

Forum:[Hack Forums](#)

Thread: [Carrier Unlock S24 Ultra \(TMB\)](#)

xchrisxxxx - October 5, 2024, 10:48 pm

Hey all, long time lurker here. Have always loved these forums they have provided much insight. Recently I bought an S24 Ultra 256gb (TMB) from FB market. The listing said it was "paid off" and unlocked..... Well to no surprise it isnt. its fully carrier locked to tmb and i use google fi. So after being scammed twice, once buying the phone and once using one of those "unlocking" services. I have run out of all options.

The previous owner blocked me in all ways so i cannot communicate with them.

I have tried all methods my brain could fathom, digging deep into the hidden menus and flashing different CSC firmwares to no avail.

If anyone has any solution to truely carrier unlock a S24 Ultra you'd be my savior.

Bastille - October 5, 2024, 11:19 pm

Hey, welcome to HF

I know that [WarpBrothers](#) has a thread regarding removing Android FRP, he maybe has few tips for us regarding your carrier locked phone

<https://hackforums.net/showthread.php?tid=6271825>

I'm interested in this as well and curious if it's possible. I asked ChatGPT, and it mentioned two potential methods:

Contacting the mobile carrier: However, if you're not the original owner or if the phone hasn't been fully paid off, they're unlikely to unlock it.

Using a third-party unlocking service: These services may be able to unlock it, but they might need authorization from the mobile carrier.

Technical Explanation

From a technical perspective, it seems that the IMEI is registered with the mobile carrier in a database. When you try to use a SIM card, the network checks this database to verify if the phone is allowed to use the network associated with that SIM card. To unlock the phone, changes would need to be made in this database, which only the mobile carrier (or a subcontractor authorized by them) can do.

The locking mechanism also works at another level within the phone's firmware, specifically in the baseband, which contains instructions regarding which mobile carriers the phone can connect to. This information is stored on an EEPROM chip in the phone, and the chip compares the MCC (Mobile Country Code) and MNC (Mobile Network Code) allowed for use.

IMEI Blacklist Check

It's also important to check if the IMEI is blacklisted. There are online tools that can help with this. Here are some I found, though I'm not sure how reliable they are:

<https://www.imeipro.info/>

https://imei24.com/blacklist_check/

<https://www.checkmend.com/eu/>

Flashing the Baseband

It appears that the lock might be bypassed by flashing the EEPROM where the baseband is configured, but there is a risk of bricking the phone in the process. ChatGPT also mentioned that some third-party services modify the EFS partition to remove the restriction, but I don't have the technical details on how to do this. A quick search on YouTube shows a few videos, and some of them mention tools like "TFM Tool."

xchrisxxxx - October 5, 2024, 11:47 pm

I would love if chatgpt could point me in the direction of these third party services as i would love to not brick my phone trying myself... :)

Bastille - October 6, 2024, 12:52 am

(Oct 5, 2024 11:47 PM)xchrisxxxx Wrote: [\[CITE\]](#) I would love if chatgpt could point me in the direction of these third party services as i would love to not brick my phone trying myself... :)

You can ask here : <https://chatgpt.com/> it also depends on your current location I guess

WarpBrothers - October 6, 2024, 1:55 am

Thanks Bastille,

Can you please provide me with the IMEI number? I'm happy to look into this for you. Please private message, don't paste the IMEI onto this thread. Thanks

xchrisxxxx - October 6, 2024, 12:43 pm

(Oct 6, 2024 01:55 AM)WarpBrothers Wrote: [\[CITE\]](#) Thanks Bastille,

Can you please provide me with the IMEI number? I'm happy to look into this for you. Please private message, don't paste the IMEI onto this thread. Thanks

unfortunately i cannot pm you without paying for an upgraded account. ive checked my imei, the phone isnt blacklisted. but i have spoke with tmb and they said the previous owner still has a large balance on the phone.

(Oct 6, 2024 01:55 AM)WarpBrothers Wrote: [\[CITE\]](#) Thanks Bastille,

Can you please provide me with the IMEI number? I'm happy to look into this for you. Please private message, don't paste the IMEI onto this thread. Thanks

ive even changed the csc to XAA, its on XAA firmware also, in the service menus ive run across "sim lock blob" but when i click on it it says " service NOT supported. also in the china settings there is another area for sim lock, the only thing i havent tried yet is flashing china software to try and access the china settings in fear that it will make my whole phone in chinese haha. ive studied methods for baseband flashing and i cannot find any methods online. the software previously mentioned also does not support the s24 ultra. any insight would be great. I love learning new things.

WarpBrothers - October 7, 2024, 3:45 am

(Oct 6, 2024 12:43 PM)xchrisxxxx Wrote: [\[CITE\]](#) unfortunately i cannot pm you without paying for an upgraded account. ive checked my imei, the phone isnt blacklisted. but i have spoke with tmb and

they said the previous owner still has a large balance on the phone.

ive even changed the csc to XAA, its on XAA firmware also, in the service menus ive run across "sim lock blob" but when i click on it it says " service NOT supported. also in the china settings there is another area for sim lock, the only thing i havent tried yet is flashing china software to try and access the china settings in fear that it will make my whole phone in chinese haha. ive studied methods for baseband flashing and i cannot find any methods online. the software previously mentioned also does not support the s24 ultra. any insight would be great. I love learning new things.

Thanks for the info, flashing the device will not gain unlock. I need the IMEI number, I might be able to use server to remove but might cost.

xchrisxxxx - October 9, 2024, 11:56 pm

(Oct 7, 2024 03:45 AM)WarpBrothers Wrote: [\[CITE\]](#) Thanks for the info, flashing the device will not gain unlock. I need the IMEI number, I might be able to use server to remove but might cost.

I much rather learn. Could I pay you to teach me how to do it?

Bastille - October 9, 2024, 11:58 pm

[xchrisxxxx](#) [WarpBrothers](#) Take care guys :

Out of Marketplace

All marketplace-style threads or posts such as buying, selling, trading, offering a paid service, appraising, and auctioning belong to the Marketplace. Users failing to comply will earn a A seven-day posting ban and a warning is the penalty for posting marketplace threads outside of the Market tab. This includes threads with "optional payments" or "not free" remarks.

xchrisxxxx - October 10, 2024, 7:38 pm

(Oct 9, 2024 11:58 PM)Bastille Wrote: [\[CITE\]](#) [xchrisxxxx](#) [WarpBrothers](#) Take care guys :

Out of Marketplace

All marketplace-style threads or posts such as buying, selling, trading, offering a paid service, appraising, and auctioning belong to the Marketplace. Users failing to comply will earn a A seven-day posting ban and a warning is the penalty for posting marketplace threads outside of the Market tab. This includes threads with "optional payments" or "not free" remarks.

understood, i really dont want to pay for anything. im asking the community here for help in the matter. if anyone has a method, id like to learn. ChatGPT has been no help at all. im not sure if you were referring to ChatGPT to be funny or for legal reasons lol but it is no help to me. Is unlocking a phone really that hard of a thing to do that no one actually knows how to? seems funny because there are alot more complex things people figure out then a method of flashing a baseband or changing parameters of a cellphone to allow the phone to accept a new sim/esim. The phone isnt blacklisted so its only a firmware related issue. The firmware saying the phone is locked.

Kaleb - October 10, 2024, 7:51 pm

I don't think carrier locks are easy to bypass, pretty sure its a fairly solid thing. Are you sure you didn't just steal this phone btw? Seems much more likely to me. I'm known as the computer guy amongst my friends and have had more than one person bring obviously stolen phones to me asking me to unlock them, no thank you.

xchrisxxxx - October 15, 2024, 1:14 am

(Oct 10, 2024 07:51 PM)Kaleb Wrote: [\[CITE\]](#) I don't think carrier locks are easy to bypass, pretty sure its a fairly solid thing. Are you sure you didn't just steal this phone btw? Seems much more likely to me. I'm known as the computer guy amongst my friends and have had more than one person bring

obviously stolen phones to me asking me to unlock them, no thank you.

Lol no I did not steal the phone I bought it off Facebook marketplace supposedly being unlocked. The phone itself has no lock on it other than my own passcode and Samsung account.

I get that the simlocks are solid, but what gets me is that there use to be methods in the "hidden" service menus to unlock the phone.

Said menus now say either "not support" or "menu doesn't exist" but there are still clearly simlock options in these menus and it begs the question , is there a way to access these menus, or simply flash the baseband to remove that portion of the firmware that blocks the simcard / esim. I've had a few people on other forums tell me they have methods but want payment. Which I'm not here to discuss paying for it. I'd like to learn and understand how it's done.

samsungseeker - October 15, 2024, 8:41 am

have you ever heard of samsung lock @wrap brothers some say its impossible to bypass this is it true?

xchrisxxxx - October 16, 2024, 1:13 pm

(Oct 15, 2024 08:41 AM)samsungseeker Wrote: [\[CITE\]](#) have you ever heard of samsung lock @wrap brothers some say its impossible to bypass this is it true?It's definitely not impossible. The only thing that would make it impossible is if you were black listed. At the end of the day it is a software based lock, there are multiple ways I can fathom a bypass, but I do not have the knowledge on how to change certain parameters or flash the baseband.

Logically though, since the baseband is updated via software updates than it can be bypassed. Those who know are just keeping the secret so they can profit from it. I'll continue my tinkering and when I do eventually find a working method I'll make sure to post it publicly for everyone.

samsungseeker - October 17, 2024, 4:24 am

(Oct 16, 2024 01:13 PM)xchrisxxxx Wrote: [\[CITE\]](#) It's definitely not impossible. The only thing that would make it impossible is if you were black listed. At the end of the day it is a software based lock, there are multiple ways I can fathom a bypass, but I do not have the knowledge on how to change certain parameters or flash the baseband.

Logically though, since the baseband is updated via software updates than it can be bypassed. Those who know are just keeping the secret so they can profit from it. I'll continue my tinkering and when I do eventually find a working method I'll make sure to post it publicly for everyone.

i would be willing to pay if anyone has a way aorund it

WarpBrothers - October 18, 2024, 6:00 am

(Oct 17, 2024 04:24 AM)samsungseeker Wrote: [\[CITE\]](#) i would be willing to pay if anyone has a way aorund it

When you say Samsung lock do you mean FRP or KG lock?

(Oct 15, 2024 01:14 AM)xchrisxxxx Wrote: [\[CITE\]](#) Lol no I did not steal the phone I bought it off Facebook marketplace supposedly being unlocked. The phone itself has no lock on it other than my own passcode and Samsung account.

I get that the simlocks are solid, but what gets me is that there use to be methods in the "hidden" service menus to unlock the phone.

Said menus now say either "not support" or "menu doesn't exist" but there are still clearly simlock options in these menus and it begs the question , is there a way to access these menus, or simply flash the baseband to remove that portion of the firmware that blocks the simcard / esim. I've had a few people on other forums tell me they have methods but want payment. Which I'm not here to discuss paying for it. I'd like to learn and understand how it's done.

Like Kaleb said, carrier locks are not easy and cannot be unlocked by flashing software or "hidden menus". The phone isn't a Nokia 3310 haha. Like I said, from my professional advise, only Server will remove the carrier lock. Again, be a paid service.

On another thought, even if you do get it unlocked it's a high risk of getting blacklisted with the previous owner owing money already.

P1N7 - October 19, 2024, 6:36 pm

Sorry you got scammed, it is basically a money pit to pay any supposed unlock provider found on google. Before you offer your credit card information be weary that some places charge for the initial consultation and then hundreds of more dollars to actually unlock the device.

xchrisxxxx - October 22, 2024, 12:53 am

(Oct 18, 2024 06:00 AM)WarpBrothers Wrote: [\[CITE\]](#) When you say Samsung lock do you mean FRP or KG lock?

Like Kaleb said, carrier locks are not easy and cannot be unlocked by flashing software or "hidden menus". The phone isn't a Nokia 3310 haha. Like I said, from my professional advise, only Server will remove the carrier lock. Again, be a paid service.

On another thought, even if you do get it unlocked it's a high risk of getting blacklisted with the previous owner owing money already.

I'm just bewildered that I've been offered a service, they have a method, but keep it to themselves for market control. I have no intentions on market, just want to learn the method(s) that exist and share it with everyone. Yes it runs a huge risk of being blacklisted, but if it's not blacklisted it should still be usable. It shocks me no one has a method here. I guess this is the end of my journey with trying to learn. This next thing I will say is souky for educational purposes. But one could change the S/N and or IMEI and completely bypass this. For educational purposes I'd like to learn how to do that. ?

WarpBrothers - October 22, 2024, 1:31 pm

(Oct 22, 2024 12:53 AM)xchrisxxxx Wrote: [\[CITE\]](#) I'm just bewildered that I've been offered a service, they have a method, but keep it to themselves for market control. I have no intentions on market, just want to learn the method(s) that exist and share it with everyone. Yes it runs a huge risk of being blacklisted, but if it's not blacklisted it should still be usable. It shocks me no one has a method here. I guess this is the end of my journey with trying to learn. This next thing I will say is souky for educational purposes. But one could change the S/N and or IMEI and completely bypass this. For educational purposes I'd like to learn how to do that. ?

Without sounding rude, you need to learn not everything is free in life. Yes your on a hack forum but unfortunately these things are not free. Speaking from someone who removes/bypasses FRP and icloud accounts, even for me it isn't free. Depending on the locked state of an device sometimes the king (server) needs to be paid to remove or bypass locks and carrier locks especially with your situation. Anyway, I've offered a paid service which would probably unlock with 24hrs but you keep going for free handout. I wish you all the best!

Warpbrothers ?

Syndicate - October 23, 2024, 10:09 am

(Oct 22, 2024 12:53 AM)xchrisxxxx Wrote: [\[CITE\]](#) I'm just bewildered that I've been offered a service, they have a method, but keep it to themselves for market control. I have no intentions on market, just want to learn the method(s) that exist and share it with everyone. Yes it runs a huge risk of being blacklisted, but if it's not blacklisted it should still be usable. It shocks me no one has a method here. I guess this is the end of my journey with trying to learn. This next thing I will say is souky for educational purposes. But one could change the S/N and or IMEI and completely bypass this. For educational purposes I'd like to learn how to do that. ?

Why is this bewildering to you exactly? It's a profession. You pay for professional service. If you can't figure out how to do it yourself then you pay someone to do it for you. When your car breaks down, do you ask the mechanic to do it for free or ask him to teach you how to fix it yourself for free? No.

xchrisxxxx - October 24, 2024, 1:12 am

(Oct 23, 2024 10:09 AM)Syndicate Wrote: [\[CITE\]](#) Why is this bewildering to you exactly? It's a profession. You pay for professional service. If you can't figure out how to do it yourself then you pay someone to do it for you. When your car breaks down, do you ask the mechanic to do it for free or ask him to teach you how to fix it yourself for free? No.

My car breaks down, I join a forum and ask the community for guidance, or consult youtube and I buy the tools to do the work myself. It seems like certain communities are just stingier than others with their capacity to teach or be helpful in any manner.

Syndicate - October 24, 2024, 9:56 am

(Oct 24, 2024 01:12 AM)xchrisxxxx Wrote: [\[CITE\]](#) My car breaks down, I join a forum and ask the community for guidance, or consult youtube and I buy the tools to do the work myself. It seems like certain communities are just stingier than others with their capacity to teach or be helpful in any manner.

If I had a niche method and I was the only one on this forum able to do it, you're absolutely right that I would sell it. Why teach someone like you? I'm assuming once his method is caught on then it will be patched as well. I wouldn't be teaching anyone.

xchrisxxxx - October 28, 2024, 8:02 pm

(Oct 24, 2024 09:56 AM)Syndicate Wrote: [\[CITE\]](#) If I had a niche method and I was the only one on this forum able to do it, you're absolutely right that I would sell it. Why teach someone like you? I'm assuming once his method is caught on then it will be patched as well. I wouldn't be teaching anyone.

Knowledge should be shared. The lazy or incapable are the ones who pay or screw up said activity trying to do it themselves. I have actually figured out a "niche" method to do it and have my phone fully working now with google fi. with much thanks to an earlier comment on flashing the baseband. And my method is free to anyone who wants to know it. just PM me, note : phone cannot be black listed. method will not bypass a blacklisted phone. :) thanks for the negative rep btw syndicate <3 much love.

Syndicate - October 28, 2024, 8:27 pm

(Oct 28, 2024 08:02 PM)xchrisxxxx Wrote: [\[CITE\]](#) Knowledge should be shared. The lazy or incapable are the ones who pay or screw up said activity trying to do it themselves. I have actually figured out a "niche" method to do it and have my phone fully working now with google fi. with much thanks to an earlier comment on flashing the baseband. And my method is free to anyone who wants to know it. just PM me, note : phone cannot be black listed. method will not bypass a blacklisted phone. :) thanks for the negative rep btw syndicate <3 much love.

Great job! Now you can sell that method and make some money ?

Terry Thompson - March 21, 2025, 2:00 am

From what your describing to me sounds like mdm lock ,sometimes called a financial lock. Some company's like us cellular put them on their post-paid phones in case someone does not pay off there phone. And some company's use mdm when they supply a phone to their employees so if they quit and don't turn phone in they can't use it. With a standard Sim lock or imei lock for a specific carrier all u need is a network unlock code .. or imei unlock. Mdm is a bitch to remove. But it can be done via a 3rd party that has access to the server or done via a qt code you can buy .. but those ways you have to deal with people outside united states and it's hard to find someone that won't take your \$. The network it is locked to can do it remotely and a unlocking company in the

United States can do it but you would have to send them the phone. There are reputable companies in us..message me if u need more info.