

Forum:[Hack Forums](#)

Thread: [Data recovery off of an old unencrypted android phone](#)

Monogram6 - August 13, 2024, 6:39 am

Okay, so i have this old phone that i do not know the pin to (it is only 4 digits), the data there is unencrypted and i would like to access it.

What are the tools, paid or free that could let me access the data or perhaps bruteforce the 4 digit pin through my computer or a raspberry pi (brute force would be preferable).

the phone is a huawei p8 lite (ALE-L21).

Thanks in advance for any help.

shadowcrow - August 13, 2024, 7:06 am

Is USB-debugging on?

Monogram6 - August 13, 2024, 7:08 am

(Aug 13, 2024 07:06 AM)shadowcrow Wrote: [\[CITE\]](#) Is USB-debugging on?
i do not know how do i check it if the phone is locked?

shadowcrow - August 13, 2024, 7:11 am

connect it with a cable to your computer and check if you can get a connection with adb for example (<https://developer.android.com/tools/adb>)

Monogram6 - August 13, 2024, 7:18 am

this is what adb returned:

```
daemon not running; starting now
daemon started successfully
List of devices attached
```

i ran the command 2 times and no devices were showed in my terminal so i am gonna assume debugging is off

but for some reason there my computer registers the phone as a cd rom but it only has 6mb of space and when i click on it there is only the hisuite application.

shadowcrow - August 13, 2024, 7:57 am

This is an emulated discdrive with software from huawei.

With usb debugging of you have to find a vulnerability for the device or the androidversion on it.
You could try flashing twrp as custom recovery but it could lead to a complete factory reset.

Monogram6 - August 13, 2024, 8:12 am

(Aug 13, 2024 07:57 AM)shadowcrow Wrote: [\[CITE\]](#) This is an emulated discdrive with software from huawei.

With usb debugging of you have to find a vulnerability for the device or the androidversion on it.
You could try flashing twrp as custom recovery but it could lead to a complete factory reset.

Yeah man, im not really that advanced i was hoping that there was some way for a program to detect the data or something since its unencrypted or perhaps i could install some kind of bruteforce

tool on my linux computer

DramaKing - August 13, 2024, 10:17 am

(Aug 13, 2024 07:57 AM)shadowcrow Wrote: [\[CITE\]](#) This is an emulated discdrive with software from huawei.

With usb debugging of you have to find a vulnerability for the device or the androidversion on it. You could try flashing twrp as custom recovery but it could lead to a complete factory reset. You have to unlock the bootloader to flash TWRP. You can't unlock the bootloader without unlocking the phone and enabling developer options.

(Aug 13, 2024 08:12 AM)Monogram6 Wrote: [\[CITE\]](#) Yeah man, im not really that advanced i was hoping that there was some way for a program to detect the data or something since its unencrypted or perhaps i could install some kind of bruteforce tool on my linux computer

I would try bruteforcing the PIN. Try 10 common PINs. If it doesn't lock you out, you know that the device is vulnerable (probably is) and can try an automated attack.

I would also try a lockscreen bypass if that doesn't work, name CVE-2022-20465 (details available online). You can also try [software that claims to unlock Android devices](#). I would think that such a tool should work on Marshmallow.

Monogram6 - August 13, 2024, 10:35 am

Thanks, i will definitely try some of the screen unlock tools but from what i have seen none of those tools work without erasing data which is all i care about.

notagh0st - August 13, 2024, 10:46 am

Definitely do what Drama did, type in a bunch of popular pins and see if it locks you out for a period of time, or warns you that it will lock you out. If it doesn't, then you can use brute force tools like: <https://github.com/urbanadventurer/Android-PIN-Bruteforce>

Since it's only 4 digits, there are only 10,000 possible scenarios which is basically nothing in brute force time.

shadowcrow - August 13, 2024, 12:25 pm

(Aug 13, 2024 10:17 AM)DramaKing Wrote: [\[CITE\]](#) You have to unlock the bootloader to flash TWRP. You can't unlock the bootloader without unlocking the phone and enabling developer options.

Not on this old phone

<https://xdaforums.com/t/huawei-p8-lite-install-twrp-recovery-v2-v3-0-0-v3-0-2-full-system-backup.3597170/>

you can start in fastboot mode and flash it via ADB - that should do the trick without factory reset - but NO GUARANTEE for that - it is a risk.

I would definitife try the bruteforce method with nethunter and the HID-Attack first.

DramaKing - August 13, 2024, 12:34 pm

(Aug 13, 2024 12:25 PM)shadowcrow Wrote: [\[CITE\]](#) Not on this old phone

<https://xdaforums.com/t/huawei-p8-lite-install-twrp-recovery-v2-v3-0-0-v3-0-2-full-system-backup.3597170/>

you can start in fastboot mode and flash it via ADB - that should do the trick without factory reset -

but NO GUARANTEE for that - it is a risk.

Ah. All I did was check the process for unlocking the bootloader, rather than seeing if it was strictly needed. Which, come to think of it, even in fastboot, ADB debugging should still need to be enabled. Not 100% sure, but I'm reasonably confident on that one.

(Aug 13, 2024 12:25 PM)shadowcrow Wrote: [\[CITE\]](#) I would definitely try the bruteforce method with nethunter and the HID-Attack first.

OP may not have the option or be willing to take the risk of flashing Nethunter full with HID support on another phone.

(Aug 13, 2024 10:46 AM)notagh0st Wrote: [\[CITE\]](#) Definitely do what Drama did, type in a bunch of popular pins and see if it locks you out for a period of time, or warns you that it will lock you out. If it doesn't, then you can use brute force tools like:

<https://github.com/urbanadventurer/Android-PIN-Bruteforce>

Since it's only 4 digits, there are only 10,000 possible scenarios which is basically nothing in brute force time.

Reasonable assumption, but don't assume.

globalroot - August 13, 2024, 12:38 pm

Data in the phone is NOT plain. If the phone is not Android 3, the data is encrypted. You have to enter the PIN.

You don't have much options available. Except bruteforcing as you say.

shadowcrow - August 13, 2024, 12:50 pm

(Aug 13, 2024 12:38 PM)globalroot Wrote: [\[CITE\]](#) Data in the phone is NOT plain. If the phone is not Android 3, the data is encrypted. You have to enter the PIN.

You don't have much options available. Except bruteforcing as you say.

Are you sure about that?

Ok full-disk-encryption was implemented in 4.4 but I thought it was optional until android 8 or 9 or so (If I remember this right), when they moved from full-disk to file-level-encryption. I flashed many androids these days but this was 6-7 years ago so I don't remember clearly.

@DramaKing: Nethunter can be started without flashing in a busybox but I am not sure if it has HID-support.

globalroot - August 13, 2024, 12:52 pm

(Aug 13, 2024 12:50 PM)shadowcrow Wrote: [\[CITE\]](#) Are you sure about that?

Ok full-disk-encryption was implemented in 4.4 but I thought it was optional until android 8 or 9 or so (If I remember this right), when they moved from full-disk to file-level-encryption. I flashed many androids these days but this was 6-7 years ago so I don't remember clearly.

@DramaKing: Nethunter can be started without flashing in a busybox but I am not sure if it has HID-support.

The encryption type really doesn't matter much. The /data is encrypted. And I don't think he is using some low Android version.

shadowcrow - August 13, 2024, 12:59 pm

I think the stock rom on the p8 light was 5 or 6. But maybe you're right /data has always been good protected.

One thought @Monogram6: There is no sd-card in the device which could hold what you need, hmm?

Monogram6 - August 13, 2024, 1:17 pm

(Aug 13, 2024 12:59 PM)shadowcrow Wrote: [\[CITE\]](#) I think the stock rom on the p8 light was 5 or 6. But maybe you're right /data has always been good protected.

One thought @Monogram6: There is no sd-card in the device which could hold what you need, hmm?

No, i already Took out the sd card from the phone like 2 years ago.

DramaKing - August 13, 2024, 1:19 pm

(Aug 13, 2024 12:50 PM)shadowcrow Wrote: [\[CITE\]](#) @DramaKing: Nethunter can be started without flashing in a busybox but I am not sure if it has HID-support.

I've only ever heard of HID being supported with a custom kernel. Of course, Nethunter Rootless and Nethunter Rooted can simply be installed in Termux, but that doesn't give you HID.

Monogram6 - August 13, 2024, 1:21 pm

(Aug 13, 2024 12:25 PM)shadowcrow Wrote: [\[CITE\]](#) Not on this old phone

<https://xdaforums.com/t/huawei-p8-lite-install-twrp-recovery-v2-v3-0-0-v3-0-2-full-system-backup.3597170/>

you can start in fastboot mode and flash it via ADB - that should do the trick without factory reset - but NO GUARANTEE for that - it is a risk.

I would definitife try the bruteforce method with nethunter and the HID-Attack first.

Wait, so correct me if i am wrong but according to this article i can flash twrp on my phone,without knowing my pin AND without data loss, and basically make a full backup of it including photos? because if so then this is the solution

DramaKing - August 13, 2024, 2:00 pm

(Aug 13, 2024 01:21 PM)Monogram6 Wrote: [\[CITE\]](#) Wait, so correct me if i am wrong but according to this article i can flash twrp on my phone,without knowing my pin AND without data loss, and basically make a full backup of it including photos? because if so then this is the solution [shadowcrow](#) is clearly saying that you can flash TWRP to the phone with the real possibility of data loss. I'm saying that USB debugging needs to be enabled, or, as you saw before, ADB will show no devices connected. Even on that old of a phone. It wouldn't be that easy. It would, however, be easy to confirm. No harm in trying.

shadowcrow - August 14, 2024, 7:15 am

@MonoGram6 Did anything from above work?

Monogram6 - August 15, 2024, 2:51 am

(Aug 14, 2024 07:15 AM)shadowcrow Wrote: [\[CITE\]](#) @MonoGram6 Did anything from above work? Thanks for asking mate, i am considering trying the nethunter method since i have some spare phones but i am gonna need to order the usb otg cable because i do not have that.

I am also considering trying the exploit with the sim card (CVE-2022-20465).

But these are my 2 only options since i do not want to flash twrp because of the data loss probability.

I would appreciate if there are any other methods i could add to my toolbox in case these 2 are not going to work.

