<u>Мой канал на YouTube</u>

Xiaomi Redmi 9 – обход авторизации EDL.

Удаление из памяти телефона блокировки по Mi-аккаунту и Google-аккаунту (FRP).

Нам понадобиться:

- Телефон Xiaomi Redmi 9 заблокированный по Mi-аккаунту
- Компьютер с установленным софтом (я делал на Windows 10)
- Кабель для подключения телефона к ПК
- Флешка MicroSD

Что делать:

- 1) Необходимо разобрать телефон и получить доступ к разъему батареи.
- 2) Установить на компьютер:
 - а. <u>Драйвера МТК</u>;
 - b. <u>Python</u>, и пакеты к нему:
 - После установки Python, запустить его
 - Активировать командную строку (нажать на клавиатуре «Win+R» и написать «CMD»)
 - Проверить что **Python** активен набрав в командной строке Python (выдаст версию Python), набрать exit() для выхода из **Python**
 - Выполнить в командной строке команды pip install pyusb, pip install pyserial, pip install json5



с. Установить <u>LibUSB</u> и с помощью приложения Filter Wizzard добавить устройство в список разрешаемых действих с устройством через Python

Device Selection	the list of unfiltered devices help	w. If your
device isn't listed, it may already be filt incompatible with the libusb-win32 filter	ered, be in a "driverless" state, o r driver.	r
Hardware ID	Description	21
vid:041e pid:406b rev:8314	Составное USB устройство	12
vid:0e8d pid:0003 rev:0100	MediaTek USB Port	
No.0120 pla. 1000101-0021111-00	осо ондсоустронство	
vid:04d9 pid:a070 rev:0110 mi:02	USB-устройство ввода	
vid:04d9 pid:a070 rev:0110	Составное USB устроиство	
Vid:0409 pid:a070 Pev:0110 mi:01	овечиство введа	~
<		>

d. Запустить SP Flash Tools, указать DA файл и Scatter-файл, перейти на вкладку «Format»

Smart Phone Options	e Flash Too Window	l(Runtime Tr Help	ace Mode)						- 0
			Welcom	e Format		Readback N	lemory Test			
				4	(D				
			D	ownload	S	top				
			Downl	oad-Agent	E: \Xiaomi F	Redmi 9 Bypass Mi Acco	unt and FRP\Xiaomi Redr	mi 9 DA.bin		Choose
			Scatte	r-loading File	E: (Xiaomi F	ledmi 9 Bypass Mi Accou	unt and FRP\MT6768_Ar	ndroid_scatter.txt		✓
			Author	atication File						v 🗖 chaosa
MT	676	58	Autre	nucauon nie						- choose
			Down	oad Only			4	4	1	
				Na	me	Begin Address	End Address	Region	Location	^
				Not suppo	rt flashing	0x00000000000000000	0x000000000046ca3	EMMC_BOOT1_BOOT2	E:\Xiaomi Redmi 9 Bypass N	/li Accou
				recovery		0x00000000008000	0x00000000000000000	EMMC_USER		
		_		vbmeta		0x000000005608000	0x000000000000000000	EMMC_USER		
	·			vbmeta_sy	stem	0x000000005e08000	0x000000000000000000	EMMC_USER		
				vbmeta_ve	ndor	0x000000006608000	0x000000000000000000	EMMC_USER		
				logo		0x00000001df00000	0x000000000000000000	EMMC_USER		
				md1img		0x00000001e700000	0x000000000000000000	EMMC_USER		_
				spmfw		0x000000026700000	0x000000000000000000	EMMC_USER		
				scp1		0x000000026800000	0x000000000000000000	EMMC_USER		_
				scp2		0x000000026e00000	0x000000000000000000	EMMC_USER		
				sspm_1		0x000000027400000	0x000000000000000000	EMMC_USER		
				sspm_2		0x000000027500000	0x000000000000000000000000000000000000	EMMC_USÉR		¥
				0 B/s	01	Bytes EM	MC High Speed	0:00 UAR	T: COM1, 921600	
				,-					,	

е. Прописать адрес Mi-аккаунта/FRP/USER DATA поочередно в памяти телефона

🗧 Smart Phone Flash Tool(Runtime Tr	ace Mode)	_		×
File Options Window Help				
вм	Welcome Format Download Readback Memory Test Validation Validation Validation Validation Validation	Start	Stop	
MTGZGO	 Auto Format Flash Manual Format Flash 	# MiCloud 0x104a2000		
M16768	Specify the region, begin address and length of the format area Region EMMC_USER Begin Address[HEX]: 0x104a2000 Format Length[HEX]: 0x3000000	0x3000000 # Frp		
	WARNING! Calibration data is erased if begin address is 0.	0x5508000 0x100000		
		# Userdata 0x26c800000 0xc0000000		
	0 B/s 0 Bytes EMMC High Speed 0:0	00 UART: COM1, 921600		

Мой канал на YouTube

f. Запустить <u>эксплоит brom.bat</u>, подключить аккумулятор к телефону, зажать на телефоне кнопку «громкость вниз» и подключить телефон к ПК (это EDL режим). Если эксплоит прошел успешно, то должно быть так. Если нет, все проверяем и пробуем еще раз, должно получиться.

	BOOM STORE	
S C:\WINDOWS\system32\cmd.exe	- C	- X
[2021-02-01 01:21:02.571610] Waiting for bootrom		~
[2021-02-01 01:21:12.409006] Found port = COM9		
[2021-02-01 01:21:12:450990] MALADIECH TEMM Device INV LOUE, 07/07		
[2021-02-01 01:21:12:451974] HALABIECH TEAN Device Nw Sub Code: 0x6000		
[2021-02-01 01:12:451974] HALABIECH TEAM Device in version: 0xcado		
[2011-02-01 01:21:12:453954] HALABIECH TEAM Device Swite Ston, 0x0		
[2021-02-01 01:12:12:452051] HALABTECH TEAM sovice serial link authorization: True		
[201] 02-01 01:21:12 452951] HALABTECH TEAM Device download agent authorization: True		
Lease of of other second		
[2021-02-01 01:21:12.453926] Disabling watchdog timer		
[2021-02-01 01:21:12.454905] HALABTECH TEAM Disabling protection		
[2021-02-01 01:21:12.486642] Protection disabled		
Для продолжения нажмите любую клавишу		
3 ¹		
		100
		v

g. Зайти в настройки SP Flash Tool и выбрать СОМ-порт к которому подключен телефон изменить скорость

e Options Windo 💽 Option			×		
General Appearance	Connection	Connection			
Key Language Startup and Shutdown Tracing	Connection Setting	<i></i>	La	Stop	
Download stall/Update	COM port Baud rate	921600			
1 1767	USB speed	Battery with battery			_
	Timeout	wyo battery @ auto detect			

h. Закрываем настройки Flash Tool и на вкладке Format прописав адреса памяти нажимаем кнопку «Start». Проделать с пункта «e» для Mi-аккаунта/FRP/USER DATA.

Все данные об Mi-аккаунте, Google аккаунте и FRP мы с телефона удалили. Теперь отключаем телефон от компьютера, включаем его, **НЕПОДКЛЮЧАЕМ ТЕЛЕФОН К ИНТЕРНЕТ**, делаем первоначальные настройки. Устанавливаем с флешки приложение <u>drony.apk</u>, блокируем с его помощью сервисы Mi «Обновление» и «Поиск телефона». Теперь телефон можно подключить к интернет и не боятся блокировки. Или как пример, можно получить root и удалить Mi-сервисы с телефона.

Видеоверсия этой инструкции на YouTube