# ChameleonMini RevE Rebooted -Deutsch-

Erst einmal vorweg ich bin genau wie Ihr ein Newbie und kein Profi so wie die Anderen hier. Ich erstelle diese Anleitung für all die die wie ich extreme Probleme haben die Materie zu verstehen.

Dank der Hilfe aus dem Repo von Iceman und seinen Usern.

In dieser Anleitung geht es um das ChameleonMini RevE Rebooted von LAB401. Um die neue Firmware von Iceman&co auf das Chameleon zu schreiben geht man wie folgt vor:

Am besten nutzt man ein Linux System wie Debian, Ubuntu oder Kali Linux. Es geht aber auch mit Windows und MacOSX.

MacOSX überspringe ich da ich ein solches System nicht besitze.

Bei mir kam nur eine VMWare Kali Linux 2018.1 und Windows 10 zum Einsatz. VMWare ist eine Virtuelle Umgebung in der Kali Linux 2018.1 unter Windows 10 gestartet wird.

Hier der link:

https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/ Benutzer :root

Passwort : toor

Einfach 32/64bit Version downloaden je nachdem was man für eine Windows Version hat, wird aber heutzutage wohl auf 64bit hinauslaufen. Der Download ist ca. 2,5GB groß. Dieser wird dann in Windows gestartet und man hat ein Linux System in Windows.



Als erste sollte man in dem Linux System ein Update durchführen. Dazu ruft man im Linux System ein Terminal auf und tippt folgendes ein

#### sudo apt-get update

das sollte die Ausgabe sein. Bei dem ein oder anderen könnte auch mehr stehen und einiges mit "y" für Ja bestätigt werden.

root@kali: ~	000
File Edit View Search Terminal Help	
<pre>root@kali:~# sudo apt-get update Get:1 http://ftp.halifax.rwth-aachen.de/kali kali-rolling 2 Get:2 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/r</pre>	nRelease [30.5 kB] ain amd64 Packages [1
6.7 MB] Fetched 16.8 MB in 3s (5,156 kB/s) Reading package lists as Donetennaley Application Bin	Button c Button h Ch
root@kali:~# el.c el.h esktop	

Als nächstes muß eine bestimmte Entwicklerumgebung im Linux installiert werden.

- avr-libc
- binutils-avr
- gcc-avr
- avrdude
- libusb-dev

Hierzu muß man folgendes installieren. Dies erfolgt mit folgendem Befehl in dem zuvor geöffneten Terminal.

## sudo apt-get install avr-libc binutils-avr gcc-avr avrdude libusb-dev

					root@ka	li: ~			0	•	0
File Edit	View	Search	Terminal	Help							
<mark>root@kal</mark> Get:1 ht Get:2 ht	<b>i:~#</b> s tp://f tp://f	udo apt tp.hal: tp.hal:	t-get up ifax.rwi ifax.rwi	date h-aachen h-aachen	.de/kali ka .de/kali ka	li-rollir li-rollir	ng InRelease ng/main_amd6	[30.5 kB] 4 Packages	[16.7	7 MB	1
=etched root@kal	16.8 M <b>1</b> :~# s	B in 39 udo apt	s (5,150 i-get in	i kB/s) istall av	r-libc binu	itils-avr	gcc-avr avr	dude libust	o-dev		
ackton				intennaLev el.h				Button h	Cham Min		

Unter Umständen kann es auch sein das man die Packete einzeln installieren muß, weil es mit dem obigen Befehl in einem nicht funktioniert. Also nacheinander installieren.

sudo apt-get install avr-libc

sudo apt-get install binutils-avr

sudo apt-get install gcc-avr

sudo apt-get install avrdude

sudo apt-get install libusb-dev



Am Ende sollte alles installiert sein und es keine Fehler geben. Als nächstes wird die Software mit allen Bestandteilen auf die Linux Umgebung übertragen.

Dies geschieht mit folgendem Befehl einfach im root Verzeichnis:

#### git clone https://github.com/iceman1001/ChameleonMini-rebooted.git



Den soeben angelegten Ordner mit der Software findet man nun im "root" oder auch "Home" Verzeichnis.

10 K	ali-Linux-2018.1-vbox-a	md64 [wird ausgeführt] - Oracle VI	/ VirtualBox								-		×
Datei	Maschine Anzeige	Eingabe Geräte Hilfe			Tuo (16:2	7			14			A	1
а	schon usgefuehrt				100.3				4		. ,		
		< > < 企 Home	•					۹ ::	= 0 0	0			
	ก	C Recent				æ		1	4				
6		û Home	Chameleon	Desktop	Documents	Downloads	Music	Pictures	Public				
\$		Desktop	Mini- rebooted	/									
		Documents		A									
M		Downloads	Templates	Videos									
-		∬ Music											
-		1 Pictures											
12		☐ Videos											
8		窗 Trash											
8		+ Other Locations											\$
F													

Dann wechselt man in dieses Verzeichnis mit:

### cd ChameleonMini-rebooted

## cd Firmware/Chameleon-Mini



Um nun die Zwei neuen Dateien zu generieren die man benötigt um die Firmware auf das Chameleon zu schreiben führt man folgenden Befehl in diesem Ordner aus:

make



So sollte die Ausgabe nach dem Komplementieren aussehen und es sollten diese beiden Dateien entstanden sein.

- Chameleon-Mini.eep
- Chameleon-Mini.hex

Für die weiter Vorgehensweise werden diese beiden Dateien auf eine USB Stick kopiert und im Windows verwendet. Das sollte man auf jeden Fall machen da bei dem Firmware Update auch einiges schief laufen kann und die Erfahrung der Profis gezeigt hat das das durchschleifen des USB Ports in der VMWare nicht so optimal ist. Also zurück zu Windows.

Download der kompletten Dateien von der GitHub Seite ist ebenfalls notwendig um zum Beispiel an die BOOT\_LOADER\_EXE.exe zu gelangen.

← → C ŵ	GitHub, Inc. (US)	https://github.com/iceman1001/0	Chameleon Mini-rebooted	🛛 🛛	😭 🭳 Suchen		± ∥\	🕞 🗊	≡▲	
GPS 2018 Dome RFID201	8 🛅 chameleon	🛅 chameleon -win10	📄 Igel  🛅 IMSI Bastien Baranoff	🛅 GROW G tren	ngitter t5 multivan	😵 Hundegitter Highway	🛅 gitarre1	🛅 Gitarre	>>	
Search or jump to		Pull requests Issues M	larketplace Explore				<b>ب</b>	+• 🐠		
📮 iceman	1001 / Chame	eleonMini-rebooted		🕲 Um	vatch - 19	r Star 61 V Fork 2	5			
<> Code	() Issues (28)	🕥 Pull requests 🚺 🔲 Wi	ki <u>III</u> Insights							
Chameleon chameleon	n Mini revE rebo chameleon-mini	ooted - Iceman Fork, the Cham i nfc rfid iceman firmv	eleonMini is a versatile co <sub>vare chameleonmini</sub>	ntactless smartc	ard emulator (N	FC/RFID)				
· 2	07 commits	₽1 branch	🛇 1 release	🎎 6 cont	ributors	ৰ্ব্যুঃ View license				
Provide market	ter a	anuart .		Create new file	Unland files File	d file				
bianch: mas	ivew puilt	equest		Create new nie	opioad nies Pir					
🐺 iceman	1001 Merge pull requ	uest #58 from slurdge/master		Clone	with HTTPS 🔊	Use SSH	н			
Drivers		Added missing dlls in DFU driver		Use Git	or checkout with SV	/N using the web URL.				
Firmwa	re	Rename SPI_FLASH_INFOMY to 1	SPI_FLASHINFOMY. Fixes #56	https	://github.com/ic	eman1001/Chameleo				
Softwar	re	Add a tool for crypto and scramb	oling operations in order to us	e regul	n in Doskton	Download ZIP				
📄 .gitattri	butes	import project		ope	n in Desktop	a year ay				
📄 .gitigno	ire	import project				a year ag	o			
.travis.y	ml	fix: change directory				a year ag	o			
COMPI	LING.md	Update COMPILING.md				a year ag	D			
LICENS	E.txt	import project				a year ag	D			
READM	IE.md	Update README.md				8 months ag	o			
_config.	yml	Set theme jekyll-theme-leap-day				a year ag	0			
I READM	IE.md									
https://github.com/iceman1001/Chame	leonMini-rebooted/a	archive/master.zip	<u></u>						~	
📲 🔎 🗆 🤤 🖡	3 🚺 🛞	) 💁 🝈 🚾				45 🧕 😸 ∢	『 <u>に</u> す。》 15	14:47 2.12.2018	$\overline{}$	

So nun haben wir hier die nötigen Dateien im Windows Explorer.



Die "BOOT\_LOADER\_EXE.exe" finden wir in dem Ordner

chameleon/Software/Win32 und kopieren diese mit in den Ordner in dem die .eep und die .hex Dateien sind. Wie oben zu sehen.

Als nächstes kopierst du die Dateien aus dem FlashTool Ordner in den obigen Ordner und startest die flash.bat mit einem doppel klick.

→ ★ ↑ → Dieser PC → System (C:)	» 1			
Schnellzugriff Name	^	Änderungsdatum	Тур	Größe
avr-objcopy.exe		30.10.2018 21:07	Anwendung	572 KB
BOOT_LOADER_	EXE.exe	30.10.2018 21:07	Anwendung	61 KB
OneDrive Chameleon-Min	i.eep	10,12,2018 16:08	EEP-Datei	1 KB
joerg	i.hex	10.12.2018 16:08	HEX-Datei	66 KB
Dieser PC		30.10.2018 21:07	Anwendung	63 KB
🕽 3D-Objekte 💿 flash.bat		30.10.2018 21:07	Windows-Batchda	2 KB
🔄 Bilder 🛛 🔤 msvcr rzva.dll		30.10.2018 21:07	Anwendungserwe	1.782 KB
Desktop				
🚰 Dokumente				
Downloads				
h Musik				

Jetzt sind die Dateien entstanden die auf das Chameleon installiert werden.



Die anderen Dateien können aus dem Ordner gelöscht werden, siehe oben.

Nun ist es wichtig das die Batterie aus dem Chameleon entfernt wird und die Windows Treiber installiert werden.

Die nötigen Treiber findest Du unter chameleon/Driver.

Nun schließt du das Chameleon an den USB Port indem du die schwarze Taste gedrückt hältst und den USB Stecken in den PC steckst. Im Gerätemanager sieht das dann so aus.



As nächstes öffnest Du ein Terminl unter Windows indem DU unter Windows Start Suche "cmd" eingibst. Das kann dann so aussehen.

Copyright	owerShell (C) Microsoft Co	prporation.	Alle Rechte	vorbehalten.
PS C:\WIN PS C:\WIN PS C:\WIN PS C:\> C PS C:\> C	DOWS\system32> co DOWS\system32> co DOWS> cd d 1 dir	1		
Verze	ichnis: C:\1			
Verze: 1ode	ichnis: C:\1 LastWr	riteTime	Length	Name
Verze: 1ode 	ichnis: C:\1 LastWr  30.10.2018	riteTime  21:07	Length  62464	Name  BOOT_LOADER_EXE.exe
Verze: Mode  -a	ichnis: C:\1 LastWr  30.10.2018 10.12.2018	riteTime  21:07 16:08	Length  62464 138	Name  BOOT_LOADER_EXE.exe Chameleon-Mini.eep

Nun wechselst Du in das Verzeichnis in dem die Dateien stehen, bei mir war das unter C:\1

Suggestion [3,General]: Der Befehl	BOOT_LOADER EXE.exe wurde nicht gefunden. Er ist jedoch am aktuellen Ort vorhanden. W
indows PowerShell lädt Befehle nich	t standardmäßig vom aktuellen Ort. Wenn Sie diesem Befehl vertrauen, geben Sie statto
essen ".\BOOT LOADER EXE.exe" ein.	Weitere Informationen erhalten Sie unter "get-help about Command Precedence".
PS C:\1> .\BOOT LOADER EXE.exe	
old driver bootloader	
rasing flash Success	
hecking memory from 0x0 to 0x6FFF.	Empty.
not find file	
PS C:\1> .\BOOT LOADER EXE.exe	
old driver bootloader	
dfu-old-driver: no device present.	
PS C:\1> .\BOOT_LOADER_EXE.exe	
old_driver_bootloader	
fu-old-driver: no device present.	
PS C:\1> .\BOOT_LOADER_EXE.exe	
old_driver_bootloader	
rasing flash Success	
Thecking memory from 0x0 to 0x6FFF.	Empty.
9% 100%	Programming 0x40 bytes
[>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	Success
9% 100%	Reading 0x400 bytes
9% 100%	Programming 0x5E00 bytes
[>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	Success
3% 100%	Reading 0x7000 bytes
Load_success!	
PS C:\1>	

Wie Du hier sehen kannst habe ich nun die ".\ BOOT\_LOADER\_EXE.exe" aufgerufen und damit die Firmware auf dem Chameleon installiert.

Das war es auch schon.