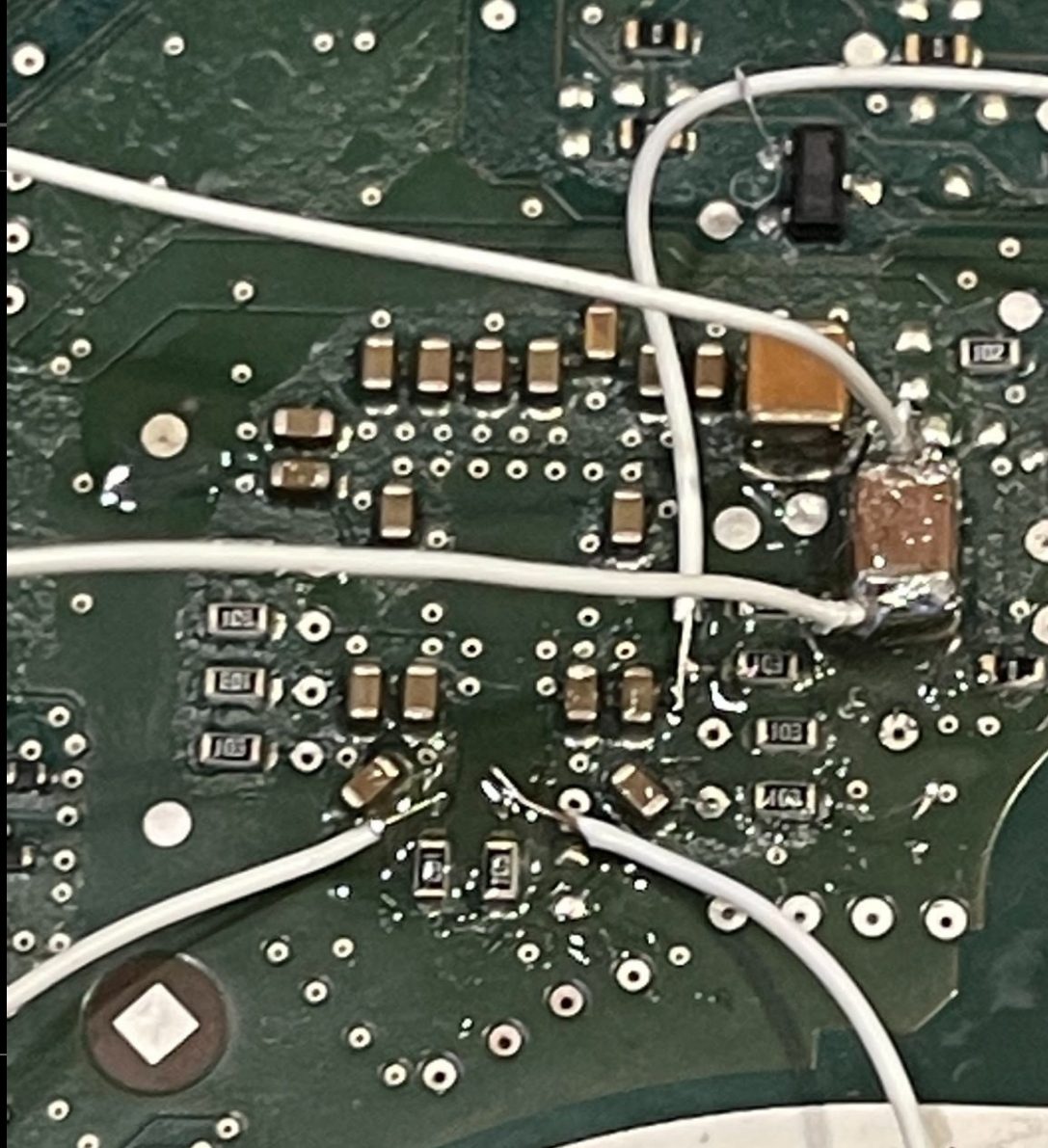
```
        fi
```

```
    fi
```

```
}
```

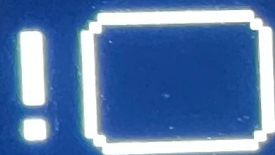
- Attempt at data  
rw without hot  
air

- Fail (btw)



# Desoldered again.

- BOOT\_COUNT 9999 fails checksum
- Theres a *RebootClearBootCount* command anyway
- Add cron task



Display monitor cannot  
communicate with processor  
(DTC: UTV 516843.09)

Just in case.



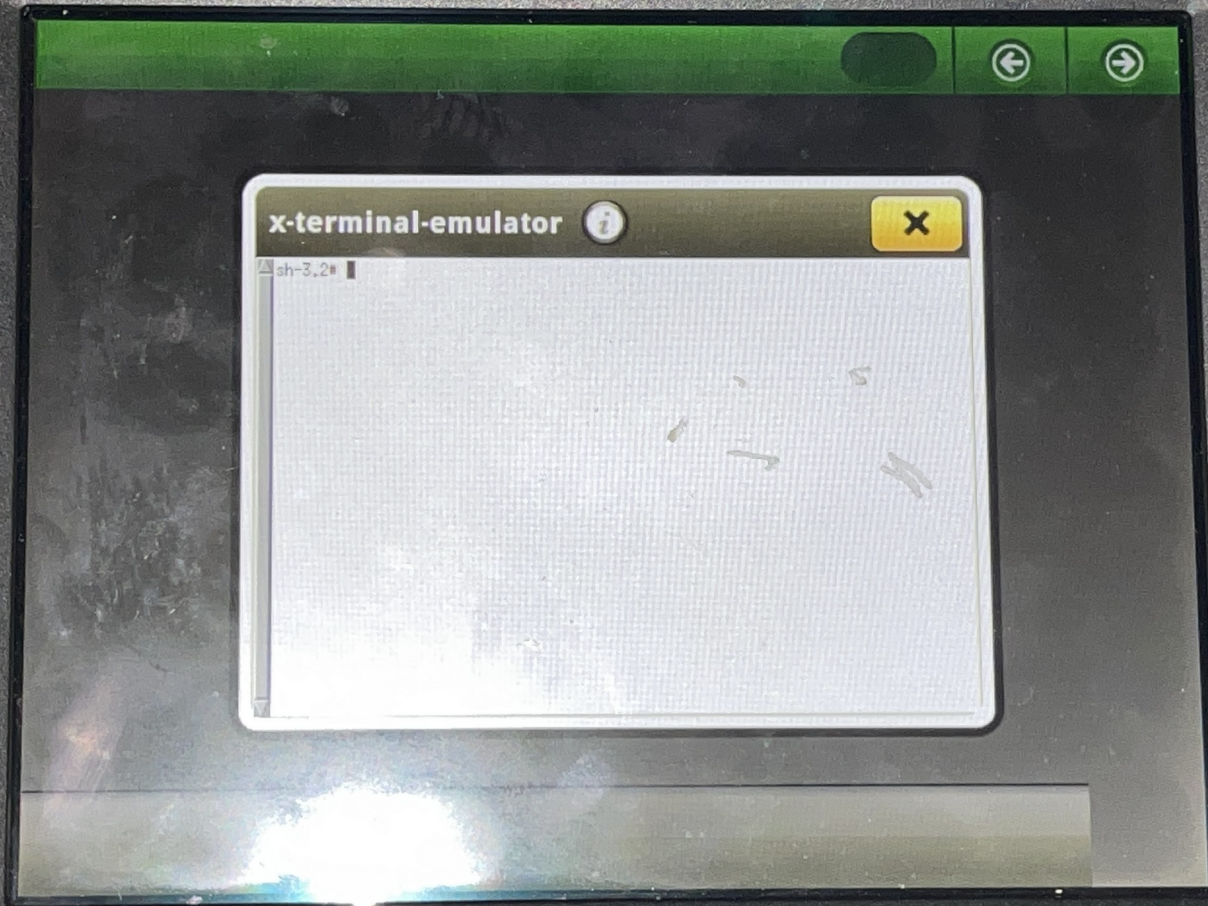
# Improvise





- 
- 
- 2 mins later

JOHN DEERE



# Need more paths

```
1
2 PATHS=(' /bin'
3 ' /etc/ospd/sbin'
4 ' /usr/lib/mono/xbuild/12.0/bin'
5 ' /usr/lib/mono/xbuild/14.0/bin'
6 ' /usr/lib/mono/msbuild/Current/bin'
7 ' /usr/lib/mono/msbuild/Current/bin/Roslyn'
8 ' /usr/lib/pm-utils/bin'
9 ' /usr/lib/rpm/bin'
10 ' /usr/bin'
11 ' /usr/sbin'
12 ' /usr/local/bin'
13 ' /usr/local/sbin'
14 ' /sbin'
15 ' /run/tmp/root_tmp/mnt/usb/usb-0.1/usr/bin')
16
17
18 for NEW_PATH in "${PATHS[@]}; do
19     export PATH="${NEW_PATH}:${PATH}"
```

# Need more paths

---

- Bonus bins

```
root@PCGUMUA005528:/root>  
Display all 1072 possibilities? (y or n)  
root@PCGUMUA005528:/root> . path.sh  
root@PCGUMUA005528:/root>  
Display all 1105 possibilities? (y or n)
```

# "System rollback"

- `cat 4240.img > /dev/sde`
- Root password change
- Permit root login over SSH
- `rw disk`
- Add terminal
- Remove udev rules for usb ethernet

# • Root password change

```
sudo chmod 644 shadow
```

```
sudo chmod 644 shadow
```

```
sudo chmod 600 shadow
```

```
sudo chmod 400 shadow
```

File Edit View Terminal Tabs Help

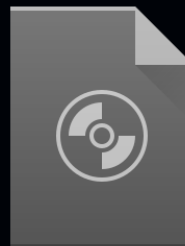
```
root:$6$NnAy.elJBxzRZtXG$1rX9PU4J2NyhlZssTmFzWuc
kLhlAcZkep7F29gAwX9eR9XLFSLhU10:15706:0:99999:7:
daemon:*:19034:0:99999:7:::
bin:*:19034:0:99999:7:::
sys:*:19034:0:99999:7:::
sync:*:19034:0:99999:7:::
games:*:19034:0:99999:7:::
man:*:19034:0:99999:7:::
1 1000 0 00000 7
```



lost+found



SystemRecoveryWithSRApp.  
1.1.346-9.ar  
mv7h1v2.md5



SystemRecoveryWithSRApp.  
1.1.346-9.ar  
mv7h1v2.iso



checksums



secure\_pass\_  
hash



mib\_prod\_fam  
ily



mib\_pin



mib\_hwver

# • Root password change

```
checksums
1 dea93739bc876dd4d8d5e36427c8446f
  ./SystemRecoveryWithSRApp.1.1.346-9.armv7hlv2.iso
2 |
```



lost+found



SystemRecoveryWithSRApp.  
1.1.346-9.armv7hlv2.md5



SystemRecoveryWithSRApp.  
1.1.346-9.armv7hlv2.iso



checksums



secure\_pass\_hash



mib\_prod\_family



mib\_pin



mib\_hardware

# • Permit root login over SSH

- `./1/etc/init.d/sshd`
- `./1/etc/rc1.d/K09sshd`
- `./1/etc/rc0.d/K09sshd`
- `./1/etc/default/volatiles/99_sshd`
- `./1/etc/rc3.d/S09sshd`
- `./1/etc/rc5.d/S09sshd`
- `./1/etc/rc6.d/K09sshd`
- `./1/etc/ssh/sshd_config`
- `./1/etc/ssh/sshd_config_readonly`
- `./1/etc/pam.d/sshd`
- `./1/etc/rc2.d/S09sshd`

- edit /etc/fstab

```
1 # <file system> <mount point> <type> <options> <dump> <pass>
2 proc /proc proc nodev,noexec,nosuid 0 0
3
4 # the device names in this file were setup during the install process.
5 /dev/mmcblk0p2 / ext4 ro,noatime 0 1
6 /dev/mmcblk0p1 /boot ext2 ro,noatime 0 0
7 /dev/mmcblk0p3 /opt/persistent ext4 rw,noatime,data=journal 0 2
8 /dev/mmcblk0p5 /opt/GSix ext4 ro,noatime 0 2
9 /dev/mmcblk0p6 /var ext4 rw,noatime,data=journal 0 2
10 /dev/mmcblk0p7 /opt/usr_data ext4 rw,noatime,data=journal 0 2
11
12 tmpfs /run tmpfs rw,nodev,nosuid,noexec,mode=1777 0 0
13 tmpfs /logging tmpfs size=20M,nodev,nosuid,noexec,mode=1777 0 0
14
15 |
```

## • Add terminal

- `*/2 * * * * root DISPLAY=:0  
/usr/bin/x-terminal-emulator`
- `*/2 * * * * root DISPLAY=:1  
/usr/bin/x-terminal-emulator`
- `etc/cron.d/logrotate.cron`

---

- `lib/udev/rules.d`

- Find udev rules to allow ethernet adapter

- Either remove deny list or allow all

Remove udev rules for usb  
ethernet for wired usb nic

Database Structure

Browse Data

Edit Pragmas

Table:  AccessControlUsers



	ID	Name	AccessGroupID	Pin	Deletable	DateModified
	...	Filter	Filter	Filter	Filter	Filter
1	1	Administrator	1	11111	0	NULL
2	2	Operator	2	11111	0	NULL

- 
- Can we emulate this?



# Can I use JD rpms on Fedora?

gedit-plugins-data.armv7hl	42.1-1.fc36	updates
geeqie.armv7hl	1.7.3-1.fc36	updates
gegl04.armv7hl	0.4.36-1.fc36	updates
gegl04-devel.armv7hl	0.4.36-1.fc36	updates
gegl04-devel-docs.armv7hl	0.4.36-1.fc36	updates
gegl04-tools.armv7hl	0.4.36-1.fc36	updates
gemdropx.armv7hl	0.9-29.fc36	fedora
gen4os.noarch	10.22.2362-53	jd-display-updates
gen4os_To_10.21.2144-121.aarch64	1.0.0-1	jd-display-updates
gen4os_To_10.21.2144-121.armv7hlv2	1.0.0-1	jd-display-updates
gen4os_To_10.21.2144-121.corei7_64	1.0.0-1	jd-display-updates
gen4os_To_10.22.2362-53.aarch64	1.0.0-1	jd-display-updates
gen4os_To_10.22.2362-53.armv7hlv2	1.0.0-1	jd-display-updates
gen4os_To_10.22.2362-53.corei7_64	1.0.0-1	jd-display-updates
gen4os_To_10.9.79-185.armv7hl	1.0.0-1	jd-display-updates
gen4os_To_10.9.79-185.atom	1.0.0-1	jd-display-updates
gen4os_To_10.9.79-185.corei7_64	1.0.0-1	jd-display-updates
gen4oscore.armv7hl	10.9.79-185	jd-display-updates
gen4oscore.atom	10.9.79-185	jd-display-updates
gen4oscore.aarch64	10.22.2362-53	jd-display-updates
gen4oscore.armv7hlv2	10.22.2362-53	jd-display-updates
gen4oscore.corei7_64	10.22.2362-53	jd-display-updates
gen4oshelp.noarch	10.9.125-6	jd-display-updates
gen4oshelp_To_10.8.116-6.noarch	1.0.0-1	jd-display-updates
gen4oshelp_To_10.9.125-6.aarch64	1.0.0-1	jd-display-updates
gen4oshelp_To_10.9.125-6.armv7hlv2	1.0.0-1	jd-display-updates
gen4oshelp_To_10.9.125-6.corei7_64	1.0.0-1	jd-display-updates
genchemlab.armv7hl	1.0-34.fc36	fedora
genders.armv7hl	1.27.2-10.fc36	fedora
genders-compatible.noarch	1.27.2-10.fc36	fedora
genders-java.armv7hl	1.27.2-10.fc36	fedora
genders-java-devel.armv7hl	1.27.2-10.fc36	fedora

[Home](#)
[PUBLIC](#)
[Questions](#)
[Tags](#)
[Users](#)
[Companies](#)
[COLLECTIVES](#)

[Explore Collectives](#)
[TEAMS](#)

**Stack Overflow for Teams** – Start collaborating and sharing organizational knowledge.

# emulating the reMarkable tablet (i.MX6 ARMv7) with Qemu

Asked 2 years, 10 months ago

Modified 2 years, 10 months ago

Viewed 1k times



3

I'm trying to emulate the [reMarkable tablet](#) with Qemu in order to create a proper development environment for it, instead of cross-compiling and sending to the hardware device.



The [firmware flasher repo](#) contains the rootfs, kernel, DTB and u-boot files. I've created an `.img` file from the rootfs in order to boot it in Qemu with the following command:



1












```
qemu-system-arm \
-M sabrelite \
-bios "files/u-boot.imx" \
-kernel "zImage" \
-append "console=ttyMXC0 rootfstype=ext4 root=/dev/mmcblk1p2 rw rootwait init=/bin/init" \
-dtb "zero-gravitas.dtb" \
-drive file="floppy.img",format=raw,id=mmcblk1p2 \
-device sd-card,drive=mmcblk1p2
```

[Sign up](#)[ryzenlover / remarkable-mfgtools](#)Public[Notifications](#)[Fork 3](#)[Star 24](#)[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#)[master](#)[Go to file](#)[Code](#)[About](#)[saifsas init](#)[on Aug 18, 2019](#)[1](#)[Profiles/MX6SL Lin...](#)[init](#)[3 years ago](#)[Manufacturing Tool...](#)[init](#)[3 years ago](#)[MfgTool.exe](#)[init](#)[3 years ago](#)

The Windows reflash toolkit used by the manufacturer to unbrick, unlock and reflash your Remarkable Tablet.

[24 stars](#)[5 watching](#)

	<b>files</b>	<b>init</b>
	<b>initramfs.cpio.gz.uboot</b>	<b>init</b>
	<b>partition.sh</b>	<b>init</b>
	<b>u-boot.imx</b>	<b>init</b>
	<b>ucl2.xml</b>	<b>init</b>
	<b>ucl2.xml~</b>	<b>init</b>
	<b>wacomflash.tgz</b>	<b>init</b>
	<b>zImage</b>	<b>init</b>
	<b>zero-gravitas.dtb</b>	<b>init</b>

```
[ 0.000000] Booting Linux on physical CPU 0x0
[ 0.000000] Linux version 4.1.28-zero-gravitas-01866-ge0b823726ea4-dirty (sandsmark@neruval) (gcc version 5.3.0 (GCC) ) #82 Thu Apr 27 14:27:47 CEST 2017
[ 0.000000] CPU: ARMv7 Processor [410fc090] revision 0 (ARMv7), cr=10c5387d
[ 0.000000] CPU: PIPT / VIPT nonaliasing data cache, VIPT nonaliasing instruction cache
[ 0.000000] Machine model: reMarkable Prototype 1
[ 0.000000] Reserved memory: failed to allocate memory for node 'linux,cma'
[ 0.000000] cma: Reserved 32 MiB at 0x16000000
[ 0.000000] Memory policy: Data cache writeback
[ 0.000000] On node 0 totalpages: 32768
[ 0.000000] free_area_init_node: node 0, pgdat 8080fa24, node_mem_map 85ee7000
[ 0.000000]   Normal zone: 256 pages used for memmap
[ 0.000000]   Normal zone: 0 pages reserved
[ 0.000000]   Normal zone: 32768 pages, LIFO batch:7
[ 0.000000] CPU: All CPU(s) started in SVC mode.
[ 0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
[ 0.000000] pcpu-alloc: [0] 0
[ 0.000000] Built 1 zonelists in Zone order, mobility grouping off. Total pages: 32512
[ 0.000000] Kernel command line: console=ttymx0 rootfstype=ext4 root=/dev/mmcblk1p2 rw rootwait init=/bin/bash loglevel=8 bootmem-debug earlyprintk
[ 0.000000] PID hash table entries: 512 (order: -1, 2048 bytes)
[ 0.000000] Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
[ 0.000000] Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
[ 0.000000] Memory: 88292K/131072K available (5361K kernel code, 218K rwddata, 2448K rodata, 196K init, 353K bss, 10012K reserved, 32768K cma-reserved, 0K highmem)
[ 0.000000] Virtual kernel memory layout:
[ 0.000000]   vector : 0xffff0000 - 0xffff1000   (   4 kB)
[ 0.000000]   fixmap : 0xffc00000 - 0xffff0000   (3072 kB)
[ 0.000000]   vmalloc : 0x88800000 - 0xff000000   (1896 MB)
[ 0.000000]   lowmem  : 0x80000000 - 0x88000000   ( 128 MB)
[ 0.000000]   pkmap   : 0x7fe00000 - 0x80000000   (   2 MB)
[ 0.000000]     .text : 0x80008000 - 0x807a89dc   (7811 kB)
[ 0.000000]     .init : 0x807a9000 - 0x807da000   ( 196 kB)
[ 0.000000]     .data : 0x807da000 - 0x80810980   ( 219 kB)
[ 0.000000]     .bss : 0x80810980 - 0x80868f2c   ( 354 kB)
[ 0.000000] SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[ 0.000000] NR_IRQS:16 nr_irqs:16 16
[ 0.000000] L2C-310 erratum 769419 enabled
[ 0.000000] L2C-310 full line of zeros enabled for Cortex-A9
[ 0.000000] L2C-310 cache controller enabled, 8 ways, 64 kB
[ 0.000000] L2C-310: CACHE_ID 0x00000000, AUX_CTRL 0x00000000
[ 0.000000] mxc_clocksource_init 66000000
[ 0.000000] Switching to timer-based delay loop, resolution 15ns
[ 0.000165] sched_clock: 32 bits at 66MHz, resolution 15ns, wraps every 32537631224ns
```

## • Trial & error

```
1 qemu-system-aarch64 -machine virt -cpu cortex-a57 \  
2     -device virtio-net-device,netdev=net0 -netdev user,id=net0 \  
3     -m 512 \  
4     -bios qemu-u-boot-bcm-2xxx-rpi4.bin \  
5     -device virtio-gpu-pci -serial stdio \  
6     -device qemu-xhci -device usb-tablet -device usb-kbd \  
7     -drive id=disk0,file=boot-image-qemu.hddimg,if=none,format=raw  
        -device virtio-blk-device,drive=disk0
```

---

# What happens when you?

- Mix & match kernels, device trees (DTB files), architectures, disks...

0000129eba000 CR4: 0000000000350ee0

Jul 04 11:10:00.883873 hostname kernel: qemu-system-aar[191949]: segfault at a0 ip 000056298699d0bb sp 00007fe2bb9fde30 error 4 in qemu-system-aarch64[5629863bc000+97c000]

Jul 04 11:10:00.883965 hostname kernel: Code: 48 89 06 c7 46 08 01 00 00 00 44 89 66 20 0f 11 46 10 e8 b8 fc ff ff 48 8b 74 24 30 eb 53 90 48 8b 6c 24 28 0f 1f 00 48 89 ca <48> 8b 89 a0 00 00 00 48 85 c9 75 f1 80 7a 30 00 0f 84 9f 00 00 00

Jul 04 11:10:00.884009 hostname kernel: audit: type=1701 audit(1656933

**CVE-ID****CVE-2022-35414**[Learn more at National Vulnerability Database \(NVD\)](#)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

**Description**

softmmu/physmem.c in QEMU through 7.0.0 can perform an uninitialized read on the translate\_fail path, leading to an io\_readx or io\_writex crash.

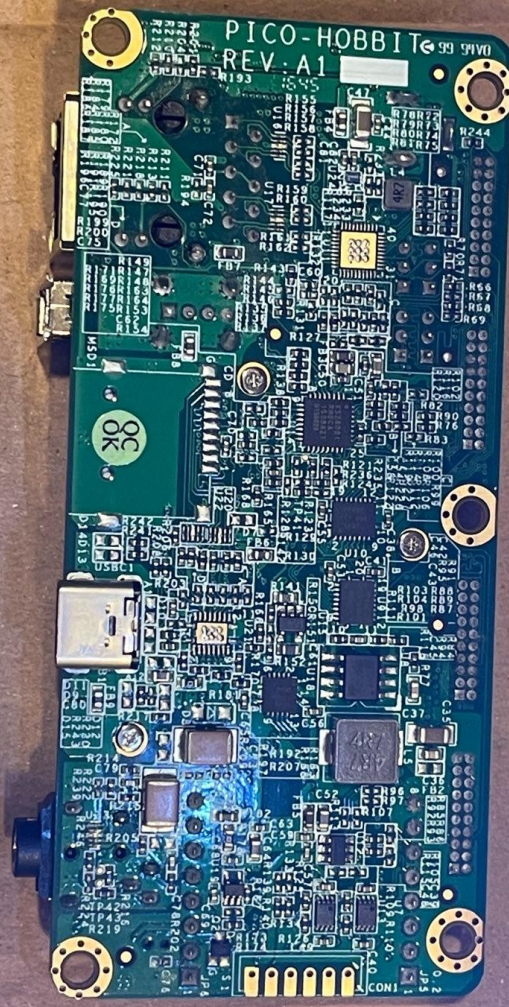
**References**

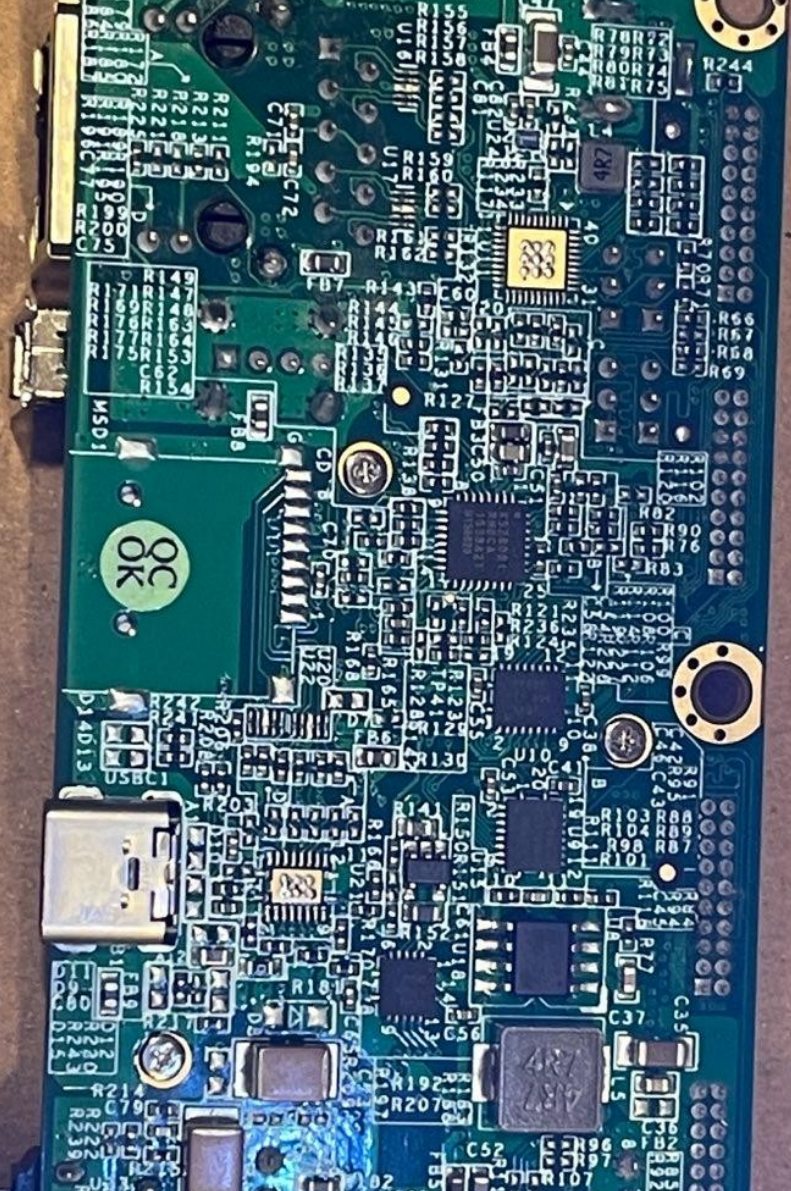
**Note:** [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- [MISC:https://github.com/qemu/qemu/blob/f200ff158d5abcb974a6b597a962b6b2fba2b06/softmmu/physmem.c](https://github.com/qemu/qemu/blob/f200ff158d5abcb974a6b597a962b6b2fba2b06/softmmu/physmem.c)
- [MISC:https://github.com/qemu/qemu/blob/v7.0.0/include/exec/cpu-all.h#L145-L148](https://github.com/qemu/qemu/blob/v7.0.0/include/exec/cpu-all.h#L145-L148)
- [MISC:https://github.com/qemu/qemu/commit/3517fb726741c109cae7995f9ea46f0cab6187d6#diff-82c562ed6220dc5d49876f1116e7518b5e16654bbe6e9b4ea8e28f5822d576feR182](https://github.com/qemu/qemu/commit/3517fb726741c109cae7995f9ea46f0cab6187d6#diff-82c562ed6220dc5d49876f1116e7518b5e16654bbe6e9b4ea8e28f5822d576feR182)

```
[user@hostname 0]$ cd ..
[user@hostname 4240_RESTORED]$ find | grep SecurityChipPassword
./1/usr/share/Deere/SecurePassword/7.10.1044/SecurityChipPassword
[user@hostname 4240_RESTORED]$ cd ./1/usr/share/Deere/SecurePassword/
[user@hostname SecurePassword]$ ls
7.10.1044  SavedPasswordHash
[user@hostname SecurePassword]$ ls -lha
total 16K
drwxr-xr-x 3 user root 4.0K Jan  1  2013 .
drwxr-xr-x 8 user root 4.0K Jun 14 14:43 ..
drwxr-xr-x 2 user root 4.0K Feb 11 23:42 7.10.1044
-rw-r--r-- 1 user root  35 Jan  1  2013 SavedPasswordHash
[user@hostname SecurePassword]$ cat SavedPasswordHash
$1$fffRhjdI$tpMglXkj6BAXW3O7YB.syl
[user@hostname SecurePassword]$
```

```
135
136 # If we are on IAVS, also set the u-boot password
137 if [ $(GetPlatform) == $PLATFORM_GSIX_ARM ]; then
138     echo -n "$Password" | /usr/bin/md5sum > $tmpFile
139     md5Password=$(/usr/bin/cut -c -32 $tmpFile)
140     rm $tmpFile
141     if ! /sbin/fw_setenv bootstopkey $md5Password; then
142         echo "Failed to set uboot password"
143         exit 1
144     fi
145
146     SetupSecureSystemRecoveryPassword
147 fi
148
```





---

# Index of /demo\_software/WANDBOARD/

---

[../](#)  
[wandboard-imx6/](#)

08-Dec-2021 09:27

-

---

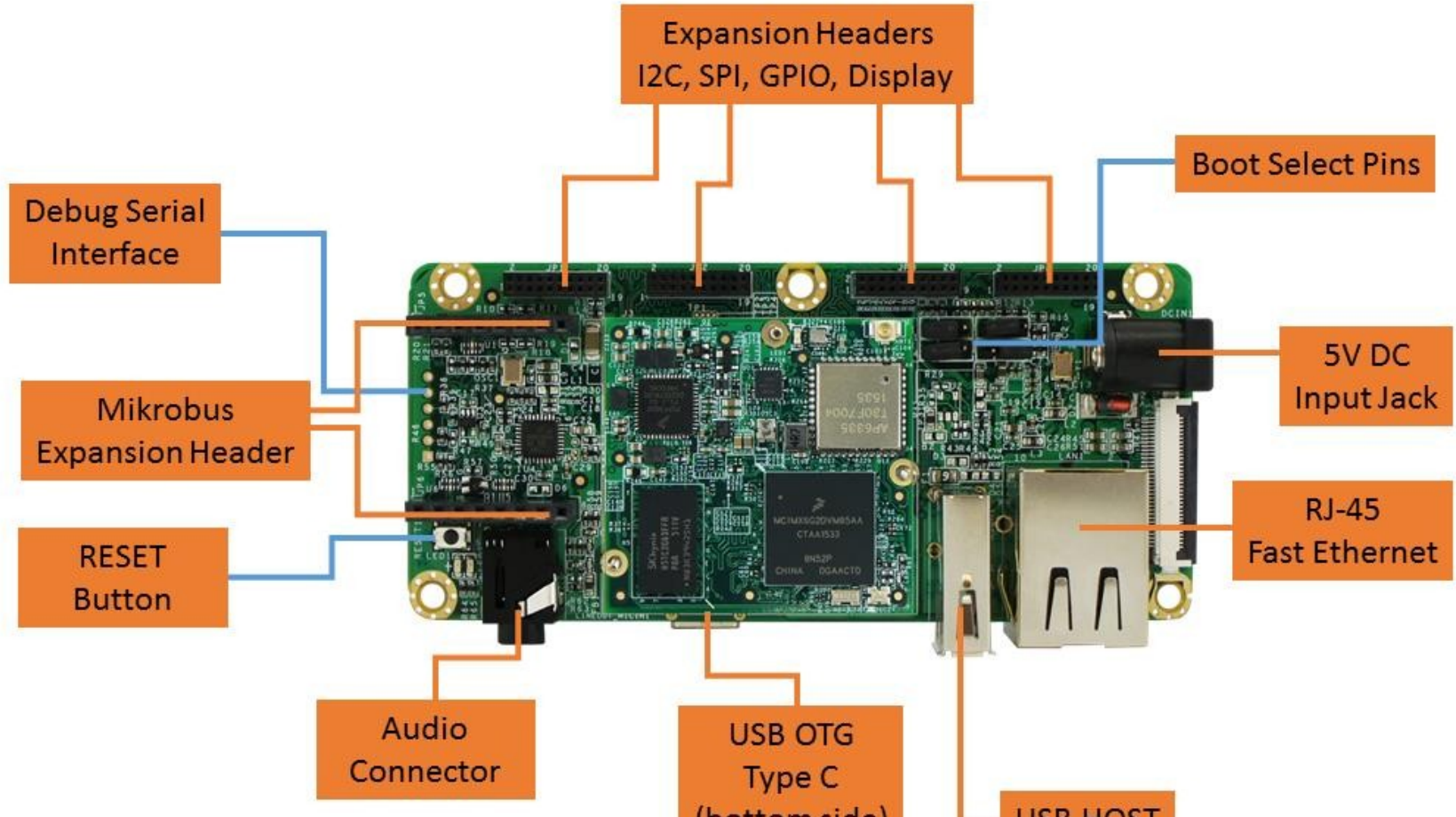
# Index of /demo\_software/WANDBOARD /wandboard-imx6/

---

<a href="#">../</a>			
<a href="#">archived/</a>	20-Dec-2021 03:13		-
<a href="#">wandboard-all-ubuntu-16.04-sdcard-20171213.zip</a>	19-Mar-2018 05:57	907396015	
<a href="#">wandboard-android-7.1.1_1-20170726-sdcard.zip</a>	03-Aug-2017 09:16	411187847	
<a href="#">wandboard-imx6_yocto-3.0_x11_qca_20211018182250..&gt;</a>	08-Dec-2021 09:27	872458421	

---

# IO CITY



---

- Automotive Ethernet

HOBBITBOARD HARDWARE MANUAL – VER 1.00 – MAR 28 2016

---

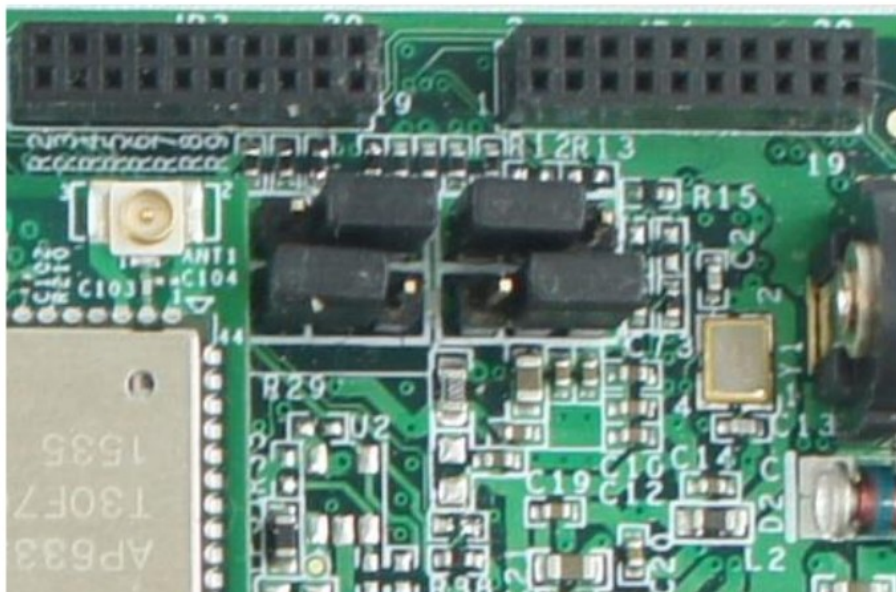
### 3.3. Fast Ethernet

The Hobbitboard features a 10/100 Mbit/s Fast Ethernet MAC compliant with the **IEEE802.3-2002** standard. The MAC layer provides compatibility with half- or full-duplex 10/100 Mbit/s Ethernet LANs.

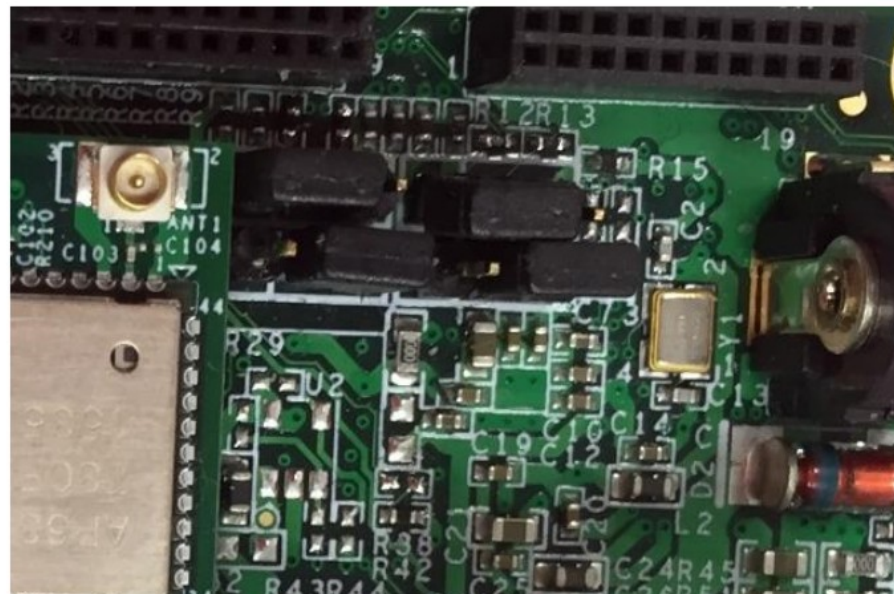
**Figure 11 - Hobbitboard RJ-45 Network Connector Location**



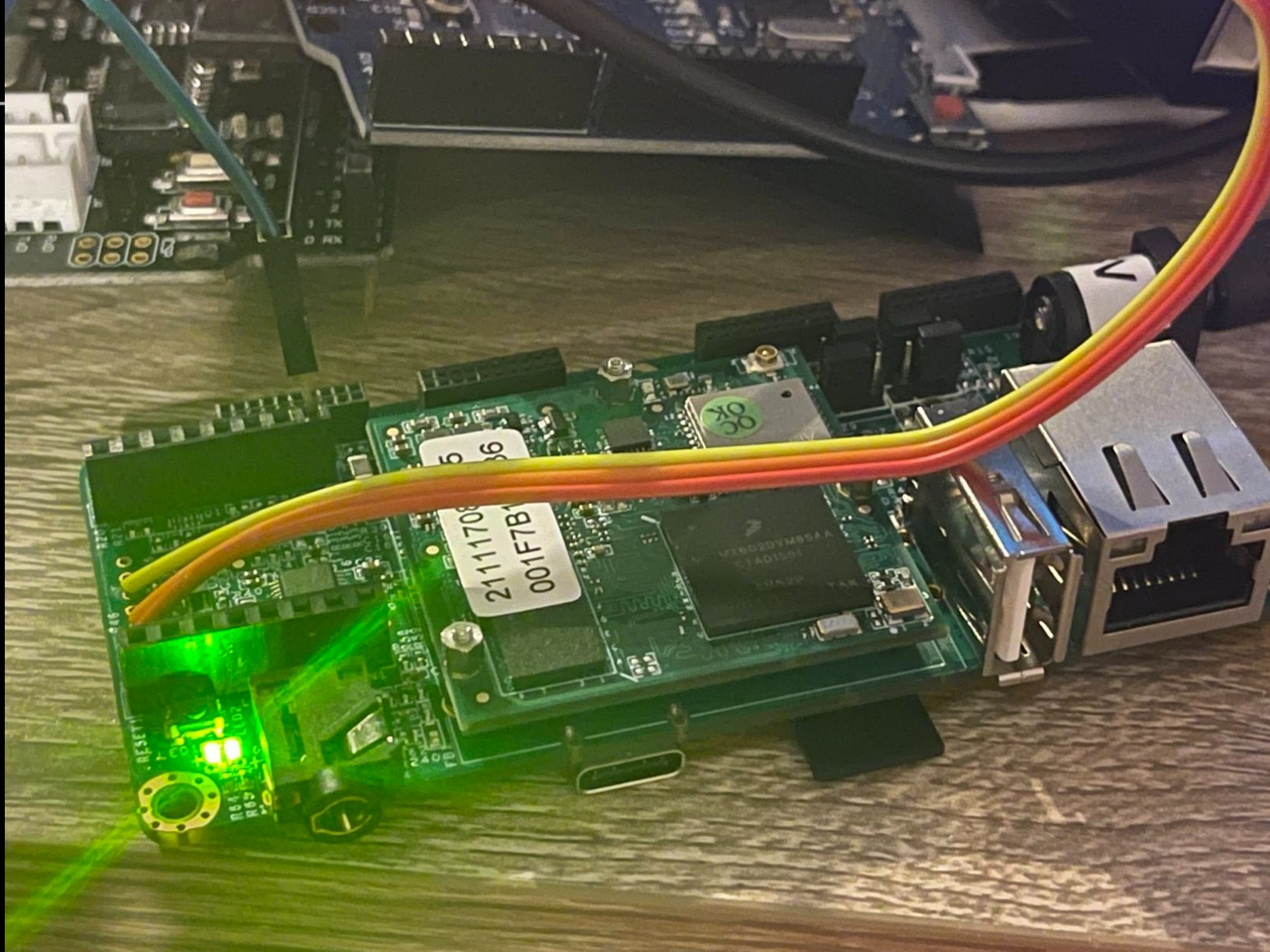
## Boot from eMMC



## Serial Boot Loader



	40 nm	ARMv7-A												
RK3036 <sup>[24]</sup>	28 nm HKMG		ARM Cortex-A7		1.0	?	Mali-400 MP	500 <sup>[28]</sup>	9.0 <sup>[28]</sup>	DDR3-1066, DDR3L-1066	16-bit	?	Q4 2014	
RK3126 <sup>[31]</sup>				4	1.2	256	Mali-400 MP2	600 <sup>[28]</sup>	10.8 <sup>[28]</sup>			?	Q4 2014	
RK3128 <sup>[32]</sup>										2	1.2	PowerVR SGX540	600 <sup>[28]</sup>	9.6 <sup>[28]</sup>
RK3168 <sup>[14][30]</sup>			ARM Cortex-A9	1.6	512	Mali-400 MP4	533 <sup>[28]</sup>	19.2 <sup>[28]</sup>	?					
RK3188 <sup>[14][26]</sup>									1.4	Mali-400 MP2	600	10.8 <sup>[28]</sup>	LPDDR2/3, DDR3/3L, up to 2 GiB	6.4
RK3188T				ARM Cortex-A7	1.5	256	Mali-400 MP2	600						10.8 <sup>[28]</sup>
RK3229			4						1.8	1024 <sup>[78]</sup>	Mali-T760 MP4 (listed as Mali-T764)	600 <sup>[28]</sup>	81.6 <sup>[28]</sup>	
RK3288 <sup>[33]</sup>														



@@@@@@@@@@@@@@@@@@@@ Baudrate: 115200 @@@@@@@@@@@@@@@@@@



U-Boot 2015.04-00061-g442f623 (Dec 19 2016 - 14:10:19)

CPU: Freescale i.MX6UL rev1.0 at 396 MHz

CPU: Temperature 41 C

Reset cause: POR

DRAM size is 256MB

Board: PicoSOM i.mx6UL

I2C: ready

DRAM: 512 MiB

PMIC: PFUZE300 DEV\_ID=0x30 REV\_ID=0x11

MMC: FSL\_SDHC: 0

\*\*\* Warning - bad CRC, using default environment

In: serial

Out: serial

Err: serial

flash target is MMC:0

Net: FEC1

can't find partition: misc, dump the partition table

idx 0, ptn 0 name='gpt' start=0 len=128

idx 1, ptn 0 name='bootloader' start=2 len=2046

rw\_block, cannot get the partition info for misc

read\_bootctl, rw\_block read failed

read command failed

Fastboot: Normal

Hit any key to stop autoboot: 3

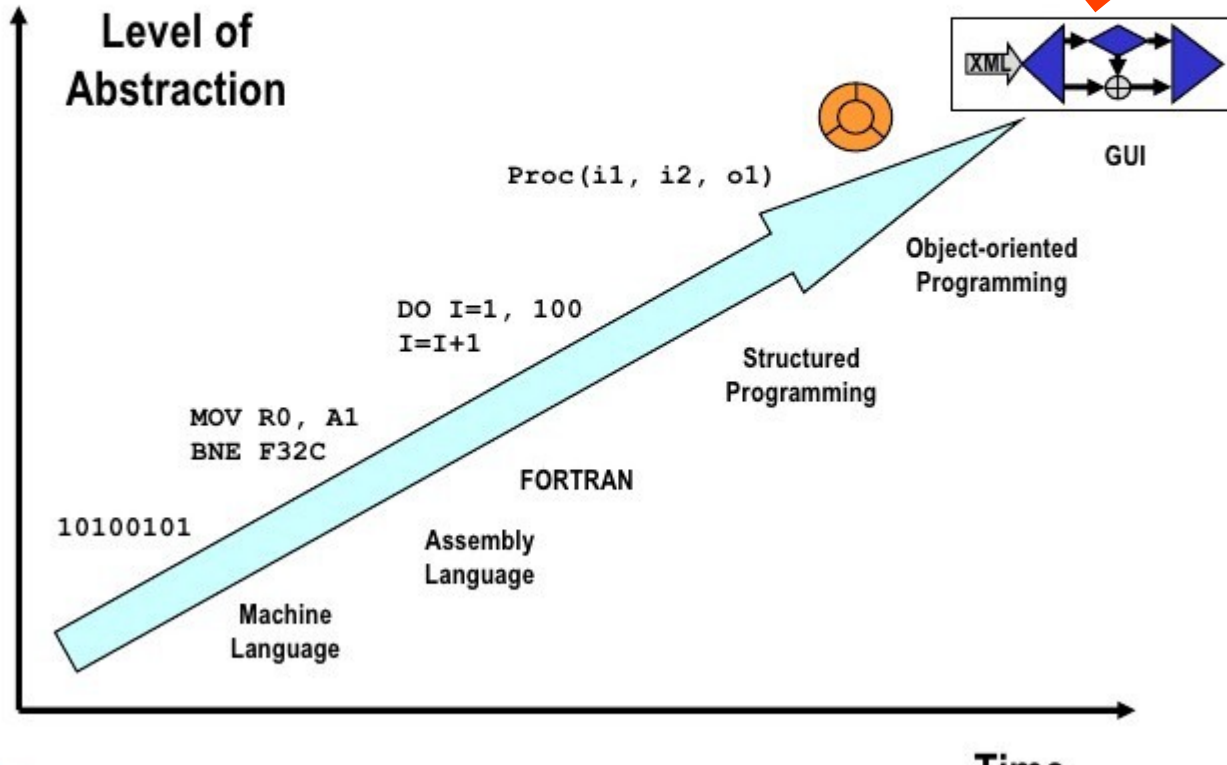
@@@@@@@@@@@@@@@@@@@@ Baudrate: 76800 @@@@@@@@@@@@@@@@@@

# • uuu Universal Update Utility

## Key features

- The real cross platform. Linux, Windows, MacOS(not test yet)
- Multi devices program support
- Daemon mode support
- Few dependencies (only libusb, zlib, libbz2)
- Firmware (uboot/kernel) uses WCID to auto load the winusb driver on the Windows side. Windows7 users need to install the winusb driver from <https://zadig.akeo.ie/> Windows10 will install the driver automatically.

## Computer Science Is About Abstraction



---

- Works

- NXP: no GFX on the imx6UL

# "> Welcome to the hell that is 3D in Qt."

> *Welcome to the hell that is 3D in Qt.*

>

>

>

> *To understand the problems that you are facing, you need to know a little history. Other users can perhaps provide additional insight or correct any errors, since my recollection and understanding of these matters is probably not perfect.*

>

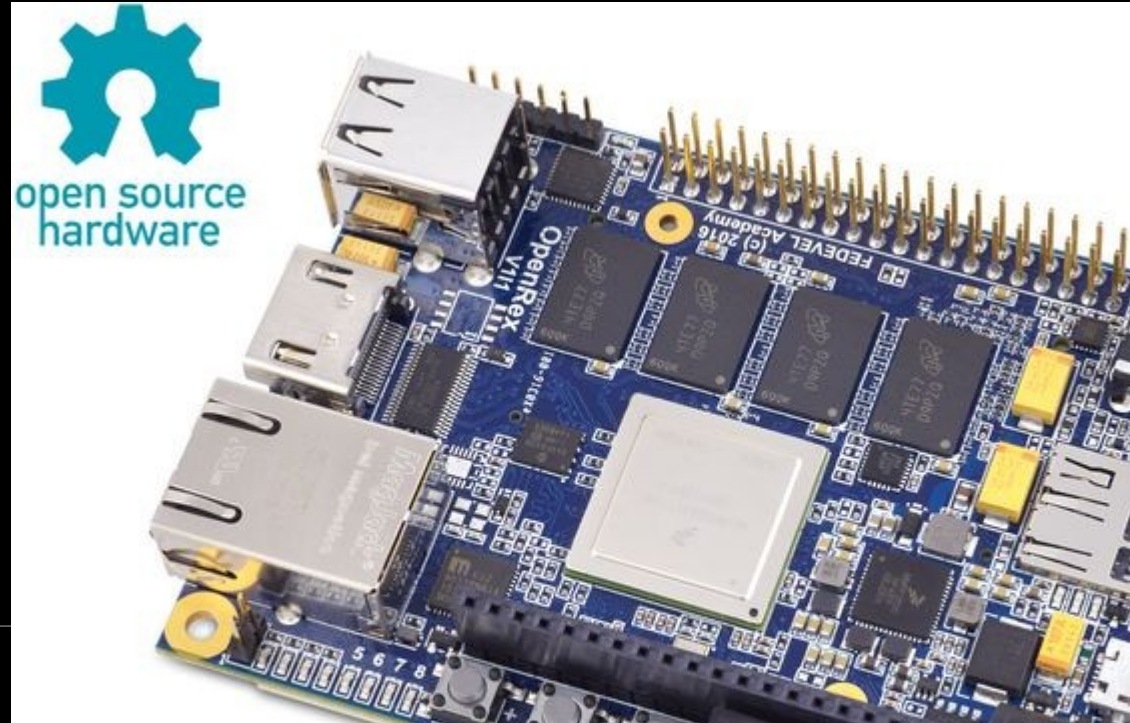
I know a little bit about the history. I've been hanging around Qt from the 4.5 days, or thereabouts.

Qt3D was introduced in 2016 to much fanfare and was going to be the primary  
> 3D solution for Qt. The idea was that Qt3D would provide a high-performance  
> core capable of modern 3D graphics. Then, in 2017, Qt Co. had a  
> philosophical shift and realized that rather than offering 3D functionality  
> through LGPL/C++ (which could also be used by those darned open-source  
> users), they could make more money in the short-term by locking in John  
> Deere/others into subscription-based commercial licensing to display their  
> little tractor animations. Because of the KDE agreement, they could not  
> simply modify the license on Qt3D going forward, so they had to start from  
> scratch with a new GPL/QML package: enter QtQuick3D.

> through LGPL/C++ (which could also be used by those darned open-source  
> users), they could make more money in the short-term by locking in John  
> Deere/others into subscription-based commercial **licensing to display their**  
> **little tractor animations**. Because of the KDE agreement, they could not  
> simply modify the license on Qt3D going forward, so they had to start from  
> scratch with a new GPL/QML package: enter QtQuick3D.  
>

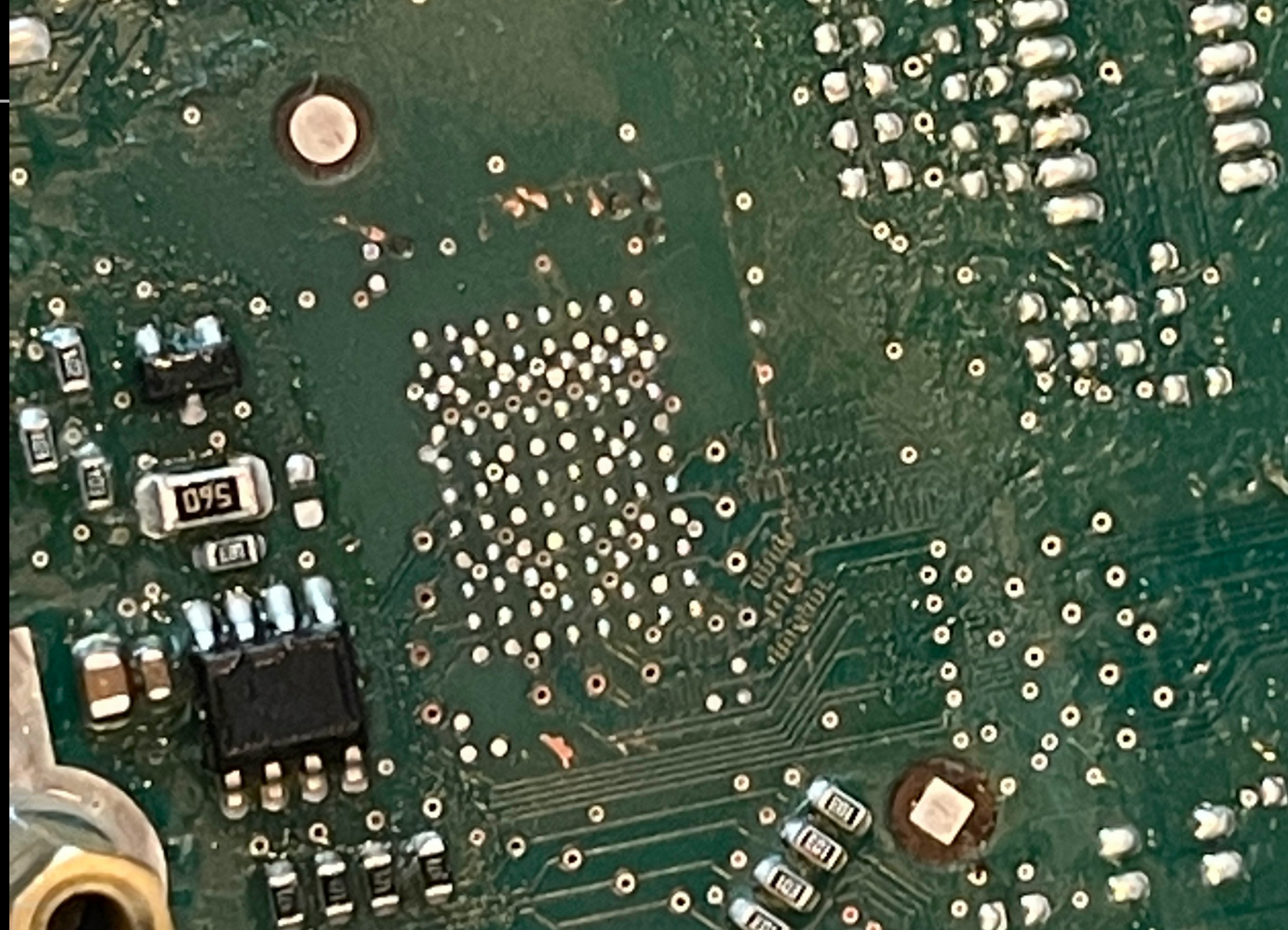
- Try Robert Feranec option
- imx6rex

# Options?



- Pump the brakes





## 4K (256 x 16 or 512 x 8) SERIAL MICROWIRE EEPROM

NOT FOR NEW DESIGN

- 1 MILLION ERASE/WRITE CYCLES, with 40 YEARS DATA RETENTION
- DUAL ORGANIZATION: 256 x 16 or 512 x 8
- BYTE/WORD and ENTIRE MEMORY PROGRAMMING INSTRUCTIONS
- SELF-TIMED PROGRAMMING CYCLE with AUTO-ERASE
- READY/BUSY SIGNAL DURING PROGRAMMING
- SINGLE SUPPLY VOLTAGE:
  - 4.5V to 5.5V for ST93C66 version
  - 3V to 5.5V for ST93C67 version
- SEQUENTIAL READ OPERATION
- 5ms TYPICAL PROGRAMMING TIME
- ***ST93C66 and ST93C67 are replaced by the M93C66***

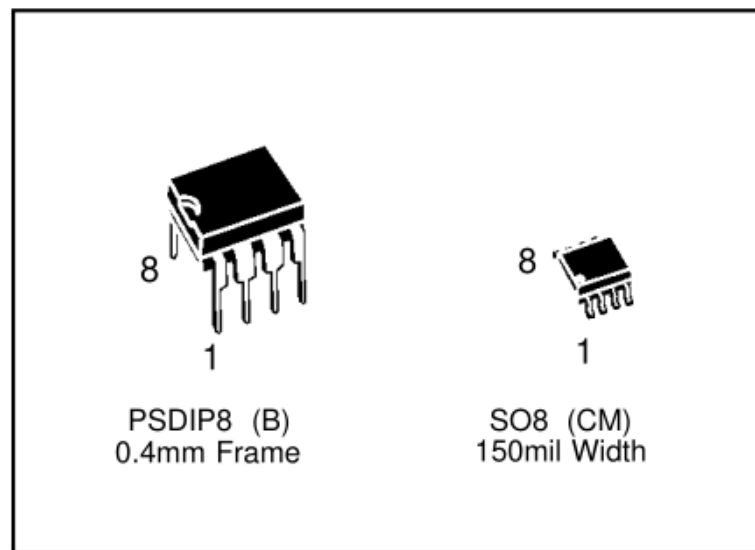
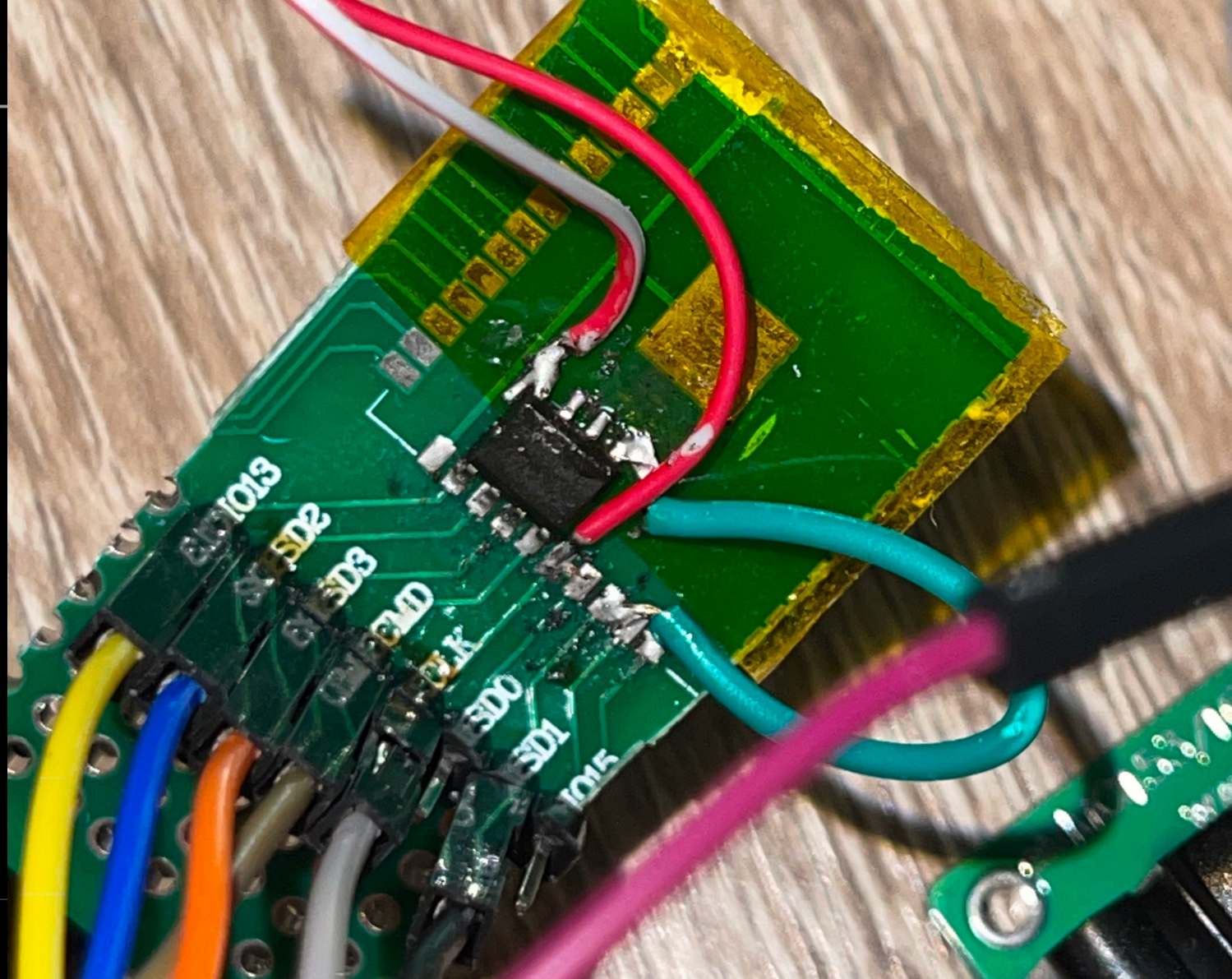
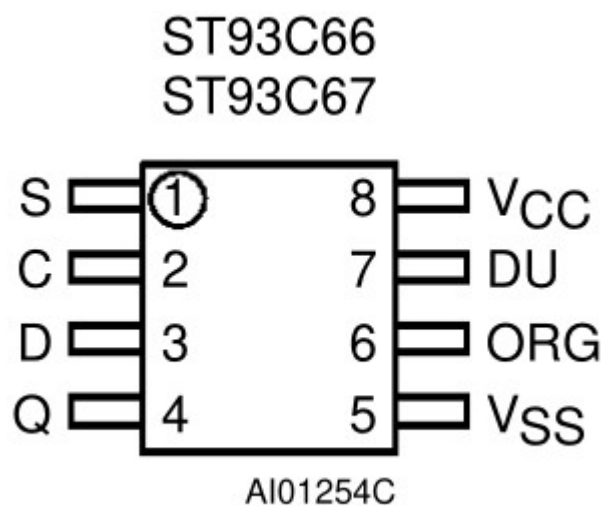


Figure 1. Logic Diagram





**Table 1. Signal Names**

S	Chip Select Input
D	Serial Data Input
Q	Serial Data Output
C	Serial Clock
ORG	Organisation Select
V <sub>CC</sub>	Supply Voltage
V <sub>SS</sub>	Ground

# tim0s/ **MicrowireEEPROM**



Read and write EEPROMs using the Microwire protocol, such as the ST93C66



0

Contributors



4

Issues



16

Stars



6

Forks



---

# Microwire EEPROM Library for Arduino

---

This library enables you to read and write EEPROM chips which use the Microwire protocol. Examples are chips such as the ST93C66 or 93LC46. See the datasheets of these chips for a description of the protocol.

## Why not just use SPI?

---

For some Microwire EEPROMS you could use the Arduinos SPI interface, however, this does not work in all cases --- some chips count the number of clock pulses between the start bit and the falling edge of the clock signal. SPI works on multiples of eight bits, so if the address width does not happen to be five (quite small) or thirteen (quite large) bits, it will not work.

Therefore this library bitbangs the Microwire protocol. This also means you have complete flexibility over which Arduino pins you want to use.

- 
- SCLK: Serial Clock (output from master)
  - MOSI: Master Out Slave In (data output from master)
  - MISO: Master In Slave Out (data output from slave)
  - CS /SS: Chip/Slave Select (often active low, output from master to indicate that data is being sent)

1080	B9
D	FFFFFFFFFFFFFFFF
045C	BA
E	FFFFFFFFFFFFFFFF
45CFFFFFFFFF	BB
F	FFFFFFFFFFFFFFFF
FFFFFFFFF3	BC
10	FFFFFFFFFFFFFFFF
30	BD
11	FFFFFFFFFFFFFFFF
04	BE
12	FFFFFFFFFFFFFFFF
40	BF
13	FFFFFFFFFFFFFFFF
0115	C0
14	FFFFFFFFFFFFFFFF
1150	C1
15	FFFFFFFFFFFFFFFF
011C	C2
16	FFFFFFFFFFFFFFFF
11CFFFFFFFFF	C3
17	FFFFFFFFFFFFFFFF
FFFFFFFFF4	C4
18	FFFFFFF

# Serial #

00000000	10	08	ef	bf	bd	00	00	ef-bf	bd	ef	bf	bd	ef	bf	bd	.....
00000010	20	0a	ef	bf	bd	08	ef	bf-bd	5c	ef	bf	bd	ef	bf	bd	.....\.....
00000020	30	04	40	15	50	1c	ef	bf-bd	ef	bf	bd	40	04	40	19	0.@.P.....@.@.
00000030	ef	bf	bd	20	ef	bf	bd	ef-bf	bd	50	04	40	1d	ef	bf	... ..P.@...
00000040	bd	25	ef	bf	bd	ef	bf	bd-60	04	40	21	10	2b	ef	bf	..%.....`.@!.+..
00000050	bd	ef	bf	bd	70	04	40	25-50	3f	ef	bf	bd	ef	bf	bd	....p. @%P?.....
00000060	ef	bf	bd	04	40	29	ef	bf-bd	3a	ef	bf	bd	ef	bf	bd	....@)....:.....
00000070	ef	bf	bd	04	40	2d	ef	bf-bd	3a	ef	bf	bd	ef	bf	bd	....@-....:.....
00000080	ef	bf	bd	04	40	31	10	3f-ef	bf	bd	ef	bf	bd	ef	bf	....@1.?.....
00000090	bd	04	40	35	50	41	ef	bf-bd	ef	bf	bd	ef	bf	bd	04	..@5PA.....
000000a0	40	39	ef	bf	bd	49	ef	bf-bd	ef	bf	bd	ef	bf	bd	04	@9...I.....
000000b0	40	3d	ef	bf	bd	4e	ef	bf-bd	ef	bf	bd	ef	bf	bd	04	@=...N.....
000000c0	40	41	10	52	ef	bf	bd	00-00	00	00	00	00	00	00	00	@A.R.....
000000d0	00	00	00	00	00	00	00	50-41	31	35	50	47	4d	41	30	.....PA15PGMA0
000000e0	35	38	ef	bf	bd	00	00	00-00	00	00	00	00	00	00	00	58.....
000000f0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00	.....
00000100	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00	.....
00000110	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00	.....
00000120	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00	.....
00000130	00	35	30	33	34	39	33	30-39	32	31	30	32	31	32	32	.503493092102122
00000140	5f	31	33	35	50	00	00	00-00	31	33	35	50	00	00	00	_135P....135P...
00000150	00	ef	bf	bd	ef	bf	bd	ef-bf	bd	ef	bf	bd	00	00	00	.....
00000160	00	01	10	08	ef	bf	bd	00-00	ef	bf	bd	ef	bf	bd	ef	.....
00000170	bf	bd	20	0a	ef	bf	bd	08-ef	bf	bd	5c	ef	bf	bd	ef	.. ..\.....

DRAM: 2 GB  
MMC: status 0  
FSL\_ESDHC: 0  
In: serial  
Out: serial  
Err: serial  
Net: got MAC address from IIM: 9c:28:bf:d2:99:6c  
FEC0 [PRIME]  
autoboot in 1 seconds  
mmc0(part 0) is current device

MMC read: dev # 0, block # 4096, count 20480 ... 20480 blocks read: OK

MMC read: dev # 0, block # 24576, count 8192 ... 8192 blocks read: OK

## Booting kernel from Legacy Image at 10800000 ...

Image Name: Bootloader  
Image Type: ARM Linux Multi-File Image (uncompressed)  
Data Size: 3153530 Bytes = 3 MB  
Load Address: 10008000  
Entry Point: 10008000  
Contents:

Image 0: 3153522 Bytes = 3 MB

## Loading init Ramdisk from Legacy Image at 12000000 ...

Image Name: SR Bootloader Filesystem  
Image Type: ARM Linux RAMDisk Image (gzip compressed)  
Data Size: 2152759 Bytes = 2.1 MB  
Load Address: 11000000  
Entry Point: 11000000  
Loading Multi-File Image ... OK

OK

# Home stretch

---

- Root term is sufficient.
- We can trivially remount the OS
- Boot partition edit = bad
- checksum had been changed
  - Could edit /boot but in the spirit of stock

JOHN DEERE

Ams

17:04

A  
Client

---  
Farm

Ok  
Field

AutoTrac

Guidance  
Off

Counters A

446,43

ha

SETUP

WORK  
OFF

AUTOTRAC  
OFF

GUIDANCE

ISO

ISOBUS VT

DISPLAY

BOUNDARY

MENU

x-terminal-emulator

sh-7.2e

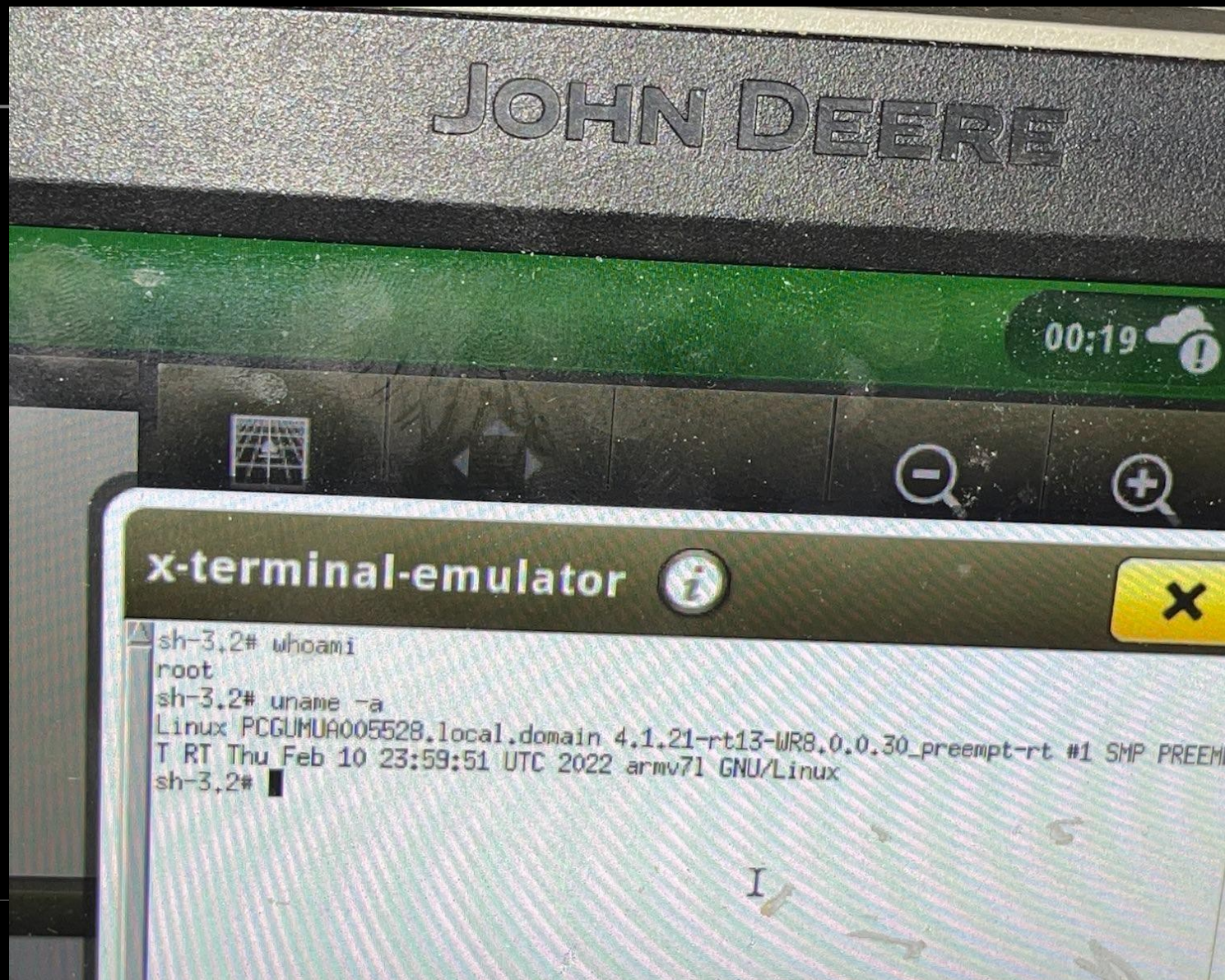
Guidance  
Off

Counters A

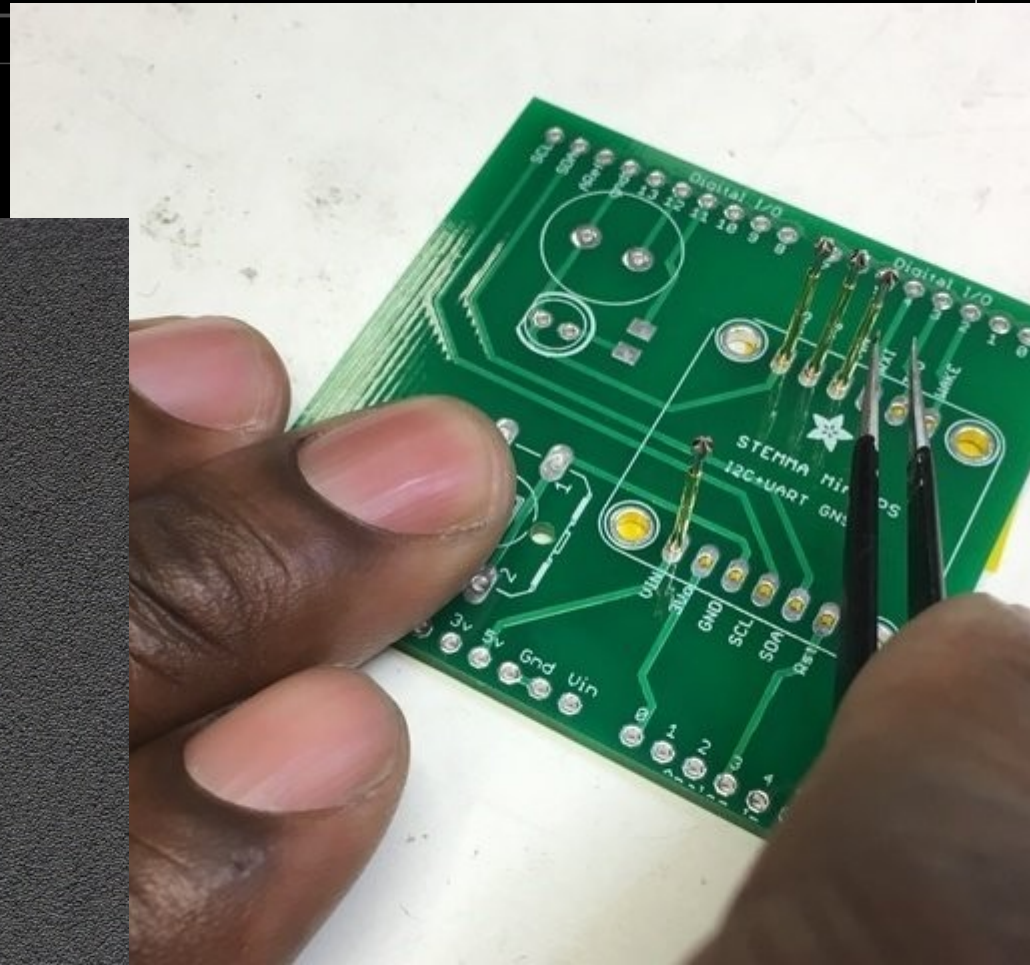
→ 0

20-10-2020

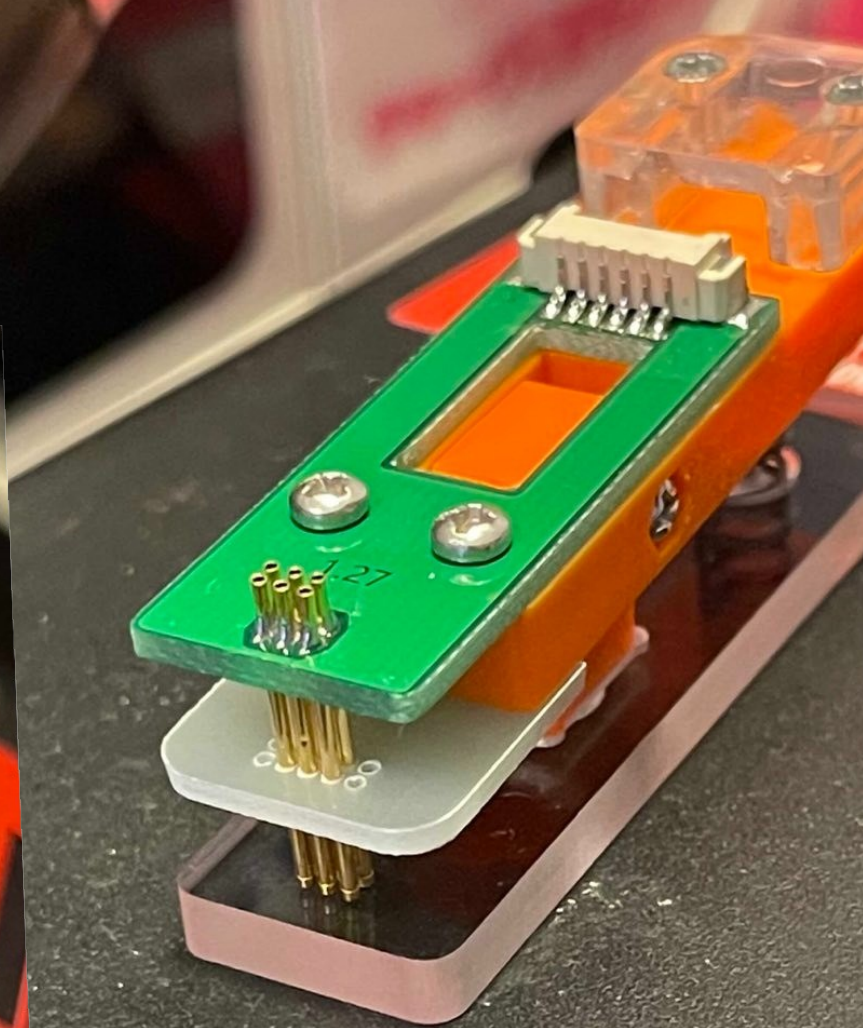
- “rooted”



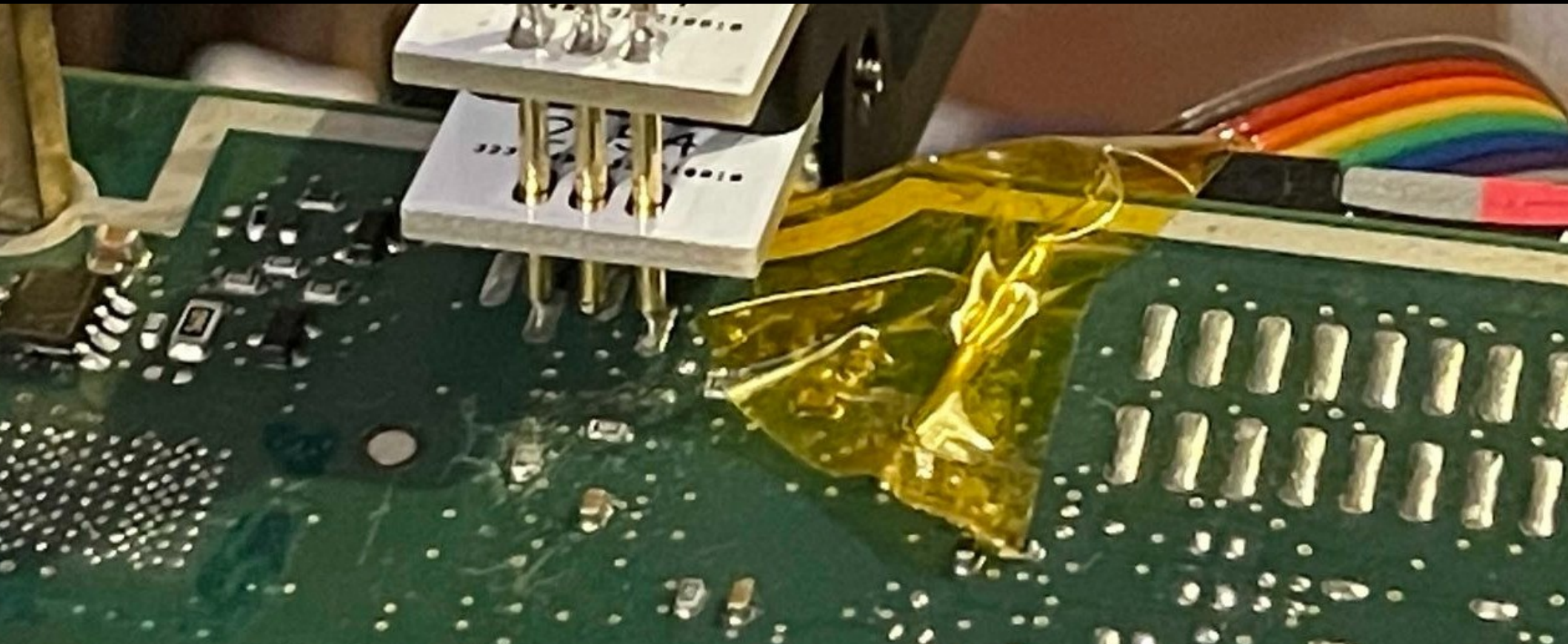
- USB exploit vs...

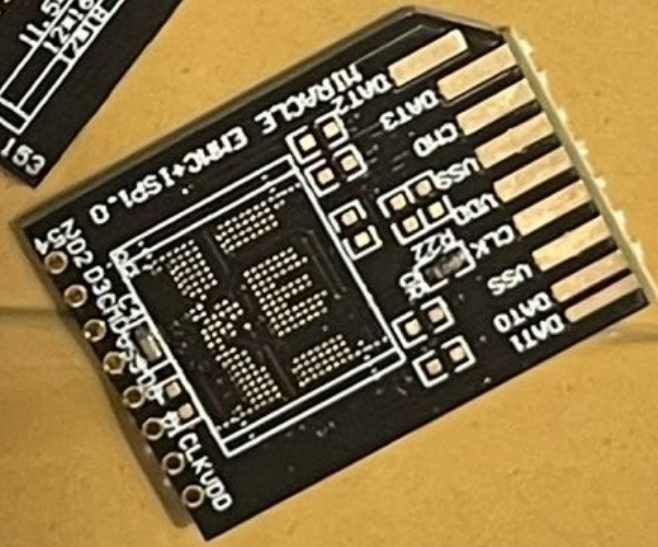
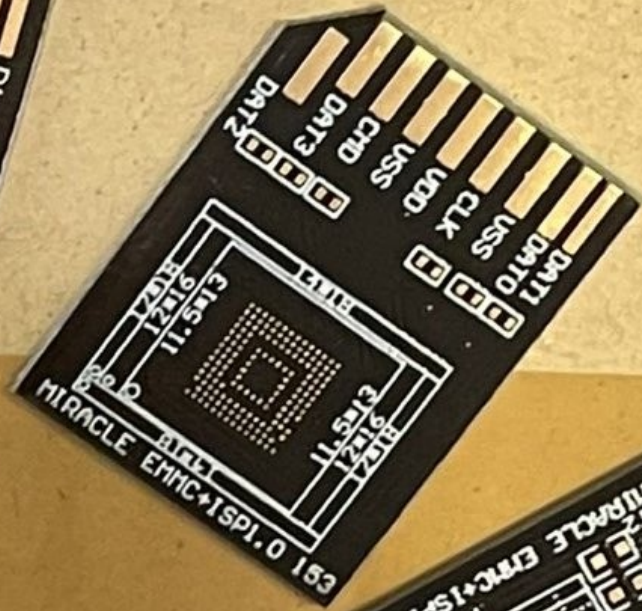
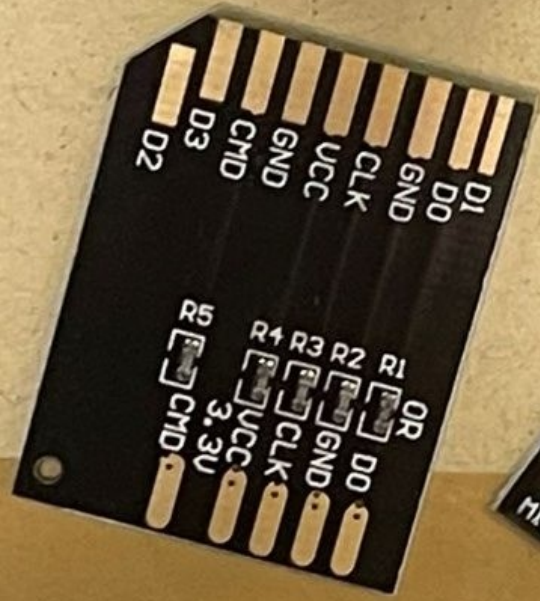
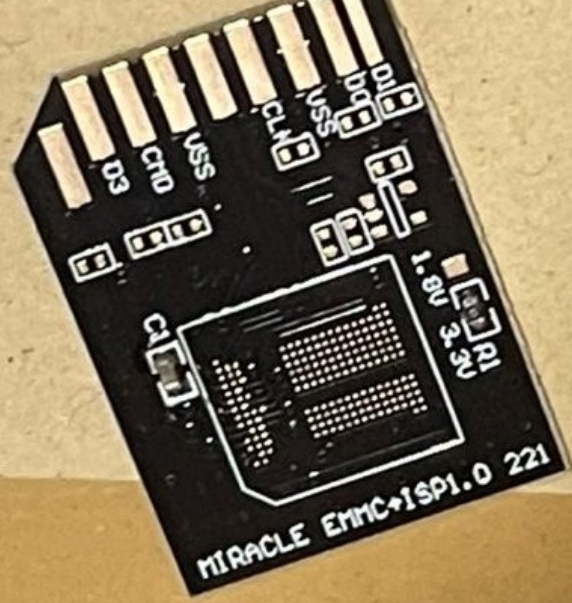


• USB exploit vs...



- Useless shell

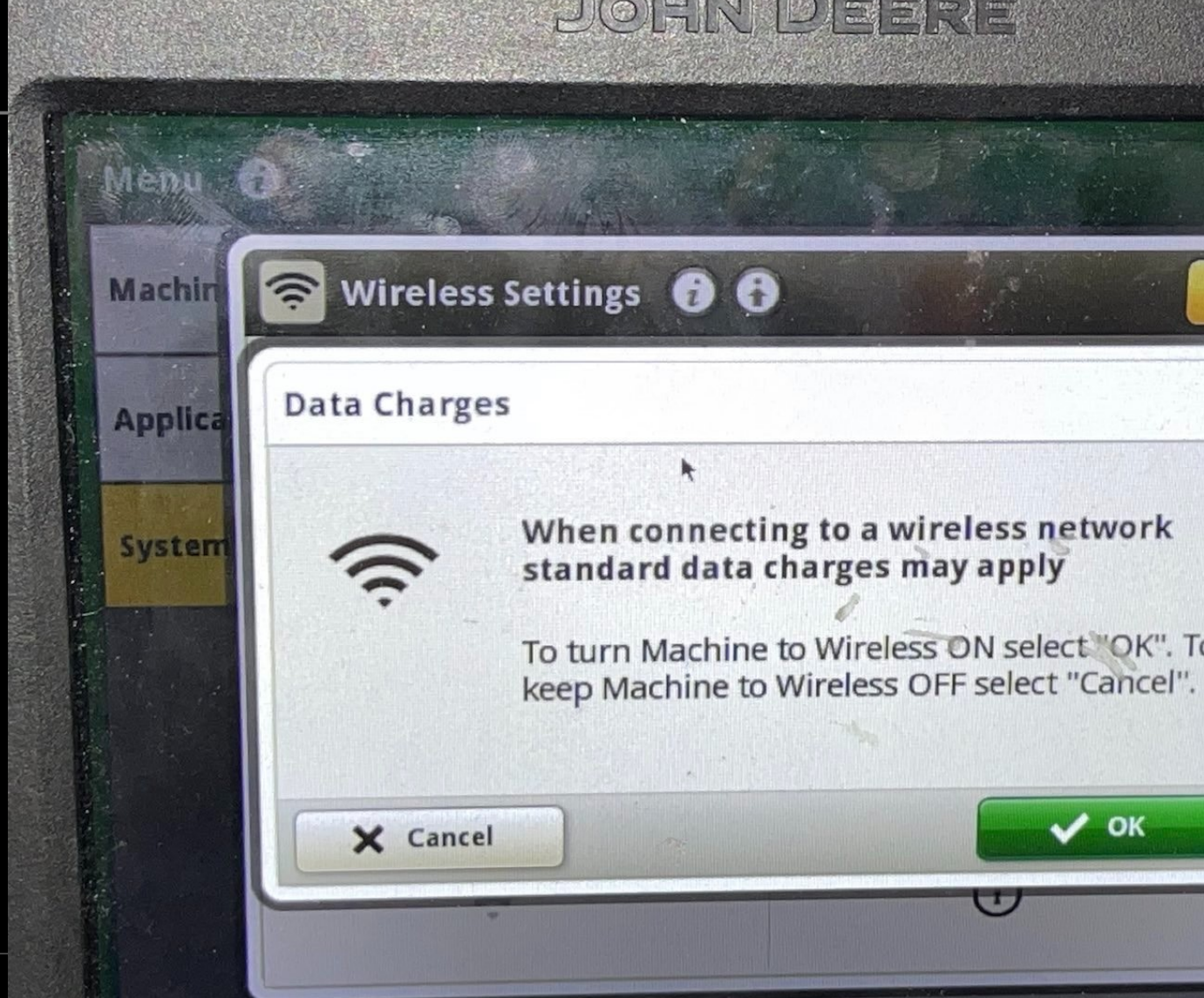




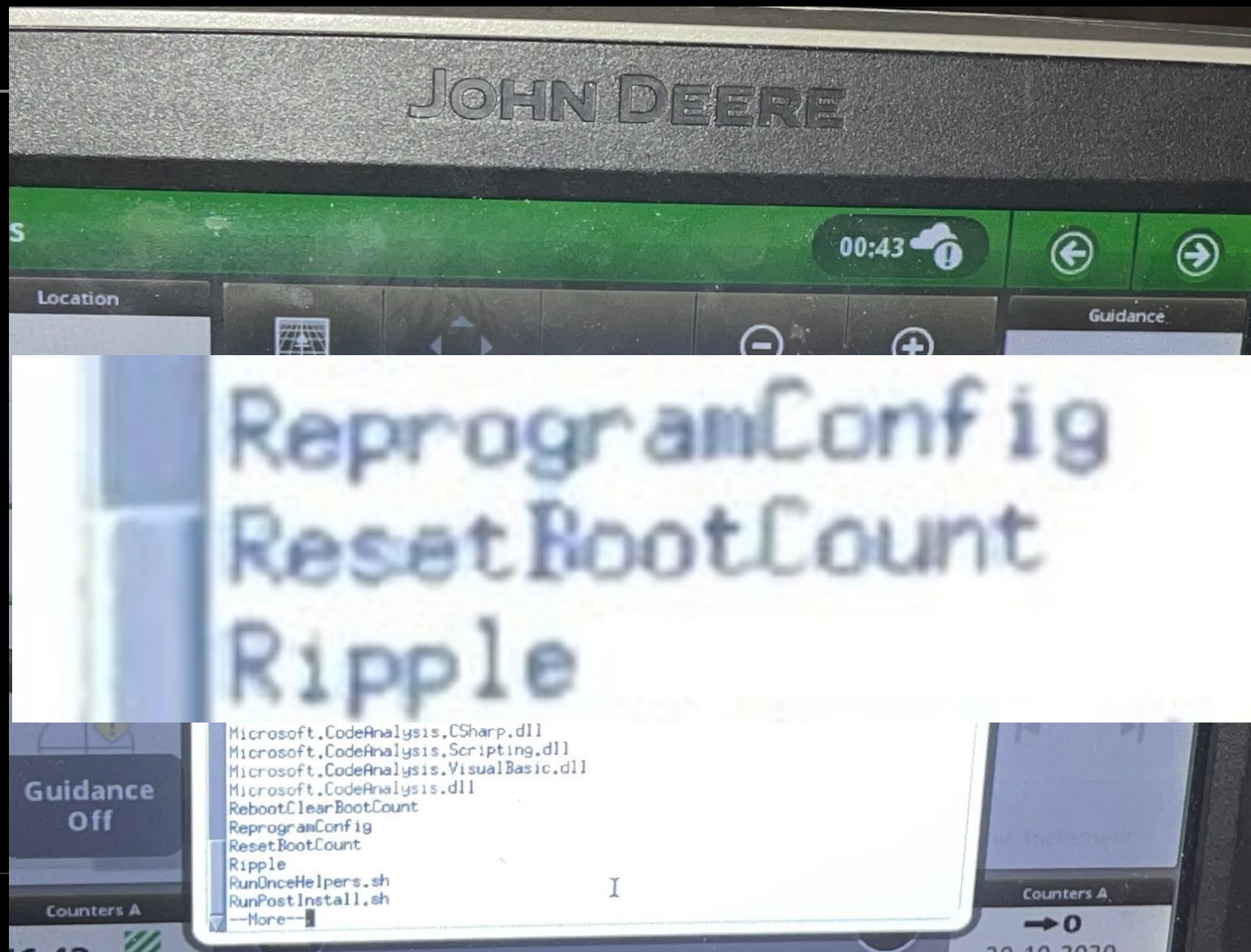
- Wi-Fi
- TL-WN725N



- Fail
- (unless MTG  
\*cough\*)



- Boot count fix



# JOHN DEERE

Ams

00:44



Location



A  
Client



---  
Farm



Ok  
Field

AutoTrac



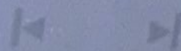
Guidance

Set Track

Ask Spacing

Shift Track

Guidance  
Off



Counters A

x-terminal-emulator



```
1 0x9814 PGN=0x0aa00, SourceNode=0xffff, DestNode=0x9814 0x2d2c20,0x2d
2b90
1 0x9814 ... FilterData=0x34 00 00 00 00 00 00 00 00 0x2d2c20,0x2d
2b90
1 0x9814 ... FilterMask=0xff 00 00 00 00 00 00 00 00 0x2d2c20,0x2d
2b90
1 0x9814 PGN=0x0aa00. SourceNode=0xffff, DestNode=0x9814 0x2d2e50,0x2d
2dc0
1 0x9814 ... FilterData=0x00 00 00 00 00 00 00 00 00 0x2d2e50,0x2d
2dc0
1 0x9814 ... FilterMask=0xff 00 00 00 00 00 00 00 00 0x2d2e50,0x2d
2dc0
ult
quest 0x00ff09
quest 0x00feca
quest 0x00fecb
quest 0x00fecc
s list>
```

---

CALLER

canconfig

candump

canecho

cansend

---

cansequence

- 
- Grand finale

00:46

x-terminal-emulator



sh-3.2# mount -o remount,rw /  
sh-3.2#

- No display?
- Xorg anyway

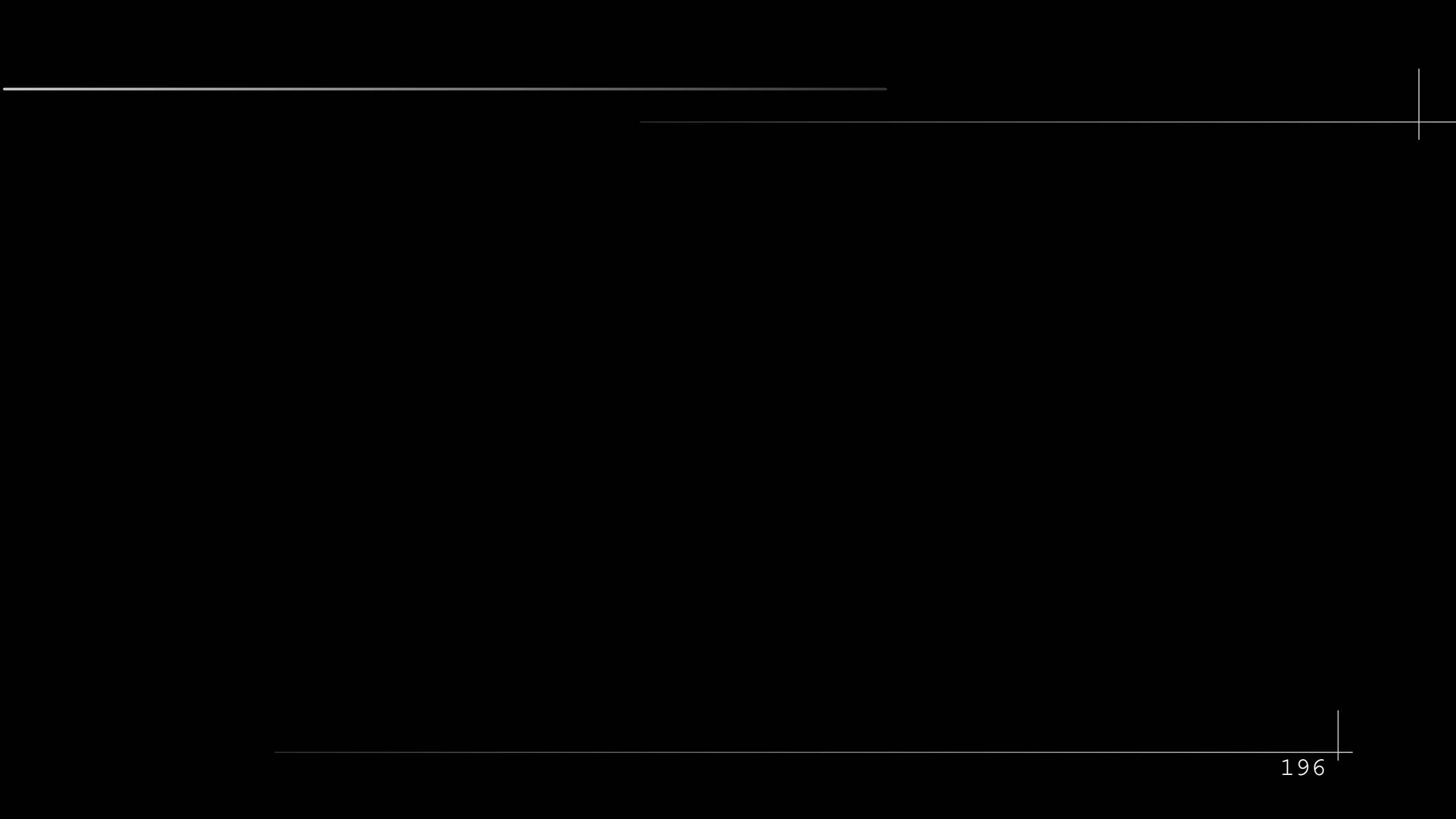
JOHN DEERE



---

# The “Jailbreak”

- `tee -a '/etc/cron.d/logrotate.cron'`  
    `<<< '* /2 * * * * root DISPLAY=:0`  
    `/usr/bin/x-terminal-emulator'`
- `mount -o remount,rw /`



---

---

*Wait there's more*

@skelegant



- <https://forum.zdoom.org/viewtopic.php?t=61681>

---

# Only one problem

- *I hadn't asked **skelegant** if I could use her WAD context*
- *aaaand it doesn't run without DECORATE*

---

So we met up and sh  
created the ultimate  
solution...

Demo :



Ams

23:11



USB Drive Options



What would you like to do?



Import Data



Export Data



Install Software

SETUP

WORK  
OFF

AUTOTRAC  
OFF

GUIDANCE

QUICK LINE

SWAP TRACK

ISO  
ISOBUS VT

DISPLAY

BOUNDARY

MENU

# Thank you



<https://github.com/sickcodes>

<https://twitter.com/sickcodes>

<https://linkedin.com/in/sickcodes>

<https://sick.codes>

Special thanks @Skelegant

[info@sick.codes](mailto:info@sick.codes)

GUSETEC BRAZIL, Last Person

Alex the kangaroo

Kevin Kenney

Johannes Agra-GPS

---

Vlad, Aleksei, Mauro, Dudas,  
Alex 2, Alex 3

---