Mod BIOS via Programmer flashen

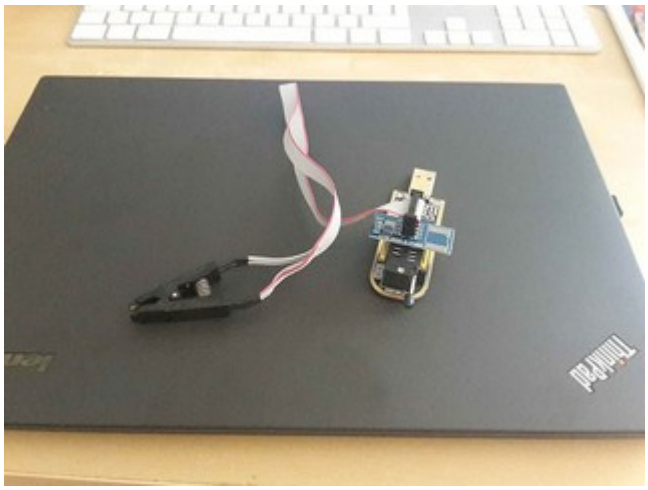
Beitrag von „Sascha_77“ vom 20. April 2018, 18:28

Bei vielen Laptops (insbesondere Lenovo) befindet sich eine Whitelist im BIOS die es verhindert andere WLan-Karten zu benutzen. Direkt nach dem Einschalten weist einem das Gerät dann darauf hin, dass die verwendete Karte nicht akzeptiert wird und dann geht es nicht mehr weiter. Bei älteren Laptops gibt es die Möglichkeit ein sog. Mod BIOS via Softwareflash auf dem Gerät zu installieren. Danach kann man sich jede beliebige Karte einbauen. Nun hat aber z.B. Lenovo seit der Tx30 (bzw. ab X230) angefangen das BIOS zu signieren. Das heisst, dass der Softwareflasher jetzt rummurrt wenn man ihm mit einem gemoddeten BIOS daher kommt und er tritt in den Streik. Schöner Mist. Also was tun? USB Dongle? Kann man machen ... muss man aber nicht.
Bei meinem Beispiel Rechner (T440) an dem ich das ganze Prozedere erläutern werde, befinden sich nur 2 USB Ports. 1 davon für einen Dongle vergeuden? Nö.

Es gibt alternativ zu einem Softwareflash noch die Möglichkeit den BIOS Chip direkt zu bespielen. Klingt im ersten Moment schwierig ist es aber nicht. Ich hatte Anfangs auch etwas Bedenken aber das sollte unbegründet sein wie sich rausstellte. Was benötigen wir für so ein Vorhaben an zusätzlicher Hardware?

https://www.amazon.de/WINGONEE...mmer-CH341A/dp/B01H938PRK
https://www.amazon.de/SOIC8-Fl...ogrammierer/dp/B01GBEST06

Die Sachen gibt es alternativ auch auf eBay direkt vom Chinamann. Versand dauert zwar etwas aber dafür kostet es einiges weniger. Ich habe für diese 2 Artikel in Summe rund 6,- Euro gezahlt.



Software
- CH341A Programmer
- Gemoddetes BIOS File

Als Erstes installieren wir jetzt den "Programmer mode Driver". Dazu einfach den Programmer einstöpseln und dann den Treiber auswählen sobald Windows rummotzt, es könne mit der Hardware nichts anfangen.
Als Nächstes installieren wir dann die eigentliche Programmer Software. Das war es Softwareseitig erst einmal.

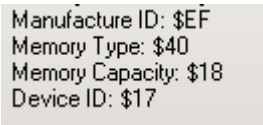
Jetzt werden wir den BIOS Chip auslesen. Dazu müssen wir ihn erst einmal lokalisieren. Bei meinem T440 kam er erfreulicherweise nach der Demontage der Bodenschale direkt zum Vorschein.

Auch gut zu sehen ist diese Vertiefung im Chip die mit einem Pfeil markiert ist. Da liegt PIN 1 an und es ist wichtig die Zange richtig herum drauf zu klemmen.

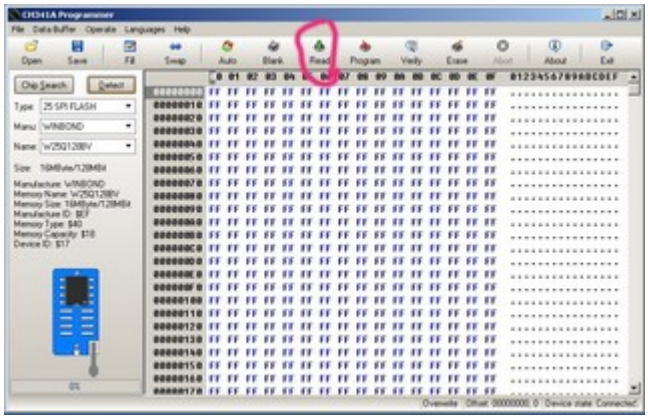
Die rote Ader befindet sich auf PIN 1. Somit ist der Rechner jetzt schonmal vorbereitet. Nun stecken wir die Zange an den Programmer:

Die rote Ader muss sich hier gemäß dieser Abbildung befinden:

Nun drücken wir auf den "Detect"-Button. Wenn die Zange richtig sitzt sollte er jetzt ein paar Werte ausgelesen haben. Wichtig an dieser Stelle ist, das hier unterschiedliche Werte stehen. Sollte dort überall "1F" stehen sitzt die Zange nicht richtig auf dem Chip und Ihr müsst nochmal nachjustieren.



Wenn nun der Chip erkannt wurde könnte ihr ihn via "Read" auslesen.



Daraufhin sollte bei der Anzeige was tun:

Das kann so 2-3 Minuten dauern je nachdem wie groß Euer BIOS Chip ist. Bei meinem T440 sind es 16 MB. Am Ende sollte es so aussehen:

Nun müsst Ihr den Bios DUMP nur noch speichern. Wenn Ihr das getan habt könnt Ihr mit diesem Dump bei den Jungs von https://www.bios-mods.com/ vorbeischauen und dort um eine Whitelist-Entfernung bitten. Erfahrungsgemäß sind die dort damit ziemlich zügig.

~~**Alternativ zum Dumpen** kann man im Mod-Forum die offizielle .exe-Datei vom BIOS-Update des jeweiligen Herstellers hochladen. Die Jungs holen sich dann das entsprechende File selber daraus. Der Vorteil dabei ist, dass man das gemoddete BIOS dann bei allen Rechnern dieses Typs verwenden kann. Ein Dump hingegen ist so gesehen immer was "persönliches", da sich dort die Seriennummer des Geräts und noch andere Informationen finden lassen und somit nur auf diesem einen Gerät verwendbar sind.~~

Wenn ihr dann das BIOS modifiziert später wieder zurückbekommen habt öffnet ihr wieder das Programm. Erstmal wieder auf Detect klicken. Danach öffnet Ihr das modifizierte BIOS File. Nun könnt ihr das BIOS zurück auf den Chip mittels "Program" schreiben. Man kann alternativ auch "Auto" benutzen wenn man ganz sicher gehen will. Der Chip wird dann erst gelöscht, beschrieben und am Ende noch verifiziert.

Hier müsst Ihr jetzt etwas Geduld aufbringen. Der Schreibvorgang findet mit einer Geschwindigkeit von 4-5 kb/sec statt. Kann also je nach Chip Größe entsprechend dauern.

Das war es eigentlich auch schon. Nun habt Ihr erfolgreich ein Mod Bios geflasht und könnt jede OSX kompatible Karte verwenden.

Noch ein Hinweis: Es empfiehlt sich vor der Aktion das BIOS auf offiziellem Wege erst einmal auf den aktuellsten Stand zu bringen. Ist natürlich kein Muss. Aber wenn man sich schonmal die ganze Arbeit macht bietet es sich ja irgendwie an.

EDIT:
Da sich das ursprüngliche Windows-Paket als nicht zuverlässig herausstellte bitte entweder direkt diese Tool für macOS nutzen oder wer möchte kann auf das Debian Image zurückgreifen. Macht aber eigtl. nur Sinn wenn man einen Programmer hat der von "flashrom" NICHT supported wird. Weil flashrom ist in G-Flash enthalten.

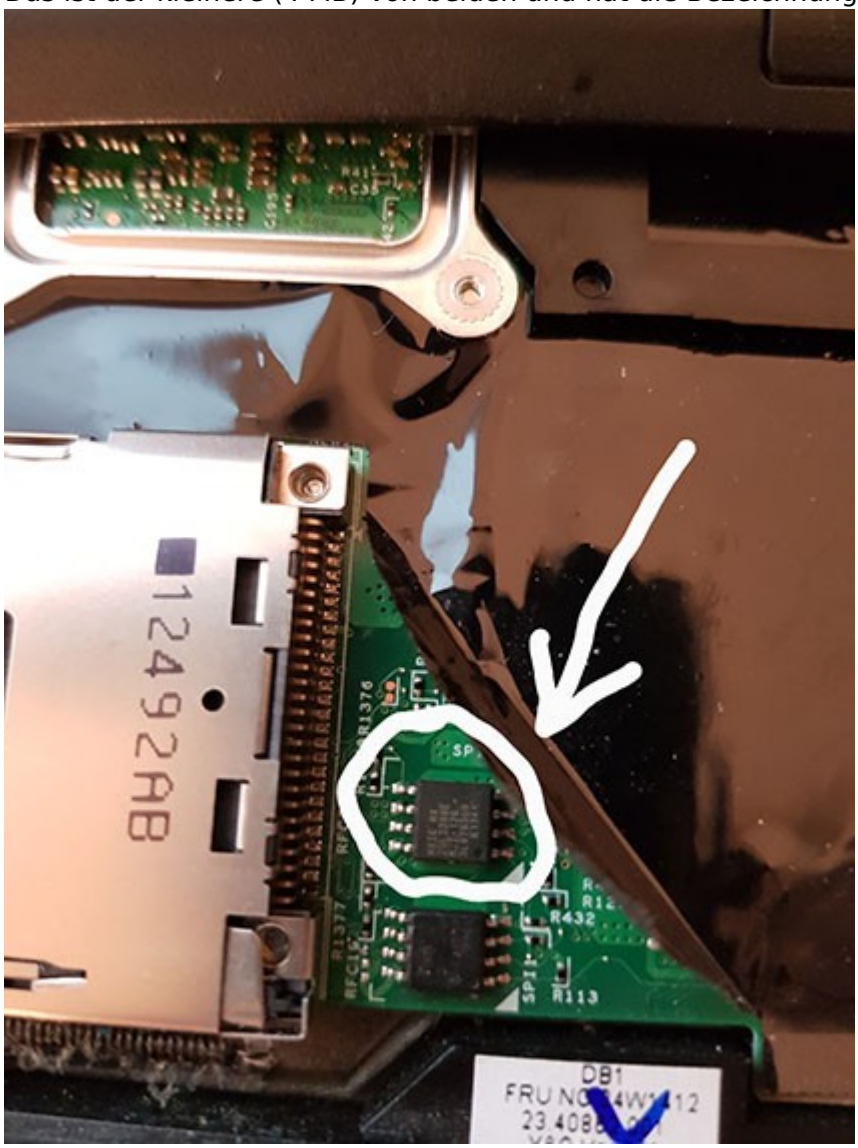
Beitrag von „Andy51105“ vom 29. April 2018, 19:52

Nach Absprache mit Sascha_77 ergänze ich diese Anleitung für das Lenovo Thinkpad X230.

Hardwareseitig sind nur wenige Unterschiede vorhanden, aber gerade beim flashen sind diese entscheident.
Diese Anleitung ist also nur eine Erweiterung zum auslesen und beschreiben der Chips. Alles andere ist gleich.

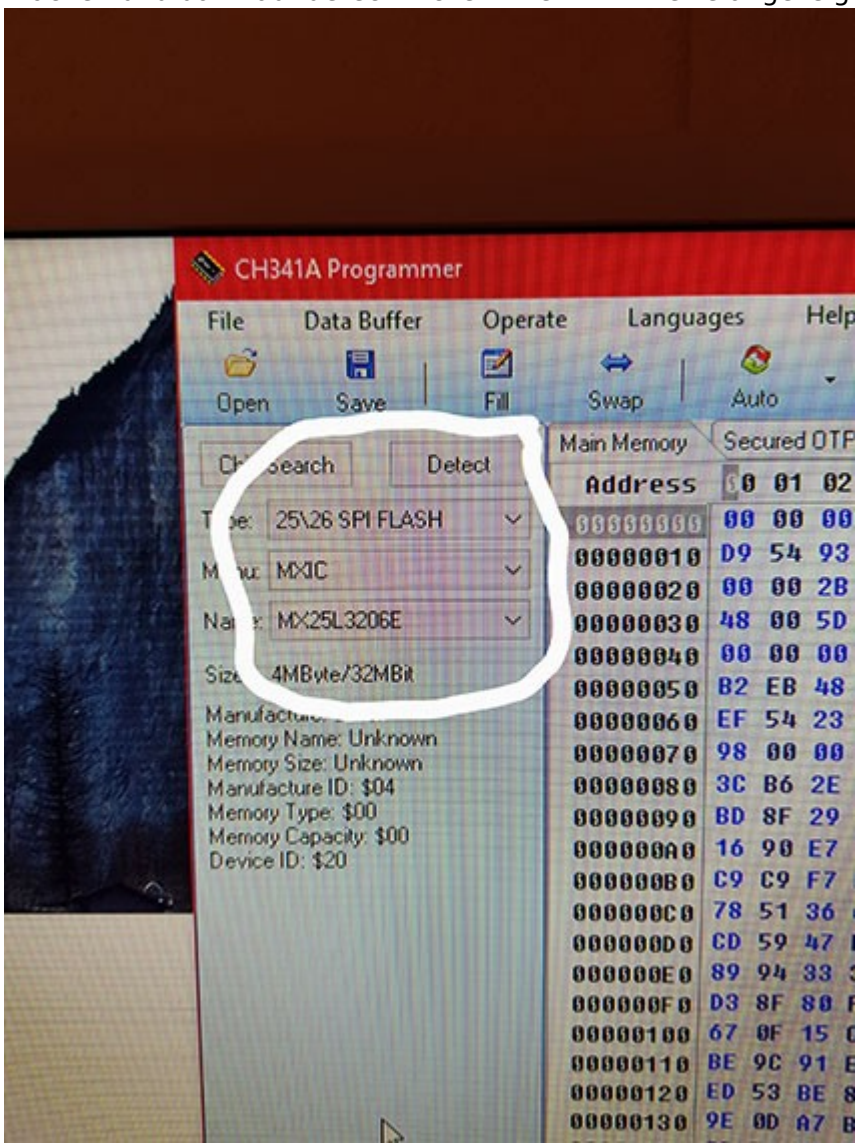
Das X230 besitzt nämlich 2 Bios-chips und das sind auch noch verschiedene untereinander.
Die beiden Chips befinden sich auf der Oberseite direkt neben dem PC-Card Einschub.

Um die Whitelist zu entfernen, braucht ihr nur die Datei des markierten Chips.
Das ist der kleinere (4 MB) von beiden und hat die Bezeichnung: MX25L3206E



Wenn ihr eure Zange angeklemmt habt, müsst ihr die Einstellungen wie auf dem nächsten Bild

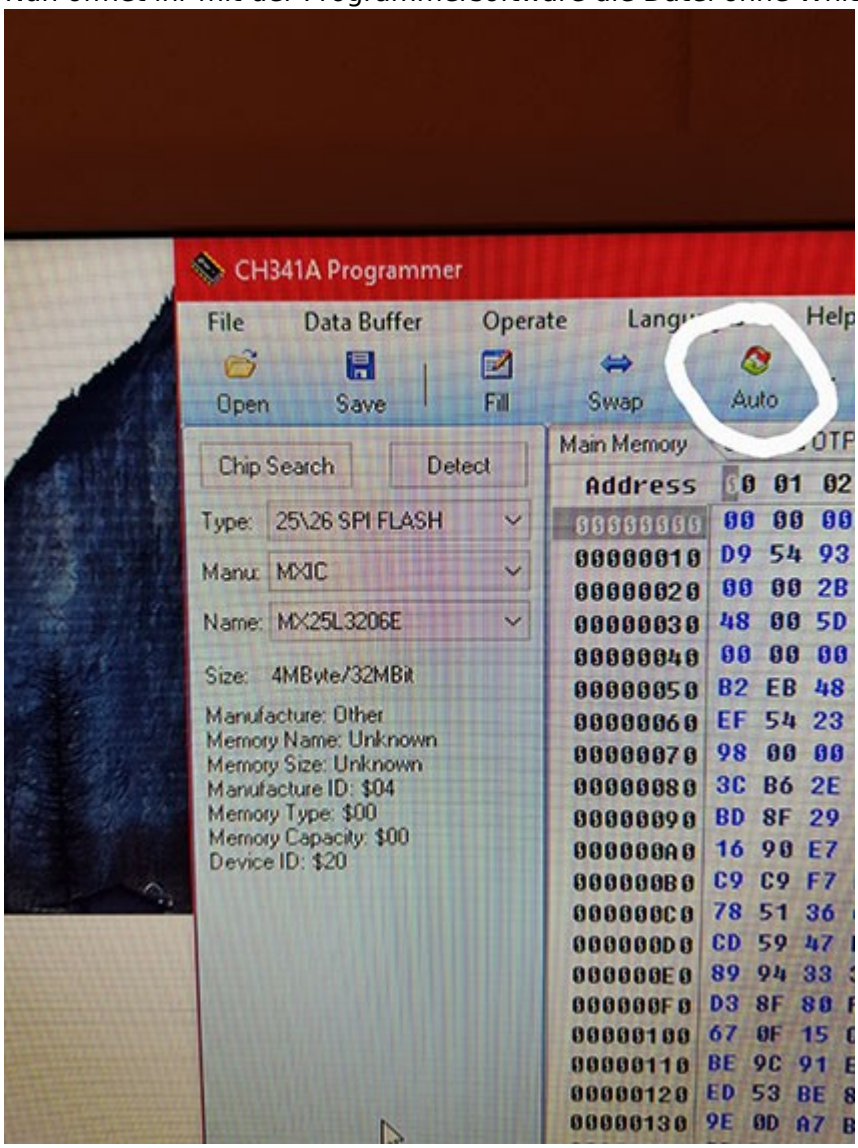
machen und dann auf detect klicken. Wenn ihr Werte angezeigt bekommt, ist alles richtig.



Nun klickt ihr, wie Sascha_77 schon beschreibt, auf "Read" und lasst euch in dem ausgelesenen File die Whitelist entfernen.
Es gibt im Netz auch eine Anleitung zum entfernen der Whitelist, wer das selber machen möchte. Ich habe es beim gleichen Anbieter machen lassen, wie Sascha_77.

Wenn ihr die Datei ohne Whitelist habt, klemmt ihr wieder eure Zange an und wählt, wie oben beschrieben, die richtigen Einstellungen und überprüft es mit einem Klick auf detect.

Nun öffnet ihr mit der Programmersoftware die Datei ohne Whitelist und klickt auf "Auto"



Das Programm arbeitet 3 Schritte ab. Löschen, Schreiben und Prüfen.
Am Ende solltet ihr eine positive Meldung bekommen und habt es geschafft.

Man kann auch noch weitere Dinge im Bios freischalten. Da ich das aber nicht brauchte, habe ich auch nur die Whitelist entfernt. Ansonsten muss man die Prozedur dann auch mit dem anderen Chip machen. Dieser nennt sich bei mir MX25L6406E und hat 8 MB Kapazität.

Im Netz habe ich öfter gelesen, daß manche von einer separaten Stromquelle von ca. 3V

reden, die unbedingt benötigt wird.
Ich kann nur von meinem Fall reden und da habe ich ausschließlich die gleichen Gerätschaften verwendet, die Sascha_77 im 1. Beitrag verlinkt hat. Bei mir hat alles gleich beim ersten Versuch funktioniert.

Viel Spaß beim Nachmachen...

Beitrag von „E$O“ vom 7. August 2018, 00:55

Moinsen ihr lieben...
hab jetzt meinen Bios Dump gespeichert, weiß jetzt aber nicht so recht weiter, an welchen "Anbierter/ Mod" ich mich bei bios-mods.com melden soll.
Welchen Anbieter habt ihr da genommen?

@Sascha_77 könntest du mir ne gute Empfehlung für eine Wifi/BT Combo für das T440 geben (sollte wenn möglich einfach ins System zu integrieren sein)?

Gruß aus Berlin 👍

Beitrag von „Sascha_77“ vom 7. August 2018, 07:49

Ja, das kann ich. Nur AC Wlan kann man nicht voll auskosten da im T440 nur 2 WLan Antennen sind. Man kann sich nat. eine 3. dazubasteln.

https://www.ebay.de/itm/DELL-D...1-Hackintosh/192503537260

Beitrag von „E$O“ vom 9. August 2018, 14:50

@Sascha_77 danke für die Empfehlung.

Ich komme nur leider mit dem bios-mods.com Forum nicht klar (zu unübersichtlich für mich) könntet ihr mir einen Link zu eurem Modder schicken?

Beitrag von „Sascha_77“ vom 9. August 2018, 15:20

Hier: ... ...

https://www.bios-mods.com/foru...Fi-WWAN-Whitelist-Removal

Beitrag von „krutojmax“ vom 9. August 2018, 22:35

Da ich hier beim Test- Lenovo x240 auch endlich MacOS mit WLAN Support haben möchte, wollte ich den Bios Chip auch auslesen und an die Kollegen von bios-mods schicken. Das NB lag bei mir lange in der Ecke und ich dachte, dass ich mir das Teil doch auch mit einem Hacky fertigmachen könnte.
Ich habe mir auch die benötigte Hardware besorgt und den Chip ausgelesen (eine 16MB große Datei). Diese habe ich dort gepostet und einer meldete sich bei mir.
Egal wie oft ich es versuche (mittlerweile mit 2 verschiedenen Kabeln), sagt mir der Modder, dass mein Dump falsch sei.

Habt ihr schon mal erfolgreich ein x240 ausgelesen? Vielleicht müsste ich was beachten?

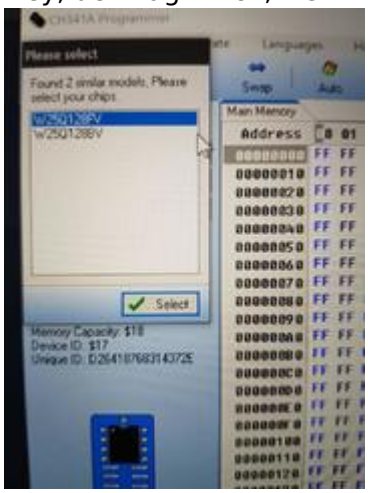
Beitrag von „jboeren“ vom 10. August 2018, 10:54

Welchen chip wird vom Programmer erkannt?

Zitat: "Yes x240 has only one 16MB chip. 25Q128FVSSIQ. FPT recognizes it as 25Q128BV though. That's because both chips share the same hardware id. And FV and Q appears to be the newer version with quad speed bit turned on."

Beitrag von „krutojmax“ vom 10. August 2018, 15:57

Hey, der fragt mich, wenn ich auf detect klicke, nach, welchen Chip ich habe:



Dann klicke ich auf die "FV" Version und sehe folgendes:

Dann klicke ich auf "read" und zum Schluss auf "save". Das war's. Und der Bearbeiter bei Bios-Mods sagt immer, es sei ein falsches Dump. ☹️

Unter folgender Anschlusskonfiguration wird der Chip erkannt:

Wenn ich die Platte beim Programmer tausche, wird der Chip nicht mehr erkannt. Also scheint dort alles richtig angeschlossen zu sein.

/ edit

Ok, hat sich erledigt. Das Gerät geht gar nicht mehr an. ☹️

Beitrag von „jboeren“ vom 10. August 2018, 16:16

Der Programma scheint den richtigen chip zu finden; das ist schon mal gut!

Kannst du Texte im fenster lezen? Irgend etwas? Vielleicht über die Suchfunktion?

edit:
Hast du den chip gelesen mit oder ohne stromversorgung/batterie?

Beitrag von „krutojmax“ vom 10. August 2018, 16:24

Welche Texte im Fenster meinst du?

Ich hatte die BIOS Batterie und die interne Batterie noch angeschlossen gehabt, als ich den Chip ausgelesen habe.
Ansonsten war das Gerät währenddessen immer aus.
Aber nun leuchtet nicht mal die LED, wenn ich Stromkabel anschließe. Das Gerät startet überhaupt nicht mehr, schade.

Beitrag von „jboeren“ vom 10. August 2018, 16:27

Oft kann man irgendwelche bios-texte im Fenster lesen.

Merkwürdig das er jetzt überhaupt nicht startet

Beitrag von „krutojmax“ vom 10. August 2018, 16:30

Ja, da waren Zahlen und Buchstaben (Hexadezimalsystem :)).
Hab ja auch noch die .bin Datei, die aber offenbar falsch ist.
Und nun fährt hier gar nichts mehr hoch, richtig merkwürdig.

Beitrag von „Raptortosh“ vom 10. August 2018, 16:55

@krutojmax Versuche mal die folgendes:
1. Notebook vom Strom trennen und Akku entfernen.
2. Bios Batterie entfernen und Kontakte kurzschliesen (z.B mit 10 Cent Münze).
3. 15 bis 30 min warten.

4. Münze entfernen und Bios Batterie wieder einsetzen.
5. Versuchen zu starten.

Beitrag von „Sascha_77“ vom 10. August 2018, 19:52

Wir hatten auf den letzten Hackcon das Gleiche Thema mit einem Lenovo. Haben den Chip ausgelesen und dem Typen von mod bios geschickt. Er meinte er könne damit nichts anfangen. Ende vom Lied war, dass der Rechner auch kein Lebenszeichen am Ende mehr von sich gab. Wenn ich das hier so lese habe ich glaube bei meinem T440 einfach nur großes Glück gehabt das Alles auf anhieb funktionierte und am Ende sogar wieder anging. Bin mal gespannt was bei dir rauskommt. Zumal du ja einfach nur normal ausgelesen und nichts auf den Chip zurückgeschrieben hast. 🤨

Das habe ich noch in einer Amazon-Rezi gefunden:

> Zitat
>
> Wichtig wäre bei neueren Chips noch das man die neueste Version der gängigen Windows-Software benutzt (>1.18, z.b 1.29), da die älteren nicht in der Lage sind verschiedene Revisionen neuerer Chips korrekt zu identifizieren

---

Beitrag von „E$O“ vom 17. August 2018, 12:54

Sorry leute, ich weiß bin echt ne Nervensäge was das angeht aber ich krieg das mit dem BIOS DUMP immer noch nicht hin..
Habe jetzt unzählige male versucht den Chip auszulesen (verschieden Programmer Versionen, verschiede Win Versionen pi pa po), nada. Mit jedem Bios Dump den ich den Jungs vom bios-mod Forum schicke können die nichts anfangen.
Immer kommt die gleiche Antwort: Mein Dump sei fehlerhaft. Habe jetzt auch in ein paar Foren gelesen das es mit dem T440 Chip wohl öfters Probleme gibt (Sind aber relativ alte Beiträge, <2015).

Hätte einer von euch ne Idee wie man auf nem anderen Weg die Whitelist weg bekommt? Möglicherweise die "alternative zum dumpen" (mit der offiziellen -> gemoddeten BIOS update .exe, falls das noch möglich ist, da @Sascha_77 das ja durchgestrichen hat).

Beitrag von „Sascha_77“ vom 17. August 2018, 12:57

Eine Alternative dazu gibt es leider keine. Aber spannend das es speziell bei dem T440 schwierig sein kann. Evtl. mal die neuste offizielle Version flashen und dann nochmal versuchen auszulesen?

Beitrag von „E$O“ vom 17. August 2018, 14:16

Och nö, dann muss ich ja die alte windoof Platte rauskramen hoffe Mal das es dann was wird kriege langsam meine Macken mit dem öden WLAN stick

---

Beitrag von „Sascha_77“ vom 17. August 2018, 18:08

Wobei ich mir nicht vorstellen kann das es daran liegt. Aber wäre so meine letzte Idee. So hättest es zumindest mal ausprobiert.

Beitrag von „Senseye“ vom 17. August 2018, 18:35

@E$O wieso nimmst du nicht einfach das fertig gemoddete bios von Sascha_77? Der hat doch auch ein T440

Beitrag von „Sascha_77“ vom 17. August 2018, 19:00

Das geht nicht weil jedes BIOS individuell gemoddet wird (wegen Seriennummer der Hardware etc). Früher haben die Jungs direkt das offizielle BIOS gepatcht und man konnte es universell auf jeden Typ des Rechners spielen. Da die dort aber auch auf Spendenbasis arbeiten kommt nat. mehr zusammen wenn jeder sein persönlichen Mod bekommt.

Beitrag von „E$O“ vom 18. August 2018, 12:41

@'Senseye soweit ich das richtig verstanden habe hat er das Model mit einem i5 und ich mit dem i7, wobei es vom T440 (ohne p/s am Ende) auch noch sehr verschiedene Varianten gibt. Habe bisschen Angst mir das Teil zu bricken, da ich das Teil jeden Tag brauche..
Sascha_77 was denkst du, gibt es da doch noch den einen unter 100 der mir das offizielle BIOS patcht?

Habe gerade im Postfach nachgeguckt und tadaa, eine kleine Karte die eingebaut werden möchte aber nicht darf 😪

Beitrag von „Senseye“ vom 18. August 2018, 15:57

@Sascha_77 kann dir doch einfach die Wlan.ffs (oder wie die sich nennt) aus seinem Bios extrahieren. Dann kannste das original update von lenovo laden und die eine Datei austauschen.

Oder falls ihr das gleiche Model habt T440/T440S kannste auch einfach sein Bios flashen. Musste nur vorher deine Seriennummer etc. sichern und dann wieder zurückschreiben.
Ob i5 oder i7 spielt keine Rolle. Microcode ist für alle CPUs im Bios vorhanden.

Welche genaue Bezeichnung haben denn eure beiden Lenovos? Mit S oder P oder ganz ohne?

Beitrag von „krutojmax“ vom 18. August 2018, 21:50

Hey,
ich hab die gleichen Erfahrungen mit dem x250 gemacht.
Egal, wie viele Dumps erstellt werden, Dodu sagt mir immer, diese seien fehlerhaft.

Mittlerweile sagt er mir, ich solle mir die Version 1.3xx kaufen und hat mir einen Link geschickt...

Beitrag von „E$O“ vom 19. August 2018, 02:25

@Senyseye habe den "normalen" T440 ohne Anhängsel..

Beitrag von „krutojmax“ vom 19. August 2018, 19:38

Gute Nachrichten,

nachdem ich die v1.34 für 10USD gekauft habe und nochmal einige Anschlusskabel vom Programmer zum BIOS Chip ausprobiert habe, hat der Mod Dodu ein "ok" gegeben. Mein Dump scheint endlich "normal" zu sein.
Jetzt warte ich darauf, dass er die Arbeit vollendet und sehe dann zu, dass ich das auf das x250 flashe.

@Sascha_77

Hat dein T440p auch einen TPM Chip?
Kann man den nach dem Flashen nicht mehr verwenden?

Ich habe u.a. folgende Info bekommen:

Spoiler anzeigen

Beitrag von „Sascha_77“ vom 19. August 2018, 19:45

Ich hatte dieses 2x5 Piepen. Ist aber weg gegangen. Wird dann wohl nen TPM Chip sein.

Beitrag von „krutojmax“ vom 20. August 2018, 10:50

So,
x250 erfolgreich geflasht.
Das Piepen ist jedes Mal nach Herunterfahren da, aber ist erstmal egal.

Neue Wifi-Karte verbaut, Treiber installiert und voila, läuft. 🙂

Als nächstes wird macOSx draufgemacht. 🙂

Danke euch für die Anleitung!

Beitrag von „Sascha_77“ vom 20. August 2018, 11:43

Gerade herausgefunden, dass dieses Programm die Hardware nun auch unterstützen soll. Vllt. eine nette Alternative.

https://review.coreboot.org/cgit/flashrom.git

Beitrag von „Tanzmusikus“ vom 3. September 2018, 17:15

Hallo Leute,

hier ist die v1.29 mit relativ aktueller DataBase (2016) & automatischer Chiperkennung.

Achtung: Ab v1.30 gibt es die Software nur noch inkl. persönlicher Freischaltung per SN bzw. Schlüssel.
D.h., man müsste diese SW kaufen. Ist natürlich verständlich. 2-5$ sind ja auch noch preiswert dafür.

Die neue Version bietet außerdem an, dass man "main memory", "secured OTP" oder "main memory + secured OTP" lesen/schreiben kann.
Lohnt sich also das Optionsmenü etwas zu studieren & je BIOS-Chip/Mainboard anzupassen.

Grüße, TM

P.S.
Denkt daran, dass Ihr das Programmier-Tool mit Admin-Rechten startet, sonst gibt es evtl. eine Fehlermeldung oder Probleme bei der Datenübertragung.

Beitrag von „jboeren“ vom 3. September 2018, 21:50

Danke seht!
Wo kann man 1.30 version kaufen?

Beitrag von „hitman20“ vom 3. September 2018, 22:25

Ich habe die V1.30 als Setup vorliegen, wenn man auf License Info klickt, erscheine eine Execption. Allerdings habe ich Version aus einem Pack wo mehrere Versionen von CH341A Programmer enthalten sind. Bei Bedarf kann ich die mal hochladen.

Beitrag von „Tanzmusikus“ vom 3. September 2018, 23:12

Hallo!
Die v1.30 kann ich persönlich nicht empfehlen, da sie mir zu abgespeckt vorkommt & bei mir nicht so rund läuft wie die v1.29.
@hitman20 Ab v1.30 wäre es wohl bedenklich diese offiziell im Forum zu verlinken. Gibt ja auch PN.
>> beim Hersteller mal nachfragen -> http://www.wch.cn/ <<

Oder direkt SkyGZ anmailen:

> Zitat von http://www.ouroms.com/2017/12/24/panduan-flash-ic-eeprom-spi-menggunakan-usb-programer-ch341a/
>
> Jika anda berminat untuk memperoleh Ch341A Mini Programer secara legal,
> silahkan hubungi pada developernya dengan alamat email: SkyGZ@qq.com.
> Harga software ini pada saat tulisan ini dibuat hanya 10U$. Harga yang
> relatif murah mengingat kegunaannya, apalagi mengingat resiko penggunaan
> software “free” yang sudah “ditanami” virus oleh orang-orang “kepinteran”.

> Zitat von Übersetzung durch g00l transl
>
> Wenn Sie daran interessiert sind, einen Ch341A Mini Programmer legal zu erwerben,
> kontaktieren Sie bitte den Entwickler mit einer E-Mail-Adresse: SkyGZ@qq.com.
> Der Preis dieser Software zum Zeitpunkt des Schreibens beträgt nur 10 US-Dollar. Der Preis
> relativ günstig in Anbetracht seiner Nützlichkeit, insbesondere unter Berücksichtigung des Verwendungsrisikos
> "freie" Software, die einen von Menschen "gepflanzten" Virus wurde mit Orang Utan "Intelligenz".

Eine GPL Linux-Version (evtl. auch in MacOS lauffähig?) gibt es übrigens hier: https://github.com/setarcos/ch341prog

Flashrom gibt's auch noch: https://review.coreboot.org/cgit/flashrom.git/

Grüße, TM

Beitrag von „a1k0n“ vom 6. September 2018, 10:51

Es ist ziemlich ratsam den Biosdump vorher per Software zu machen und anschließend per Programmer. Wenn der Hardwaredump failed habt ihr ohne Backup nur noch ein Briefbeschwerer. Würde die dumps auch anschließend per Hex überprüfen lassen.

Beitrag von „griven“ vom 18. September 2018, 21:59

Das Piepen kommt vom TPM und ist in sofern normal als das das TPM erkennt das ein modifiziertes Bios eingesetzt wird (die Checksumme bzw. Signatur ist nach der Modifikation ungültig). Man sollte sich vor dem aufspielen eines modifizieren Roms darüber im klaren sein das das TPM anschließend nicht mehr wirklich genutzt werden kann bzw. seinen Dienst mit den genannten Beeps quitiert weil die Plattform nun eben nicht mehr trusted ist. Sofern man unter Windows nicht gerade Bitlocker verwenden möchte kann man aber auf das TPM Feature relativ gut verzichten und das TPM im Bios einfach deaktivieren (SecurityChip -> Disabled) und schon ist Ruhe im Karton 😆

Beitrag von „Daniel20VT“ vom 21. Dezember 2018, 13:52

Könnte mann mit dem ch341a eine firepro 5950. in eine radeon hd6770 flashen also rom

mfg

Beitrag von „a1k0n“ vom 23. Dezember 2018, 13:20

Das kommt drauf an um was für ein EEPROM es sich handelt und ob es genug Speicher hat.

Beitrag von „Daniel20VT“ vom 24. Dezember 2018, 14:39

Gehen wir mal davon aus es hat genug speicher . Solte es ja funktionieren und ich dürfte ein bild bekommen .

Oder muss ich ein orginal i mac bios haben . Ich hab leider nur eins mit 512mb ram , meine karte hat aber 1024mb , könnte mann dieses zur not anpassen auf 1024mb ?

Mit freundlichen Grüßen

Und schöne Feiertage

Beitrag von „griven“ vom 30. Dezember 2018, 23:32

Ist möglich sofern die Karte physisch passt. Die Unterschiede bei der Bios Größe rühren daher das die Apple Varianten nur ein (u)EFI Bios besitzen während bei den PC Varianten ein Hybrid Bios zum Einsatz kommt (einer der Gründe warum sich solche Karten im Mac verbauen lassen aber erst ein Bild liefern wenn macOS die Treiber geladen hat). Was den verbauten VRAM angeht sollte das Bios aber dann aber schon dazu passen sprich ein Bios von einer Karte mit 512mb kann zwar auch mit/auf einer Karte mit 1024mb laufen muss aber nicht. Im Besten Fall nutzt die Karte eben nur 512mb im schlimmsten Fall geht es halt gar nicht. Was auch immer Du machst stell sicher das Du vor eine etwaigen Schreibvorgang auf dem EEPROM eine Kopie verifizierte Kopie des original Inhalts erstellst und gut aufbewahrst denn dann kannst Du im Falle eine Falles immer wieder auf das originale Bios zurück.

Beitrag von „Daniel20VT“ vom 31. Dezember 2018, 00:51

ich danke dir werde berichten wenn die post gelifert hat .

in diesem sine wünsch ich allen ein guen rutsch ins neue jahr

So gestern kamm mein paket hab den mac direkt zerlegt . Und ausprobiert

Er zeigt verbunden an aber kann den chip nicht lesen

Getestet am mb z97m d3h alter hd 2400

Wenn ich jetzt die spange auf die firepro setze geht die lampe von dem programmer aus und alle schaltflächen werden inaktiv

Gibt es da nich was zu beachten

Kann mir eventuell jemand sagen wo bei ner hd 6770m

Das bios sitzt habe jetzt den einzigsten chip den ich finden konnte versucht zu beschreiben, fehlanzeige geht nicht , dann hab ich gesehen gibts die selbe karte noch mal aber die hat noch einen chip links oben .

Hab von ner andern karte nen chip genommen bios geflasht , aber nix passiert

Gibt es Karten ohne bios im Notebook

Mit freundlichen Grüßen

Beitrag von „ThinkPadUser“ vom 16. Januar 2019, 08:22

Funktioniert die Methode auch für das LenovoThinkpad X250?

Beitrag von „grt“ vom 16. Januar 2019, 09:16

soweit ich weiss, hat das X250 keine whitelist mehr.

oder warum willst du flashen ThinkPadUser ?

Beitrag von „ThinkPadUser“ vom 16. Januar 2019, 09:25

grt habe das Thinkpad vor einigen Monaten bei ebay erworben und mir ist erst jetzt aufgefallen dass das BIOS passwortgeschützt ist. Habe bereits den Verkäufer kontaktiert, welcher mir nur entgegnet hat, dass er nicht wüsste dass dafür ein Passwort vergeben wurde. Zurückgeben geht auch nicht mehr, also versuch ich seit geraumer Zeit das Problem selbst in die Hand zu nehmen, was sich als komplizierter herausgestellt hat als anfänglich gedacht

---

Beitrag von „Sascha_77“ vom 16. Januar 2019, 09:34

Hm kann man das nicht zurücksetzen indem man sämtlichen Strom abklemmt inkl. CMOS Batterie?

Einfach nur flashen wird denke ich nichts bringen, da das Passwort ja nicht im BIOS Chip hinterlegt wird. Korrigiert mich wenn ich falsch liege.

Beitrag von „ThinkPadUser“ vom 16. Januar 2019, 09:36

Sascha_77 nein das geht bei den neueren TP Modellen wohl nicht mehr, meine Recherchen haben ergeben dass ein entfernen der CMOS Batterie den Laptop unbrauchbar macht weil beim nächsten Systemstart dann die Uhrzeit eingegeben werden MUSS was zur Abfrage des Supervisor Password führt.

Versteht mich nicht falsch, mein Laptop ist voll funktionsfähig mit Win 10 drauf das einzige wo ich kein Zugriff habe ist das BIOS.

Beitrag von „grt“ vom 16. Januar 2019, 09:44

wenn das passwort nicht im bios hinterlegt ist, wird auch flashen nix bringen...

ich hab dunkel in erinnerung, dass sich bei den T61 ein biospasswort mit feinen drähtchen auf die bioschip-füsschen löten/klemmen und miteinander/mit masse/whatever verbinden löschen liess. fummelarbeit, aber es soll funktioniert haben.

ggf geht beim X250 auch sowas?

sagt die tante gugl was dazu?

Beitrag von „EaseYourPain“ vom 16. Januar 2019, 09:57

Dann könnte das vielleicht für dich interessant sein.

Beitrag von „ThinkPadUser“ vom 16. Januar 2019, 10:00

EaseYourPain Hab Angst durch das Kurzschließen was kaputt zu machen

---

Beitrag von „EaseYourPain“ vom 16. Januar 2019, 10:01

Hätte ich auch, ist ja aber auch nur ein Lösungsvorschlag.

Dieses hier passt noch besser zu der x Serie. Ändert aber nichts an der Methode

---

Beitrag von „ulli“ vom 8. Februar 2019, 21:26

Hi,

hat das jemand schon an einem T430**s** probiert und kann mir das evtl. moralischen Support geben es auch zu tun?

Das BIOS habe ich mittlerweile wohl ausfindig machen können:

https://www.coreboot.org/Board:lenovo/t430s

Des weiteren greife ich die Frage von hier mal auf: Hat jemand (und wenn ja wie) vom User DuDu2002 aus dem mod-bios Forum das BIOS gepatcht bekommen?

Beitrag von „EaseYourPain“ vom 8. Februar 2019, 21:36

~~Wieso, hast du ein BIOS-Passwort Problem?~~

Ah bezog sich nicht darauf Sorry

Beitrag von „ulli“ vom 8. Februar 2019, 21:44

Sorry...hatte ich vergessen zu erwähnen, dass es sich um das Entfernen der whitelist dreht

---

Beitrag von „EaseYourPain“ vom 8. Februar 2019, 21:48

Musst du nicht erwähnen, da das das eigentliche Thema des Thread ist.

Beitrag von „vviolano“ vom 8. Februar 2019, 23:48

ulli Das T430S hat einen zu kleinen Bios-Chip, Da passt die Programmer-Zange nicht drauf. Habe ich damals mit Sascha_77 beim Stammtisch ausprobiert.

Beitrag von „ulli“ vom 9. Februar 2019, 08:47

Hi vviolano!

vielen Dank für deine Reaktion! Kannst du dich noch erinnern ob es der Chip hier war?!

Bei der Anleitung von coreboot benutzen sie den gleichen clip wie ich am x230. Was hattet ihr für einen?

Beitrag von „grt“ vom 9. Februar 2019, 09:38

du flashst mit einem raspi?

und woher kommt die zange?

Beitrag von „ulli“ vom 9. Februar 2019, 09:53

Das ist doch das Bild aus der coreboot Anleitung

Beitrag von „grt“ vom 9. Februar 2019, 09:58

achsoooo....

war gestern so beschäftigt, dass ich den link nur zur kenntnis genommen, aber nicht

angeguckt hab

Beitrag von „ulli“ vom 9. Februar 2019, 10:08

Ich werde mich aber bald nicht mehr zurück halten können. Habe zwar nur einen Clip für die SOIC-8 chips (wie die aus dem x230) und nicht für die WSON-8 Bauform, nen Versuch ist es aber wert. Wenn das nicht klappt ist ohne Auslöten kein whitelist freies BIOS auf dem T430s möglich.

Beitrag von „Sascha_77“ vom 9. Februar 2019, 10:24

Theor. dürfte mit richtiger Zange nichts dagegen sprechen, dass es nicht klappen sollte. So gesehen sind die Bios Chips eigtl. alle irgendwie gleich und unterscheiden sich nur durch die Baugröße.

Glaube nicht, dass ein Laptophersteller seine eigenen Chips produziert dafür. Die werden alle von der Stange sein.

Beitrag von „ulli“ vom 9. Februar 2019, 11:15

Eine WSON-Zange habe ich nach kurzer Recherche nicht gefunden. Da ihr es ja mit der SOIC-Zange schon ausprobiert habt, und im Netz weitere Misserfolge vermeldet werden (https://www.win-raid.com/t796f...PI-EEPROM-7.html#msg44276) scheint es wohl im Moment keine Lösung zu geben.

Erschwerend kommt hinzu, dass der BIOS-Chip des T430s mit WSON-8 Bauform nur mit einer Heißluftstation entfernt werden kann - ein normaler Lötkolben erreicht die Pins unter dem Chip nicht. Das ist eine ganz bittere Erkenntnis..

Beitrag von „Sascha_77“ vom 9. Februar 2019, 11:49

Das ist natürlich mist. ☹️

Beitrag von „grt“ vom 9. Februar 2019, 12:08

> Zitat von ulli
>
> mit einer Heißluftstation entfernt werden kann - ein normaler Lötkolben erreicht die Pins unter dem Chip nicht

mit einem normalen lötkolben mehrfüssige smd-chips auslöten ist der horror... da sind fix mal die lötpins auf der platine mit ab. würde ich jetzt soo schlimm nicht finden, den chip mit heissluft abzumachen. schlimmer fänd ich ihn überhaupt abmachen zu müssen - egal wie

---

Beitrag von „vviolano“ vom 9. Februar 2019, 13:19

Nun, habe mal die Zange ausfindig gemacht: https://www.ebay.de/itm/Origin...kEAAOSwze5bzsMk:rk:1:pf:0

ulli Ich denke dass war er.

Beitrag von „grt“ vom 9. Februar 2019, 13:26

puh.... teuer teuer.. müsste man einfach selbst drucken sowas.

Beitrag von „Sascha_77“ vom 9. Februar 2019, 13:34

40 Schleifen?? Vllt. ist ja goldene Litze im Kabel. Hab für mein Zeug damals komplett 6 Euro bezahlt und da war der Programmer mit enthalten.

Beitrag von „ulli“ vom 9. Februar 2019, 13:34

vviolano : Danke! Sascha's 5 EUR Zange tuts aber auch ..wird aber bei dem T430s halt net passen..

Bin ich grade gefrustet..

Beitrag von „vviolano“ vom 9. Februar 2019, 13:41

Vielleicht passt die Zange ja bei dem T430s?

Scheint ja so laut Bild. Oder?

Beitrag von „ulli“ vom 9. Februar 2019, 13:49

> Zitat von vviolano
>
> ulli Das T430S hat einen zu kleinen Bios-Chip, Da passt die Programmer-Zange nicht drauf. Habe ich damals mit Sascha_77

> beim Stammtisch ausprobiert.

ich dachte das hattet ihr schon probiert?!

Beitrag von „vviolano“ vom 9. Februar 2019, 15:53

Ja. Aber ist es auch die selbe Zange, oder ist bei der irgendetwas anders?

Beitrag von „ulli“ vom 10. Februar 2019, 22:48

Ich habe es an meinem T430s mal probiert. Leider wie befürchtet keine Chance mit der Zange an die Löt"füße" des BIOS Bausteines zu kommen. Es sind auch eher kleine Lötbällchen, die fast eben auf dem Board sitzen. Bei der Zange sind die Kontaktstifte leicht im Gehäuse eingelassen und kommen so niemals an diese Lötpunkte ran.

Beim T430s bleibt daher nur Auslöten -> Auslesen -> Patchen -> Rückschreiben -> einlöten

Am besten gleich diesen Chip durch einen mit SOIC-8 Bauform ersetzen, um zukünftig im Notfall nochmal drüber flashen zu können.

edit: a1k0n Ich bin grade über deinen Artikel hier gestolpert: BIOS Recovery - CH341a USB 24/25 SPI Flash EEPROM Programmer

Anscheinend kennst du dich "ein wenig" mehr aus wie ich. Hast du evtl. noch eine Idee was man machen könnte?

C25
MXIC L132291
MX25L12835EZNI-10G
7A653900

Beitrag von „userport“ vom 11. Februar 2019, 07:29

Das EEprom auf dem Foto lässt sich mit etwas Löterfahrung auch ohne einer Heissluftstation ablöten, da es Beinchen nur von zwei Seiten hat.

Ich empfehle hier zum Auslöten auf jeden Fall verbleites Lötzinn (bessere Fließeingenschaften) und eine nicht zu dünne Lötspitze.

Die Beinchen auf beiden Seiten einfach alle zusammenlöten und dann beide Seiten des ICs in schneller Folge gleichzeitig heiss machen...in der Regel lässt sich das IC dann problemlos mit einer Pinzette abziehen.

Beitrag von „Sascha_77“ vom 16. Februar 2019, 18:34

Haben es beim Stammtisch auch nochmal am T430s probiert. Habe die gleiche Zange wie 2 Posts hier drüber. Wir haben jetzt auch die vordere Plastiklippe weggefeilt damit die Kontaktpinne weiter rauskommen. Keine Chance. Haben jetzt bei Aliexpress diese eine blaue Zange da bestellt und beim nächsten mal gibts den nächsten Versuch.

Beitrag von „userport“ vom 21. Februar 2019, 05:55

Sascha_77

Direkt Kabel anlöten und nach dem Programmieren wieder ablöten wäre auch eine Möglichkeit, falls die neue Zange evtl. auch nicht passen sollte.

Beitrag von „derHackfan“ vom 21. Februar 2019, 23:11

userport So einfach die Idee so witzig und gut finde ich sie, eigentlich braucht man sie gar nicht ablöten sondern nur mit Isolierband trennen, vielleicht wegen dem nächsten Update.

Beitrag von „userport“ vom 22. Februar 2019, 17:22

Oder einfach direkt einen Steckverbinder/Header auflöten, da gibt es unzählige Varianten wenns mal in den Fingern kribbelt...

Beitrag von „vviolano“ vom 28. März 2019, 10:44

Meine Blaue Zange ist angekommen. Werde es beim nächsten Stammtisch zusammen mit Sascha_77 ausprobieren.

Beitrag von „griven“ vom 28. März 2019, 11:20

Na da freue ich mich jetzt schon drauf

Muss ja mal irgendwann klappen...

Beitrag von „Sascha_77“ vom 28. März 2019, 13:22

vviolano

Wie Schaut die Zange vorne aus? Kannst Du mal ein Foto machen?

Beitrag von „rubenszy“ vom 28. März 2019, 13:54

Was ihr braucht ist das eher

habe ich mir auch geholt, gerade für Grafikkarten.

https://www.ebay.de/itm/Progra...452c50:g:6G8AAOSweadbHO7-

Beitrag von „vviolano“ vom 28. März 2019, 13:57

Sascha_77

So schaut sie aus.

Beitrag von „rubenszy“ vom 28. März 2019, 13:58

Bringt also nicht den gewünschten Erfolg die Zange.

Beitrag von „Sascha_77“ vom 29. März 2019, 09:22

Dann feile schonmal die Plastiküberstände weg. Die sind ja massig lang.

Beitrag von „krutojmax“ vom 1. Mai 2019, 22:02

Wisst ihr, ob man auch mit den Utensilien (Seite1) den Bios-Chip des T570 auslesen/flashen könnte? 🙂

Beitrag von „griven“ vom 1. Mai 2019, 22:45

Vorsichtig gesagt ja man könnte wobei hier wirklich könnte der Ausschlaggebende Faktor ist.

Ob es klappt hängt vom verbauten EEPROM ab es gibt welche die im BGA Format daher kommen (T420/T430 zum Beispiel haben die) da hat man mit einer Zange kaum eine Chance an die Pins zu kommen bei den "normalen" Käfern klappt das aber recht gut.

Beitrag von „EaseYourPain“ vom 12. Mai 2019, 21:00

Hab es beim X240 erfolgreich flashen können.

~~Wisst ihr eigentlich wo sich der BIOS-Chip auf dem X230 Board befindet? Muss ich das Ding komplett auseinander nehmen?~~

EDIT: Ich Dödel, steht ja gut beschrieben am Anfang des Threads

---

Beitrag von „ulli“ vom 12. Mai 2019, 21:11

bei meinem x230 Tablet ist er hier:

Beitrag von „EaseYourPain“ vom 12. Mai 2019, 21:16

Danke Dir - ist ja schom mal ne Orientierung.

Werde ich mir die Woche mal anschauen.

Beitrag von „ulli“ vom 12. Mai 2019, 21:56

schön, dass ich ausnahmsweise dir mal helfen konnte

Beitrag von „EaseYourPain“ vom 12. Mai 2019, 23:46

Wusste gar nicht, dass ich dir schon mal geholfen habe, aber bitteschön

---

Beitrag von „sksh“ vom 19. Mai 2019, 19:44

Ich war die letzten 2 Tage dabei, das mit meinem T530 zu machen.

Aber egal was ich versuche, ob ich den Chip unter Linux mit Flashrom auslese oder mit dem Windows-Tool, der gute Dudu2020 von bios-mods sagt immer, dass der Dump falsch ist.

Hab mir jetzt erstmal einen zweiten Clip bestellt, weil der eine Pin irgendwie zu kurz ist (siehe Foto).

Vielleicht ist aber auch einfach die BIOS-Version zu neu für die Tools, es gab nämlich Anfang April ein BIOS-Update. Da müsste ich mal schauen, ob ich noch die alte Version irgendwo habe und einen Rollback durchführen kann. Bei Lenovo ist jedenfalls nur das neueste BIOS zu finden.

Beitrag von „EaseYourPain“ vom 19. Mai 2019, 19:48

Hi womit liest du aus bzw. welche Programme hast du versucht?

Beitrag von „sksh“ vom 19. Mai 2019, 19:58

Hi,

ich hab das von Sascha verlinkte Tool in mehreren Versionen ausprobiert und ein Programm für Linux namens Flashrom, das hier im Thread auch schon erwähnt wurde.

https://github.com/flashrom/fflashrom

Ich tippe im Moment darauf, dass der Clip die Ursache ist, da die Erkennung des Chips nur sporadisch klappt.

Aber selbst wenn ich dann mal was auslesen konnte, waren die MD5 Prüfsummen immer unterschiedlich.

Beitrag von „EaseYourPain“ vom 19. Mai 2019, 20:07

Ich hab letztes Wochenende und gestern mein X240 und X230 erfolgreich geflasht. Das hier verlinkte Prgramm erzeugt wohl corrupte dumps. 3 Mal versucht, aber der Modder meinte immer, dass der dump nicht gut ist.

Wenn du magst, sende ich dir ein Programm, welches mir dumps erstellt hat, das sowohl die modder Klem als auch Dudu2002 für gut befunden haben. Dir muss aber klar sein, welcher Bios-Chip verbaut ist, da du bei diesem Programm alles selbst einstellen/auswählen musst.

Beitrag von „sksh“ vom 19. Mai 2019, 20:17

Das wäre echt super.

Die genaue Bezeichnung des BIOS Chips hab ich.

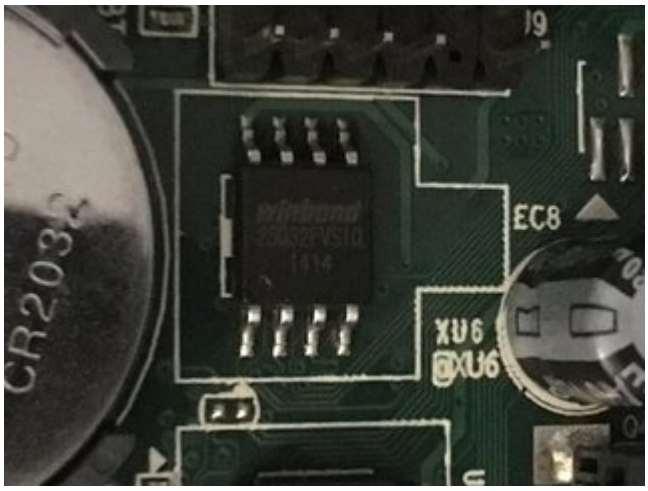
Beitrag von „EaseYourPain“ vom 19. Mai 2019, 20:31

Hast 'ne PN! 🙂

Beitrag von „EaseYourPain“ vom 26. Mai 2019, 21:12

Hallo, ich hab in meinem Tiny 2 Chips gefunden. Bin nun etwas überfragt, welcher der richtige ist...oder womöglich beide?

Kann da jemand etwas zu sagen!



Beitrag von „DonBronko“ vom 26. Mai 2019, 22:20

Ich meine zu wissen das einer das komplette Bios enthält und der andere ist für das speichern der Bioseinstellungen zuständig. Was ich machen würde, einen Dump von jedem erstellen und mit dem PhoenixTool öffnen. Dann kann man eigentlich erkennen welcher was ist.

Beitrag von „EaseYourPain“ vom 27. Mai 2019, 05:34

Ich danke dir! Ich vermute, dass es der erste ist, da ich den schon mal hatte.

Dann mach ich das mal so.

Beitrag von „a1k0n“ vom 27. Mai 2019, 12:21

Warum lest ihr euer BIOS nicht per Software aus? Die meisten EEPROMS haben doch nur eine Schreibsperre und keine Lesesperre. Bei einem Faildump per Programmer und dem einspielen ist das Geschreie dann wieder groß.

edit: Hab mal noch die 1.30er Software + Treiber angehängt. Die 1.18 erkennt leider nicht alle EEPROMS