# MSR Unlock/Cascade Lake Refresh Firmware Fix

## Beitrag von „Mork vom Ork“ vom 19. April 2020, 15:08

Ich habe mir soeben folgendes ASUS 1201er BIOS mit folgenden Tools "gepimpt":

### UBU Version 1.76.2.5

Code

1. Scanning BIOS file ASUS_1201.rom.
2. Please wait...
3. BIOS platform - AMI Aptio V
4. BIOS version - 1201
5. Manufacturer - ASUSTeK COMPUTER INC.
6. Model - WS-X299-SAGE-10G
7. 
8. [EFI Drivers - Find and Extract]
9. Intel RST GUID 91B4D9C1-141C-4824-8D02-3C298E36EB3F
10. Intel RSTe GUID A0AD1682-AE5C-4A9C-9195-F271585CE07E
11. Intel VROC_VMD GUID EFE92A04-F5D0-4E44-8757-25B3AFA3BFFF
12. Intel VMDD GUID 02A6DE33-3EA9-4C17-8EA2-5681CC7AFDED
13. AMI NVMe GUID 634E8DB5-C432-43BE-A653-9CA2922CC458
14. NVMe Drv GUID 02A6DE33-3EA9-4C17-8EA2-5681CC7AFDED
15. Intel 1Gb GUID 6CA5C9BB-0CD1-4159-99D9-67EAD218B353
16. Intel 1Gb GUID 4953F720-006D-41F5-990D-0AC7742ABB60
17. 
18. [OROM - Find and Extract]
19. VBIOS in GUID B981F167-9D2B-4CA0-82E9-63DF0E3C3BF3
20. OROM in GUID 365C62BA-05EF-4B2E-A7F7-92C1781AF4F9
21. OROM in GUID A0327FE0-1FDA-4E5B-905D-B510C45A61D0
22. OROM in GUID A0327FE0-1FDA-4E5B-905D-B510C45A61D0
23. OROM in GUID A0327FE0-1FDA-4E5B-905D-B510C45A61D0
24. Drücken Sie eine beliebige Taste . . .
25. 
26. - - - - -
27. 
28. Main Menu
29. [Current version in BIOS file]
30. 1 - Disk Controller

31. EFI Intel RST for SATA - 17.8.0.4507
32. OROM Intel RST for SATA - 17.8.0.4507
33. EFI Intel VROC for SATA - 6.2.0.1034
34. EFI Intel VROC with VMD - 6.2.0.1034
35. EFI AMI NVMe Driver present
36. EFI NVMe Driver present
37. 2 - Video OnBoard
38. FFS-OROM VBIOS SKYLAKE Version 1049
39. 3 - Network
40. EFI Intel Gigabit UNDI - 0.0.27
41. EFI Intel PRO1000 UNDI - 9.1.12
42. OROM Intel Boot Agent CL - 0.1.16
43. OROM Intel Boot Agent GE - 1.5.88
44. 4 - Other SATA Controller
45. 5 - CPU MicroCode
46. ╔═══════════════════════════════════════╗
47. ║ MC Extractor v1.42.0 r140 ║
48. ╚═══════════════════════════════════════╝
49. ╔═══════════════════════════════════════════════════════════════════════════════════════╗
50. ║ Intel ║
51. ╠═╤═════╤═══════════════╤════════╤══════════╤═══╤═══════╤═══════╣
52. ║#│CPUID│ Platform ID │Revision│ Date │Type│ Size │ Offset │Last║
53. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
54. ║1│50657│BF (0,1,2,3,4,5,7)│5002F00 │2020-01-14│PRD │ 0xCC00│0x900090│Yes ║
55. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
56. ║2│50656│BF (0,1,2,3,4,5,7)│4002F00 │2020-01-14│PRD │ 0xCC00│0x90CC90│Yes ║
57. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
58. ║3│50654│ B7 (0,1,2,4,5,7) │2000060 │2019-06-03│PRD │ 0x8400│0x919890│ No ║
59. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
60. ║4│50652│ 97 (0,1,2,4,7) │80000037│2017-05-02│PRE │ 0x7400│0x921C90│Yes ║
61. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
62. ║5│50651│ 13 (0,1,4) │8000002B│2016-02-08│PRE │ 0x7800│0x929090│Yes ║
63. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
64. ║6│50650│ 13 (0,1,4) │8000002B│2016-02-08│PRE │ 0x7800│0x930890│Yes ║
65. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
66. ║7│906E9│ 2A (1,3,5) │ D2 │2020-01-09│PRD │0x19400│0x938090│Yes ║
67. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
68. ║8│506E8│ 22 (1,5) │ 34 │2016-07-10│PRD │0x17800│0x951490│Yes ║
69. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
70. ║9│50657│BF (0,1,2,3,4,5,7)│5002F00 │2020-01-14│PRD │ 0xCC00│0xB80090│Yes ║
71. ╠═╪═════╪═══════════════╪════════╪══════════╪═══╪═══════╪═══════╣
72. ║10│50656│BF (0,1,2,3,4,5,7)│4002F00 │2020-01-14│PRD │ 0xCC00│0xB8CC90│Yes ║

```
╠══╪═════╪═══════════════════╪═══════╪══════════╪═══╪═══════╪═══════╪═══╣
╟11╢50654╢ B7 (0,1,2,4,5,7) ╢2000060 ╢2019-06-03╢PRD ╢ 0x8400╢0xB99890╢ No ╟
╠══╪═════╪═══════════════════╪═══════╪══════════╪═══╪═══════╪═══════╪═══╣
╟12╢50652╢ 97 (0,1,2,4,7) ╢80000037╢2017-05-02╢PRE ╢ 0x7400╢0xBA1C90╢Yes ╟
╠══╪═════╪═══════════════════╪═══════╪══════════╪═══╪═══════╪═══════╪═══╣
╟13╢50651╢ 13 (0,1,4) ╢8000002B╢2016-02-08╢PRE ╢ 0x7800╢0xBA9090╢Yes ╟
╠══╪═════╪═══════════════════╪═══════╪══════════╪═══╪═══════╪═══════╪═══╣
╟14╢50650╢ 13 (0,1,4) ╢8000002B╢2016-02-08╢PRE ╢ 0x7800╢0xBB0890╢Yes ╟
╠══╪═════╪═══════════════════╪═══════╪══════════╪═══╪═══════╪═══════╪═══╣
╟15╢906E9╢ 2A (1,3,5) ╢ D2 ╢2020-01-09╢PRD ╢0x19400╢0xBB8090╢Yes ╟
╠══╪═════╪═══════════════════╪═══════╪══════════╪═══╪═══════╪═══════╪═══╣
╟16╢506E8╢ 22 (1,5) ╢ 34 ╢2016-07-10╢PRD ╢0x17800╢0xBD1490╢Yes ╟
╚══╧═════╧═══════════════════╧═══════╧══════════╧═══╧═══════╧═══════╧═══╝
```

Alles anzeigen

AMIBCP5:

Spoiler anzeigen

Ich habe folgende Änderungen via AMIBCP durchgeführt:

sämmtliche Settings, die DSM2 in seinem Tutorial zu diesem Board (ASUS x299 SAGE/10G) sind standardmässig gesetzt.

Zusätzlich habe ich folgende Settings freigeschaltet:

- ACPI Settings Configuration: hier kann ich festlegen, ob ich ACPI Settings via SSDT selber bestimme, oder ob das BIOS diese konfigurieren soll (dieses Setting ist standardmässig nicht sicht-/einstellbar)

- USB Configuration: XHCI und EHCI Handoff sind "enabled" und vom User einstellbar (diese Einstellungen sind standardmässig nicht sicht-/einstellbar und voreingestellt auf "disabled")

- PCH Storage: da ich keinerlei SATA Devices nutze (CD-ROM oder 3.5" SSDs), ist diese Funktion bei mir "disabled", da M.2 Devices anders angesprochen werden. (Müsst Ihr für Euch ggf. nach dem flashen wieder enablen)

- SETUP Boot: Fastboot = disabled, Above 4G Decoding = enabled, Show Boot Logo = disabled, SETUP-Mode=Advanced,

- SETUP Boot CSM: Boot from Network Devices=UEFI first, Boot from Storage Devices=UEFI first, Launch Video OROM = UEFI, Boot from PCI Devices=UEFI first und Launch CSM=disabled

- SETUP Monitor: Monitor CPU Fanspeed=disabled, Monitor CPU Optional Fanspeed=disabled (<--- da ich eine custom Wasserkühlung benutze und sonst bei einem CMOS-Reset jedesmal der Alarm losgeht, weil der FAN zero RPM zurückmeldet und das Board davon ausgeht, das die

CPU nicht gekühlt wird)

Diese Änderungen am Standard ASUS 1201er BIOS laufen bei mir perfekt. Anbei findet Ihr das entsprechende ROM-File zum flashen via FpTW64:

ASUS_1201.rom

**!** Dieses BIOS kann ausschliesslich via FPTW64 geflahed werden - ASUS FlashBack Feature funktioniert mit diesem ROM-File **NICHT !**

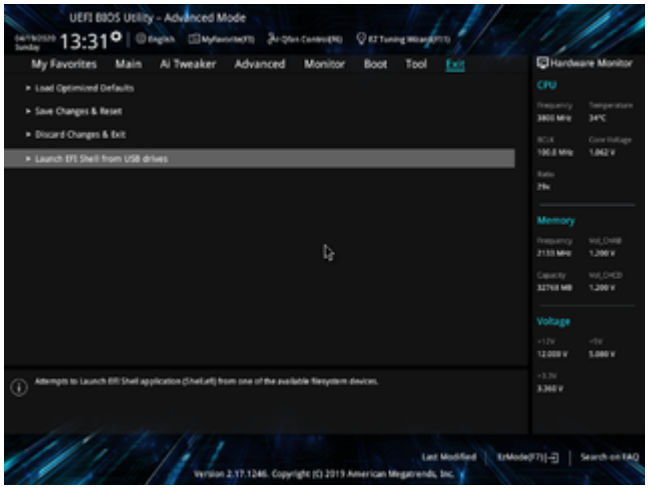
**Um dieses BIOS via FPTW64 zu flashen müsst Ihr wie folgt vorgehen: (Ich übernehme KEINE Verantwortung für das flashen. Ihr ALLEINE tragt das Risiko!)**

- flasht Euch zunächst mal Euer Board mit einem standard ASUS BIOS.

- Dann benötigt Ihr einen USB-Stick, welcher FAT32 formatiert ist. Auf diesen Stick kopiert Ihr Euch aus der angehängten FPTW64.zip Datei aus dem Ordner "FPTW64"

die Datei "Shell.efi" auf Euren USB-Stick. Der Stick muss beim booten in einem USB-Port stecken.

- Bootet in Euer derzeitiges ASUS BIOS. Geht dann im BIOS auf folgende Einstellung:




**- Hier drückt Ihr "ENTER" und es erscheint folgender Screen:**


**- Jetzt tippt Ihr folgenden Befehl:**

setup_var 0x912 0x00

**Daraufhin sollte sich bei Euch folgendes Bild zeigen:**


**Mit diesem Befehl haben wir das derzeit geflashte BIOS so freigeschaltet, das wir mittels FPTW64 nach einem Neustart unser modifiziertes BIOS flashen können. Andernfalls erhalten wir beim**

**flashen via FPTW64 einen "BIOS write protected"-Fehler!**

**- Jetzt einfach via STRG-ALT-ENTF den Rechner neu starten und in Euer WINDOWS booten. Entpackt Euch den FPTW64 Ordner aus der ZIP-Datei am besten nach C:\Temp**

**Anschliessend öffnet Ihr ein Commandfenster (CMD) als Admin und tippt dort folgende Befehle ein:**

**cd \temp\fptw64**

**Ihr wechselt damit in das Verzeichnis c:\Temp\FPTW64. Danach sollte im CMD Fenster folgendes stehen: C:\temp\FPTW64>**

**- Jetzt tippt Ihr folgendes:**

**fptw64.exe -bios -f ASUS_1201.rom**

**Das BIOS sollte nun auf Euer Board geflasht werden. Bitte achtet unbedingt darauf, dass am Ende des Flashvorgangs in etwa folgendes steht:**

Spoiler anzeigen

**Die einzelnen Einträge zu "Erasing Flash Block" und "Programming Flash Block" können bei Euch wesentlich mehr sein. Sie sind in diesem Beispiel nur deshalb so kurz,**

**weil ich das BIOS bei mir ja bereits geflahed hatte. Wichtig ist wirklich nur, daß bei Euch am Ende unbedingt "FPT Operation Successfull." steht!**

Das CMD Fenster nun via "exit" beenden und Rechner neu starten. Et voila, Euer BIOS sollte geflashed sein.

Wer von Euch beim ersten Bootvorgang einen "d4" Error gefolgt von 6 Pieptönen erhält (wie es bei mir immer passiert), der drückt einfach den Resetknopf an seinem Rechner

für einen Neustart und der Rechner sollte nun sauber booten.

**Kleiner Tipp von mir an dieser Stelle:** Ihr solltet IMMER einen USB-Stick mit einem STOCK Asus BIOS zur Hand haben, um ggf. via ASUS FlashBack Feature ein ASUS Stock BIOS flashen könnt.

Der Name des stock BIOS auf dem Stick sollte lauten: **WSXTG.CAP**