

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 rummurt 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 einstecken 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.

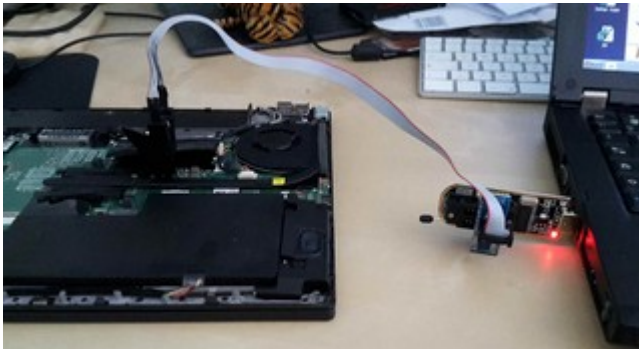


Auch gut zu sehen ist diese Vertiefung im Chip die mit einem Pfeil markiert ist. Da liegt PIN 1

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:

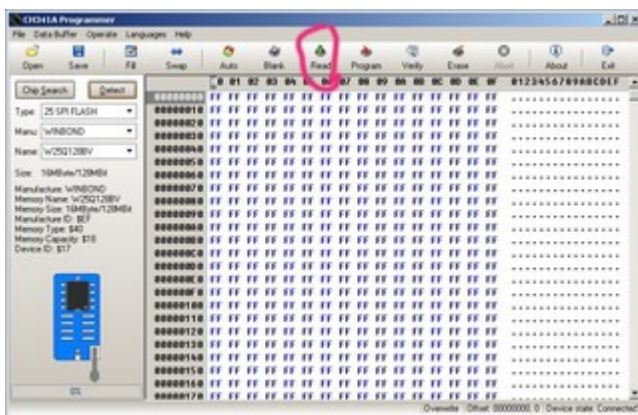


Nun drücken wir auf den "Detect"-Button. Wenn die Zange richtig sitzt sollte er jetzt ein paar Werte ausgelesen haben. Wichtig an dieser Stelle ist, das hier unterschiedliche Werte stehen. Sollte dort überall "1F" stehen sitzt die Zange nicht richtig auf dem Chip und Ihr müsst nochmal nachjustieren.

```

Manufacture ID: $EF
Memory Type: $40
Memory Capacity: $18
Device ID: $17
  
```

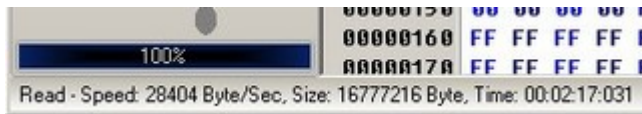
Wenn nun der Chip erkannt wurde könnte ihr ihn via "Read" auslesen.



Daraufhin sollte bei der Anzeige was tun:



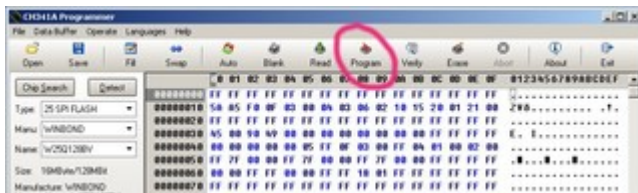
Das kann so 2-3 Minuten dauern je nachdem wie groß Euer BIOS Chip ist. Bei meinem T440 sind es 16 MB. Am Ende sollte es so aussehen:



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/> vorbeischaun 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 Programmier hat der von "flashrom" NICHT supported wird. Weil flashrom ist in G-Flash enthalten.