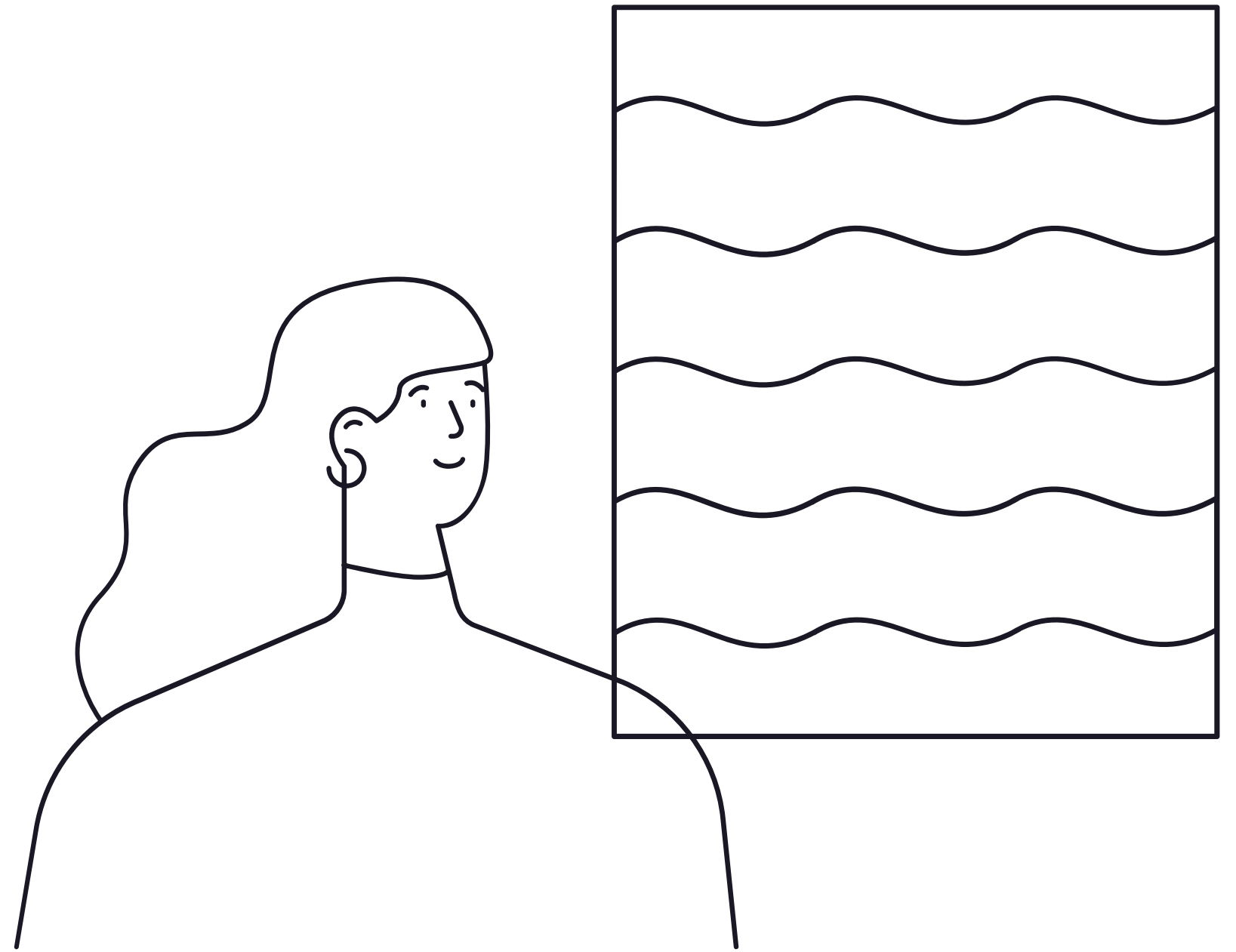


Automating your Whatsapp Chats

Aditi Bhatnagar



*Disclaimer: Contents of the talk not representative of my employer, for educational purposes only.

Hi everyone!

I'm Aditi Bhatnagar

- Researcher interested security, privacy & everything in between
- Geeking out at !Infinite Hacks (www.aditi.fyi)
- Currently working as Security Engineer at Atlassian, previously with Microsoft

  @4ditiBhatnagar  aditi.fyi



WAIT, BUT WHY?



FRIENDS, QUIRKS AND RACE

TL;DR It was just an innocent competition folks

Check your phone.

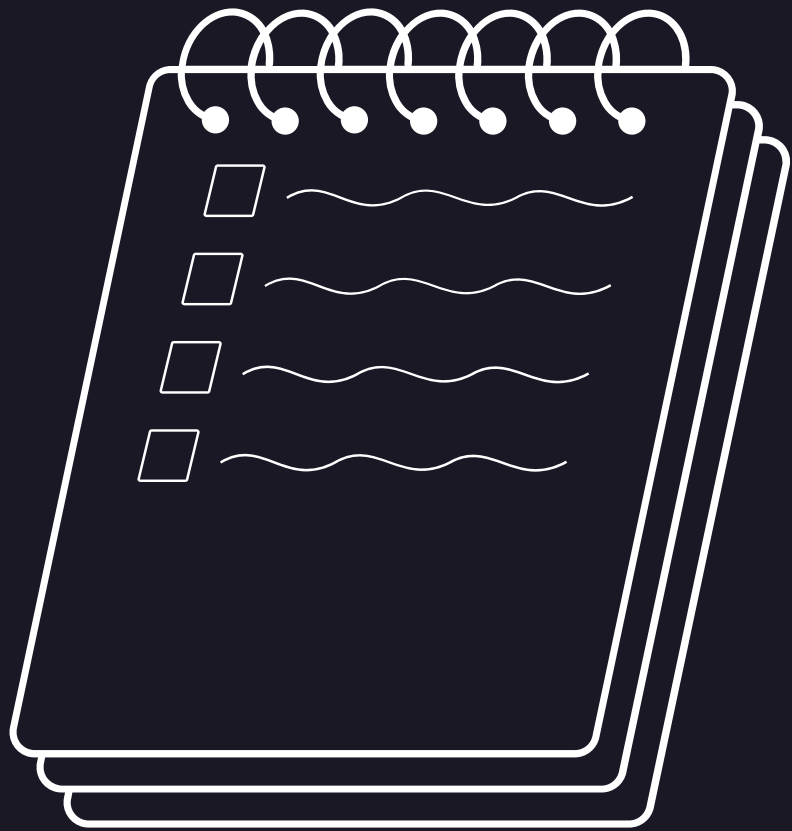
10:40 PM 

HOW CAN I POSSIBLY DO IT?

- WEB.WHATSAPP?
- ANDROID?
- SOMETHING ELSE?

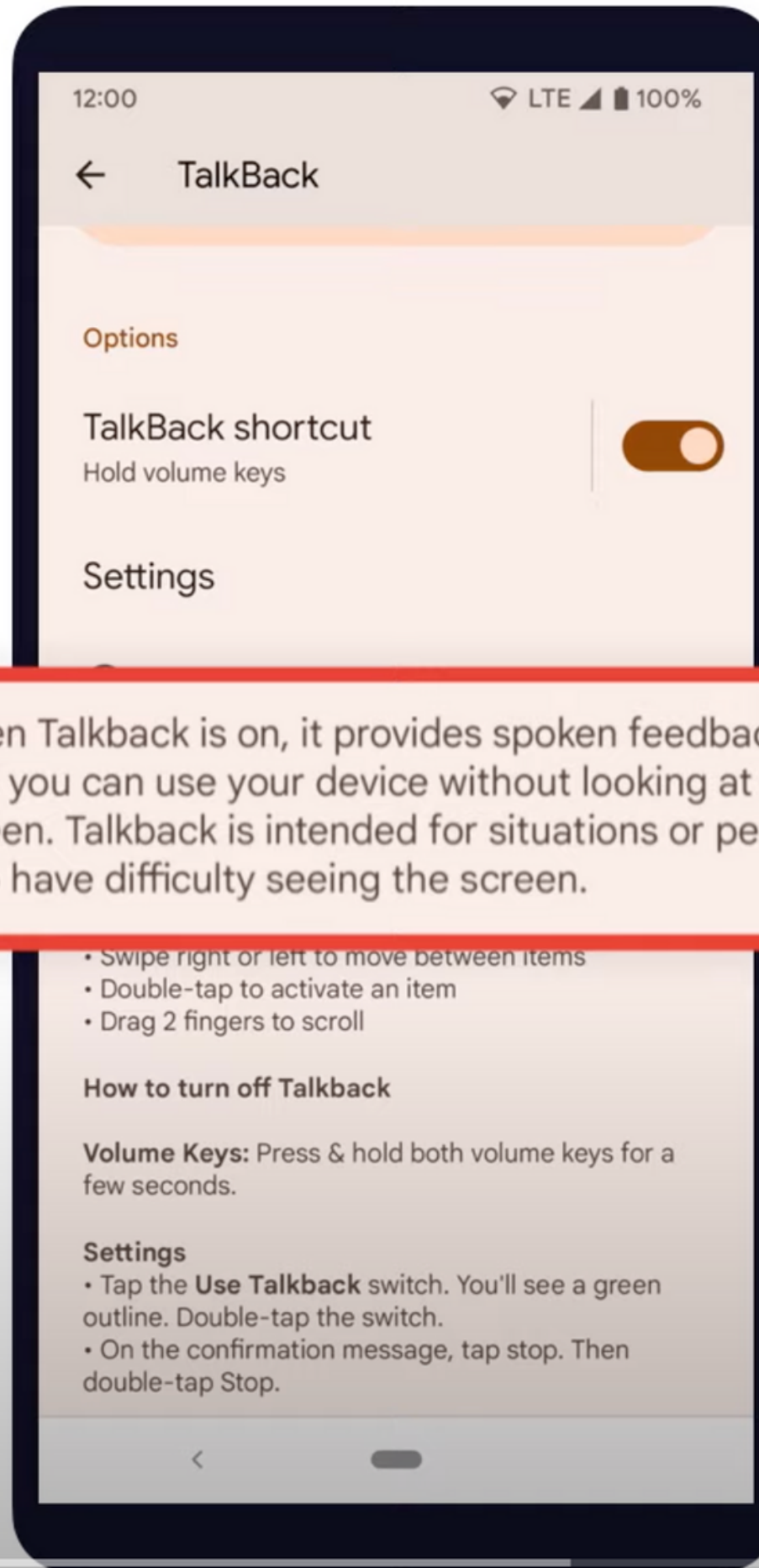


WHAT KIND OF POWERS
DO I NEED FROM THE
PLATFORM TO PERFORM
THIS



ABILITY TO

1. "READ"
2. "TYPE"
3. "PRESS BUTTON"



When Talkback is on, it provides spoken feedback so that you can use your device without looking at the screen. Talkback is intended for situations or people who have difficulty seeing the screen.

- Swipe right or left to move between items
- Double-tap to activate an item
- Drag 2 fingers to scroll

How to turn off Talkback

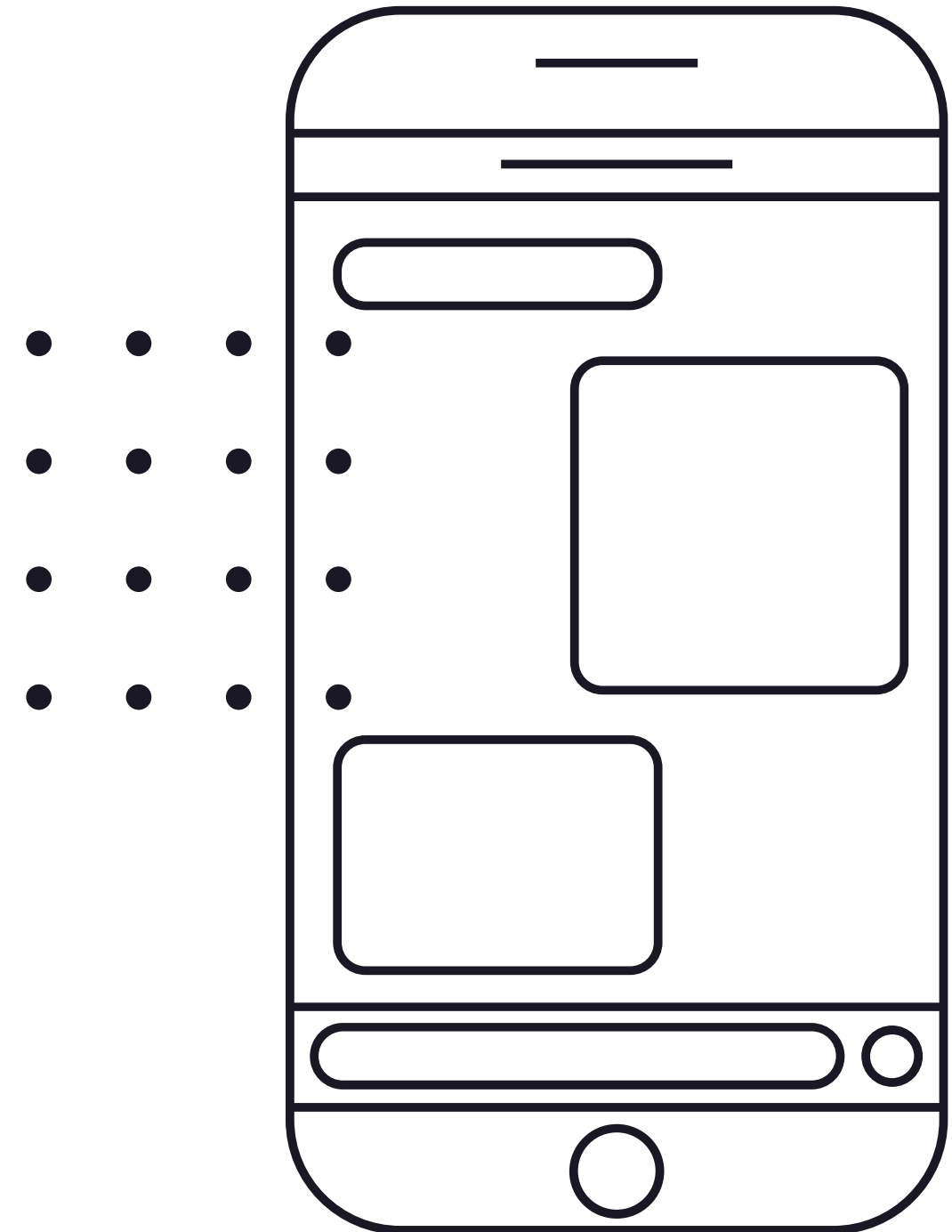
Volume Keys: Press & hold both volume keys for a few seconds.

Settings

- Tap the **Use Talkback** switch. You'll see a green outline. Double-tap the switch.
- On the confirmation message, tap stop. Then double-tap Stop.

ACCESSIBILITY SERVICE IN ANDROID

An Accessibility Service assists users with disabilities in using Android devices and apps. It is a long-running privileged service that helps users process information on the screen and lets them to interact meaningfully with a device.



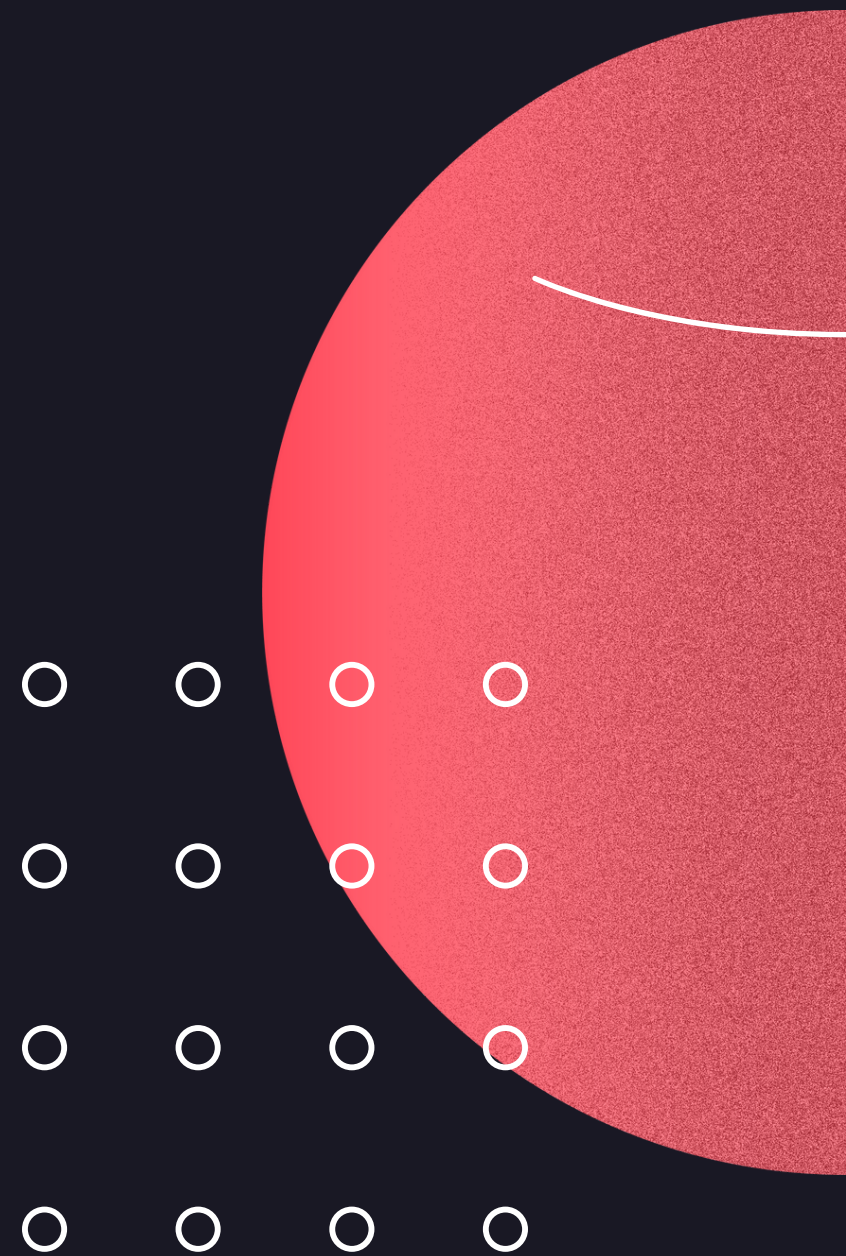
SO READING IS POSSIBLE, HOW ABOUT TAKING ACTIONS?

developers 

Create your own accessibility service

 Android Developers

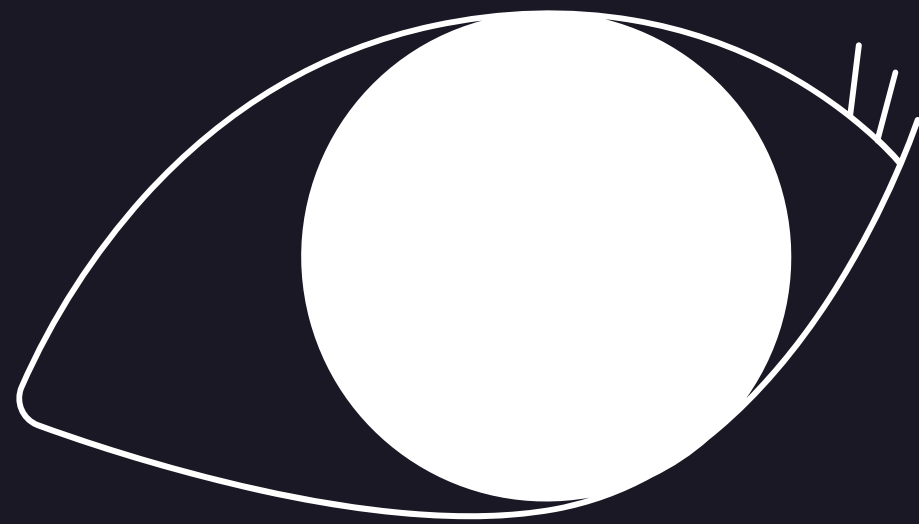
Building with Accessibility Service



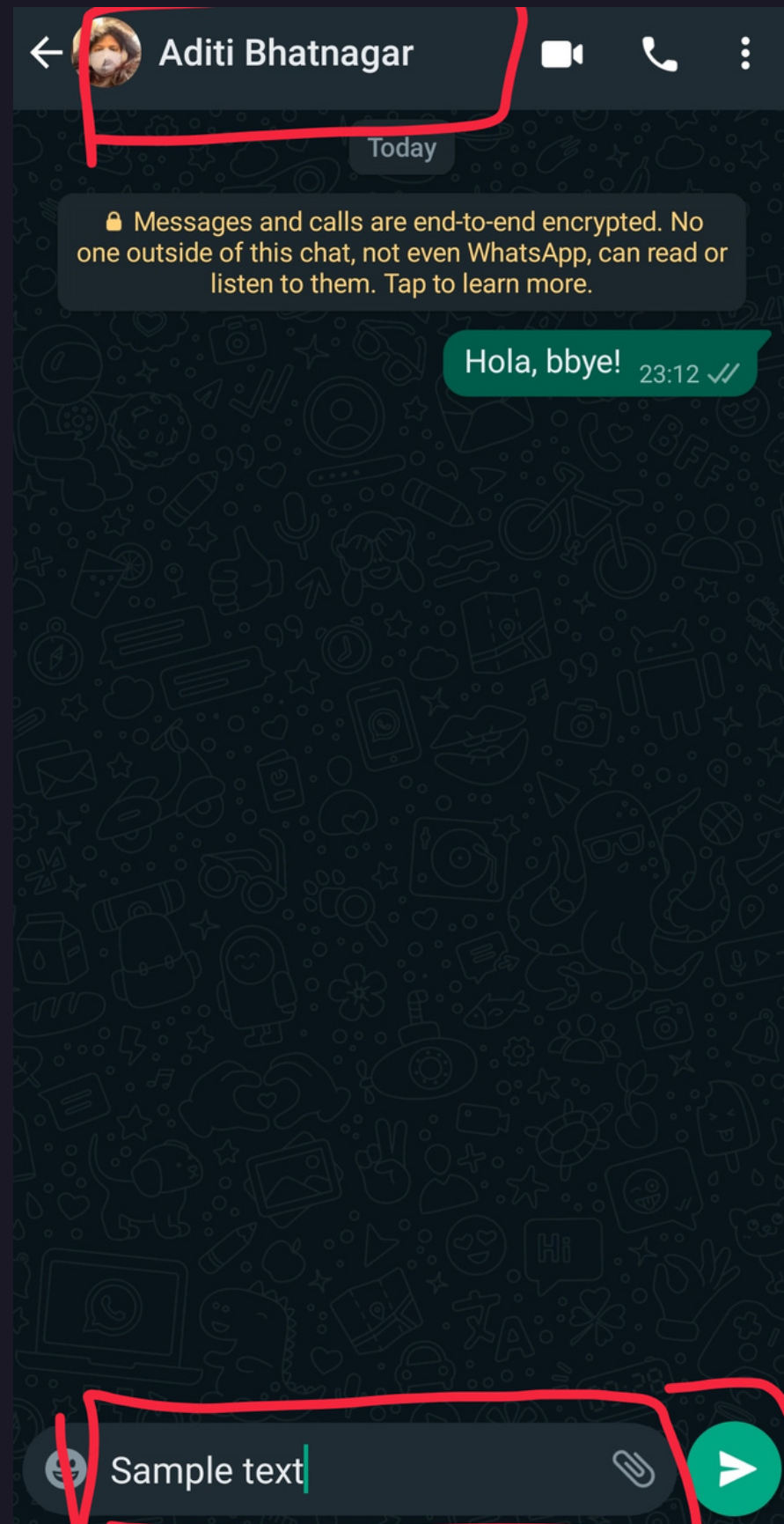
1. DEFINE ACCESSIBILITY SERVICE

2. DECLARE IT IN APP MANIFEST FILE

3. DEFINE ACCESSIBILITY CONFIG FILE **



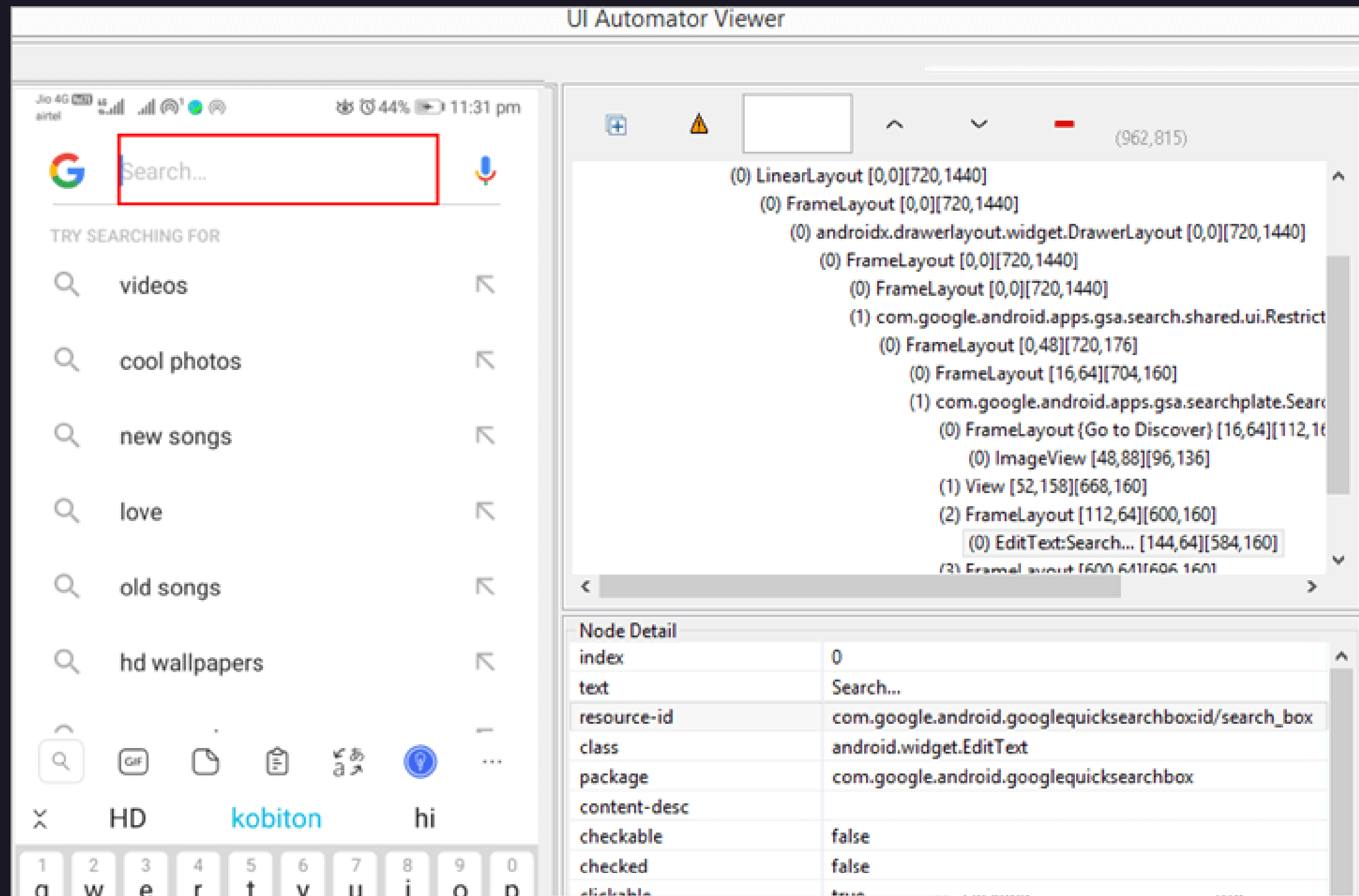
LET'S LOOK AT THE CODE



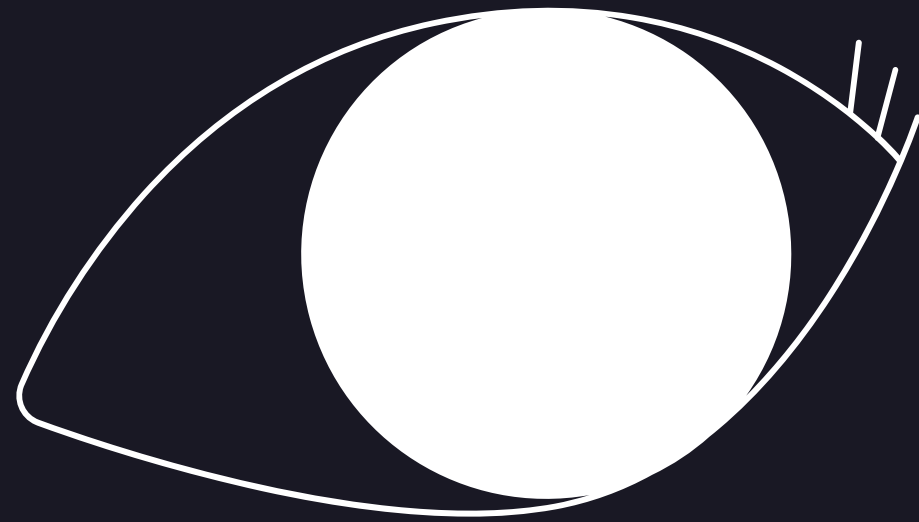
Logic

1. Whenever WhatsApp chat opens, read the name of the person
2. If that's the target, get the textbox and enter predefined message in there
3. Get the reference to send button and click it

UI Automator Viewer



~/Library/Android/sdk/tools/bin



**LET'S BUILD & TEST IT
DOES IT WORK?**

Hey bro 03:10 ✓

Hope you liked it ❤️ 03:10 ✓

Happy belated bday 03:10 ✓

I've had a long day at work 03:10 ✓

Will ttys 03:11 ✓

6 NOVEMBER 2020



27 NOVEMBER 2020

Calling you tonight 15:38 ✓

TODAY

Hey, ssup? 02:30

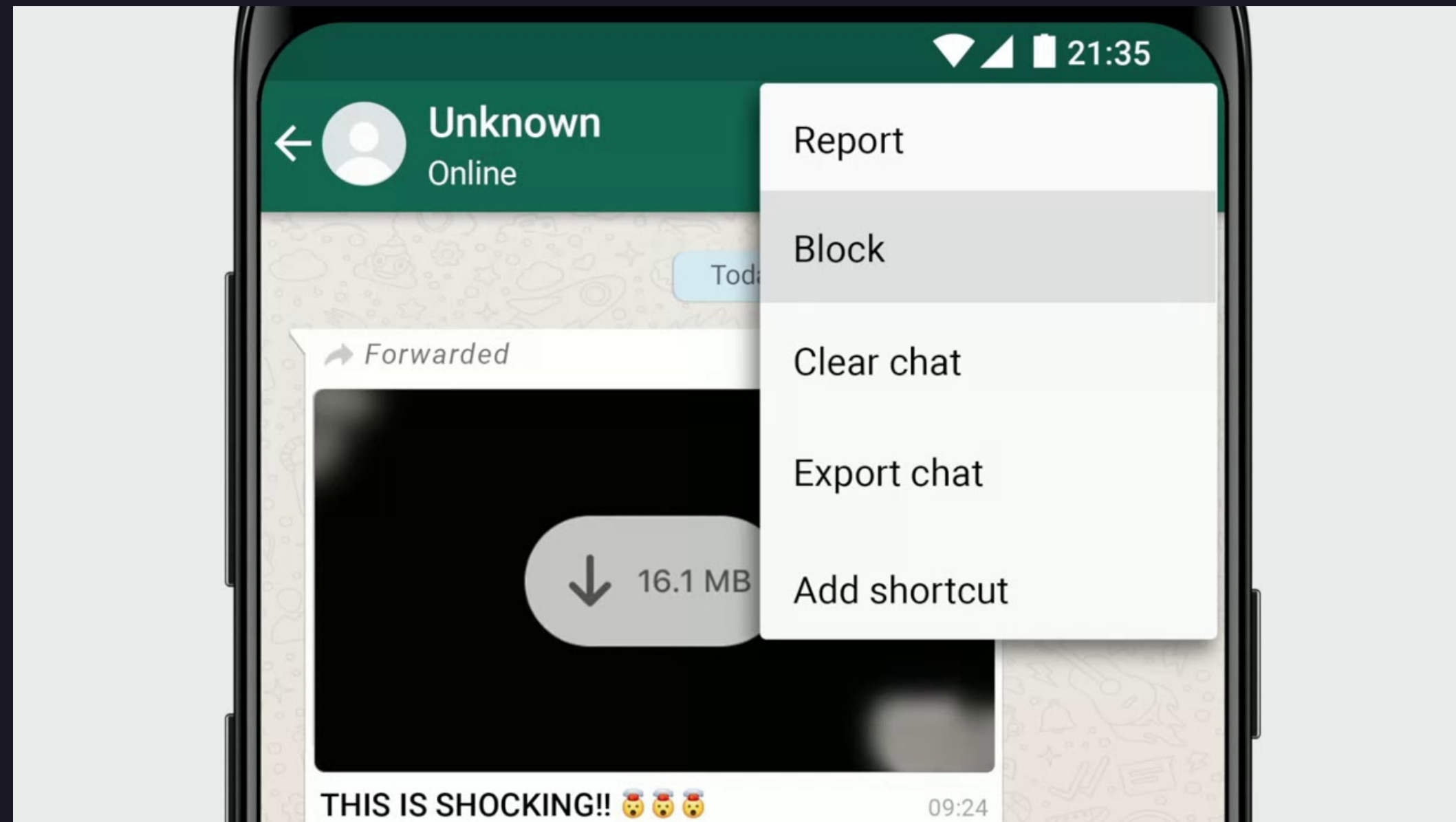
IT WORKED!

**INFACT, YOU CAN USE THIS
AUTOMATE LITERALLY ANYTHING
ON ANDROID**

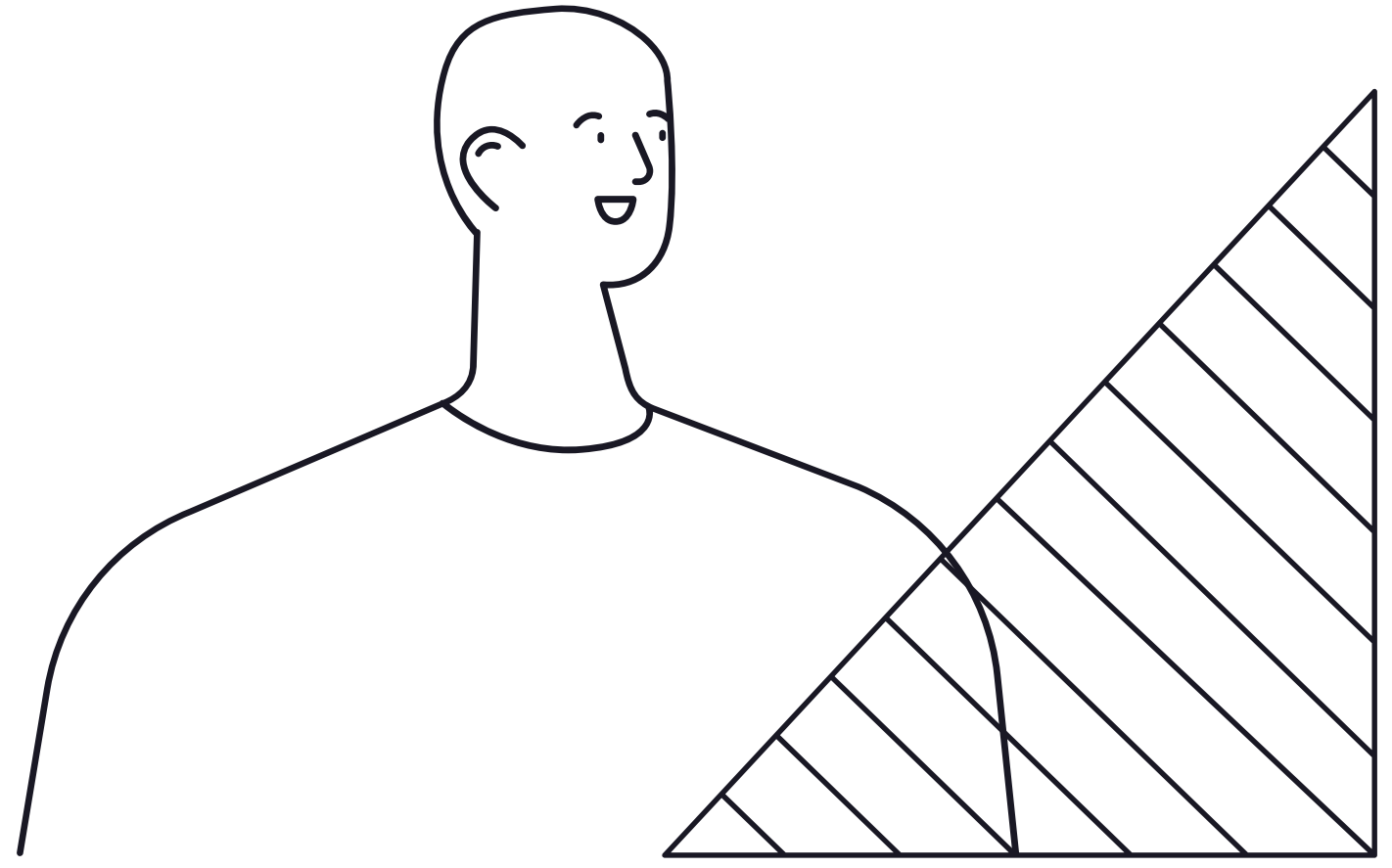
How I felt



How my friends reacted



TECHNICAL SUCCESS != HUMAN SUCCESS



**HOW IS IT RELEVANT?
(OTHER THAN BRINGING JOY)**

MOST MALICIOUS MALWARES USE ACCESSIBILITY SERVICES

**FLUBOT, SharkBot, Xenomorph, BianLian, S.O.V.A,
PixStealer, Vultur, TeaBot, Ginp, banking trojans**

**It's an excellent way to
Break Sandboxing
Go undetected
Build a spyware
Commit financial fraud**

...

Playing is the best way to learn

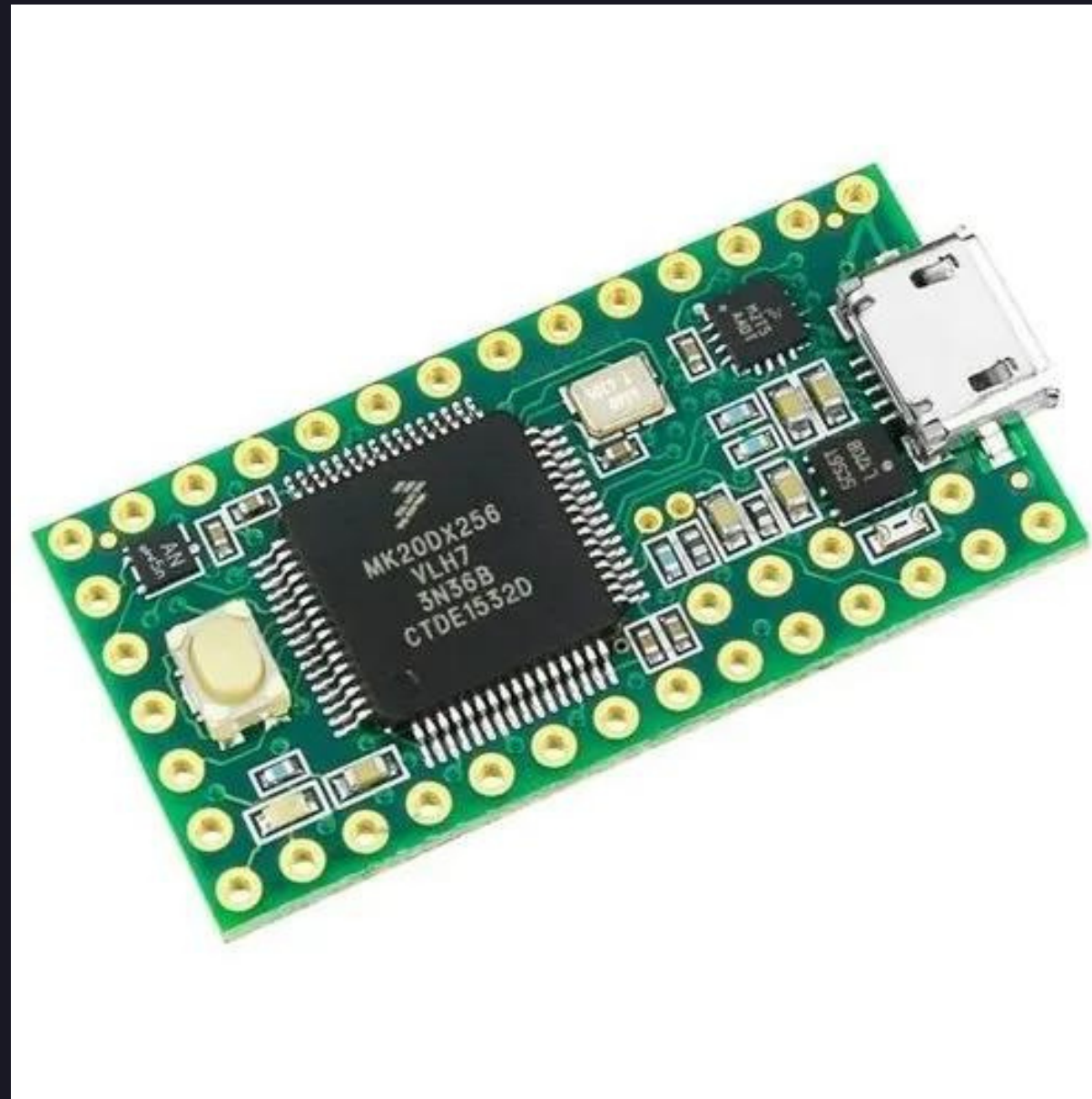
Once you know how it works you may get more
ideas on how to defend against it

So, stay safe & turn accessibility off



Back to automation

#bonus_slide



#bonus Get your free test app!



<https://www.aditi.fyi/whatsapp-hack>

Thank you!

Queries, consultation, chat?
Reach out to me at

✉ aditi.bhatnagar.mailbox@gmail.com

🐦 [@4ditiBhatnagar](https://twitter.com/@4ditiBhatnagar)

🌐 [@4ditiBhatnagar](https://www.linkedin.com/company/@4ditiBhatnagar)

🌐 aditi.fyi

