Vulnerability Scanning & Cracking Tools

For this hands-on-exercise you will work as a group of 2-3 students with the objective of using a few utilities / tools built into Kali Linux to gain access to vulnerable Wi-Fi networks.

USE THESE TOOLS IN A RESPONSIBLE MANNER ON TEST NETWORKS / SYSTEMS FOR EDUCATIONAL PURPOSES ONLY!

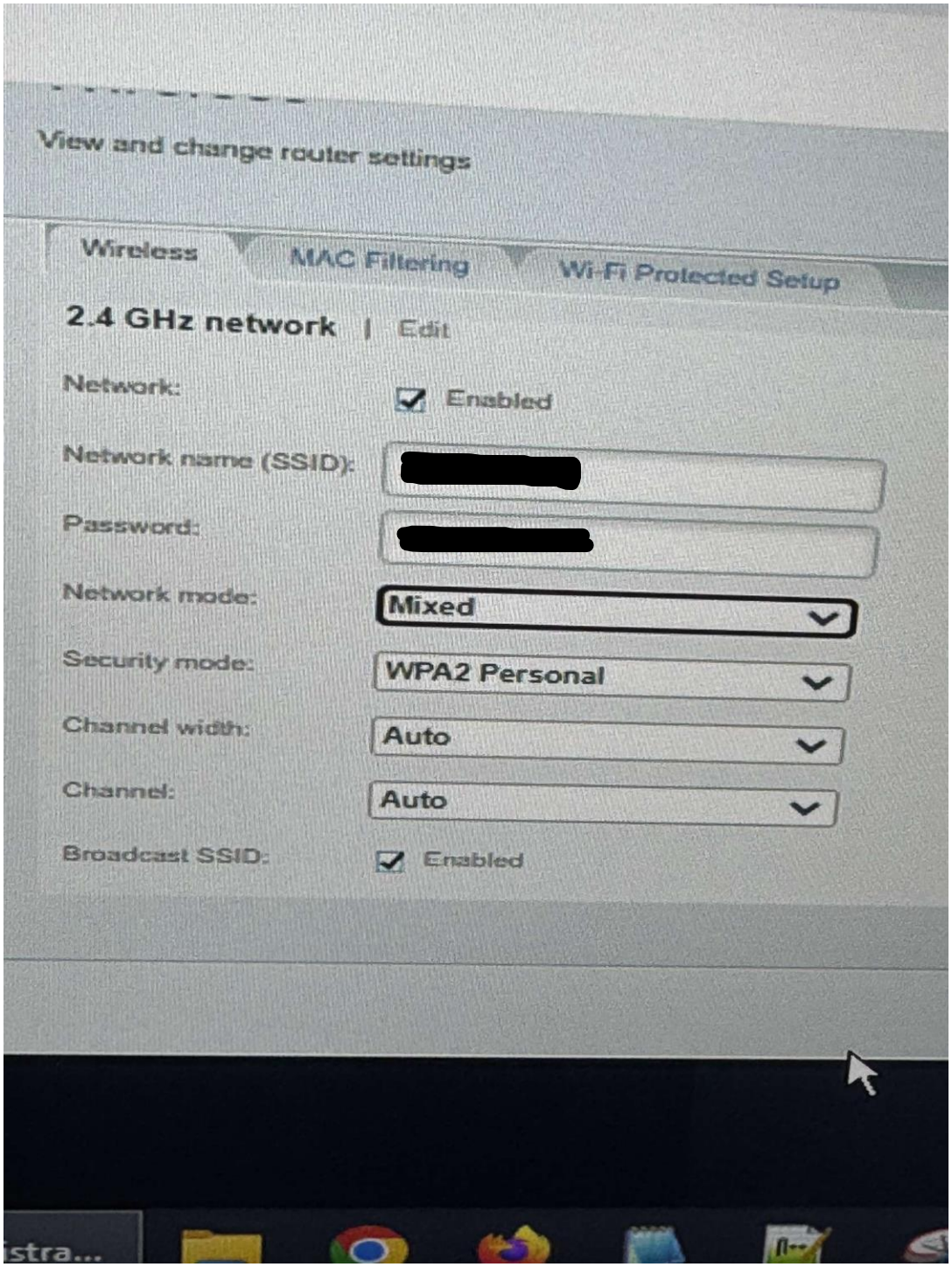
CONFIGURE Wireless Router / Access Point (15points)

Provide Screenshots / Images of Each Step

Hint: You may need to reset the router / AP back to factory defaults

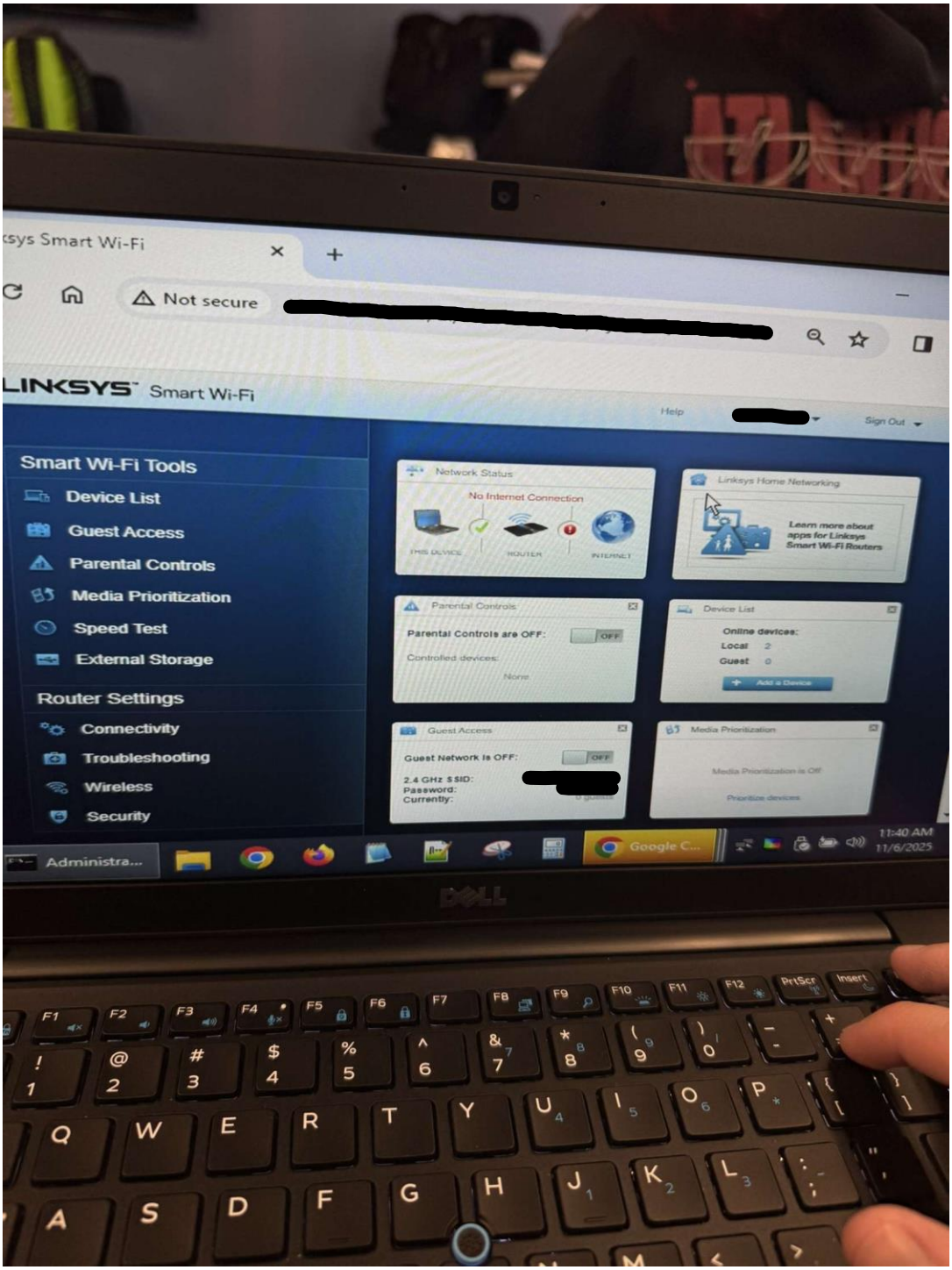
1. Configure the wireless router / access point (AP) provided to your group with the following settings:
   a. Set SSID to "Group Name"

   b. Set Wireless Security to WPA2-Personal
   c. Set Passphrase to the one provide by instructor
      (Keep the passphrase a secret!)
   d. Ensure SSID is being broadcasted



2. Write SSID on the whiteboard when your Wi-Fi network is ready to be cracked!

Complete!



3. One group member will join the group trying to hack your AP. This group member will use a device connect to the Wi-Fi network and generate traffic by continuously pinging the router / AP IP address. **THIS GROUP MEMBER MUST KEEP THE PASS PHRASE A SECRET!!!**

CRACK WPA Wi-Fi Network (15points)

Provide Screenshots / Images of Each Step

1. Boot computer from your live Kali Linux media (bootable flash USB)

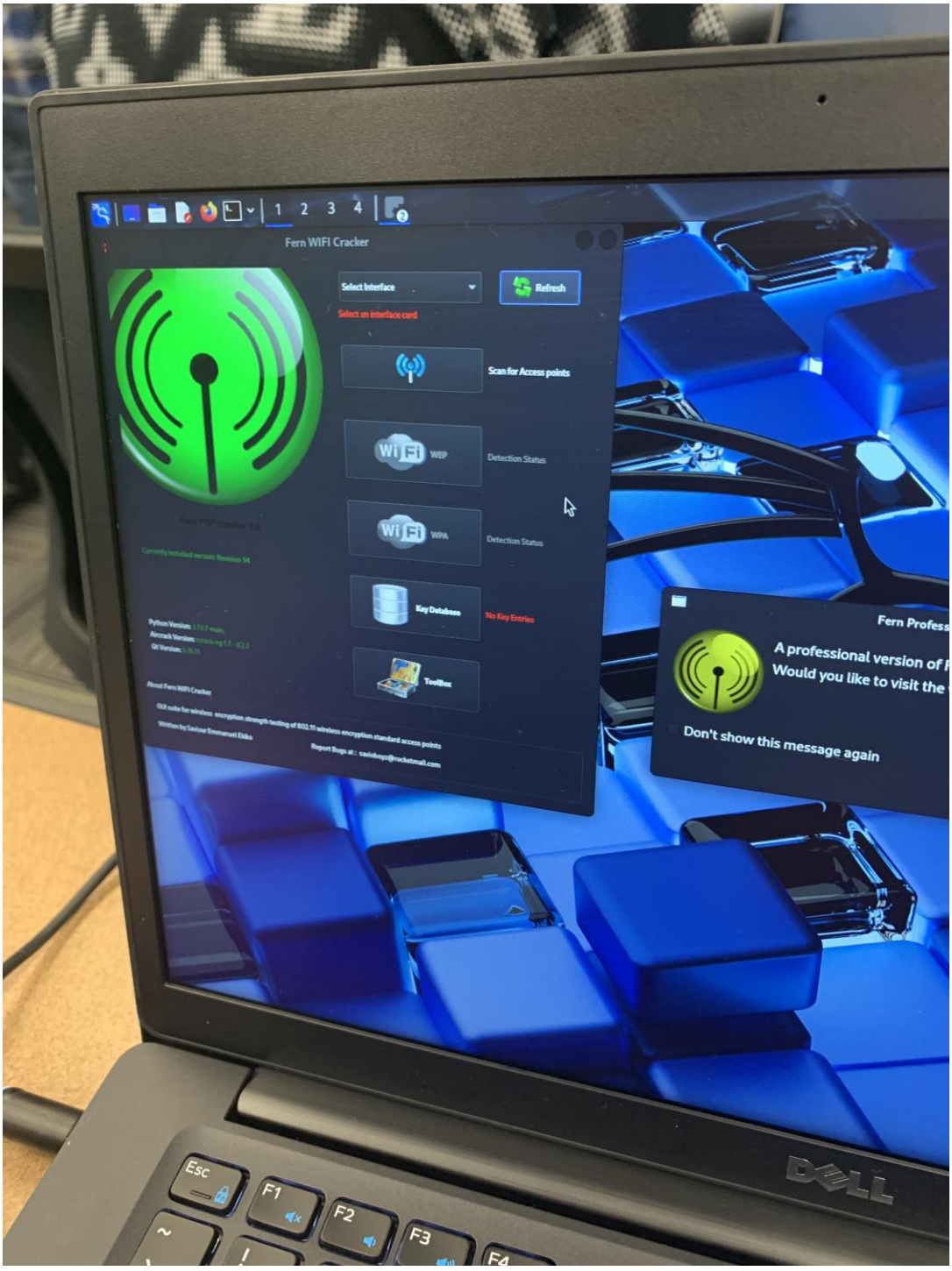
2. Start Fern-Wifi-Cracker utility

    a. Select the appropriate wireless network interface card (ie. wlan0)

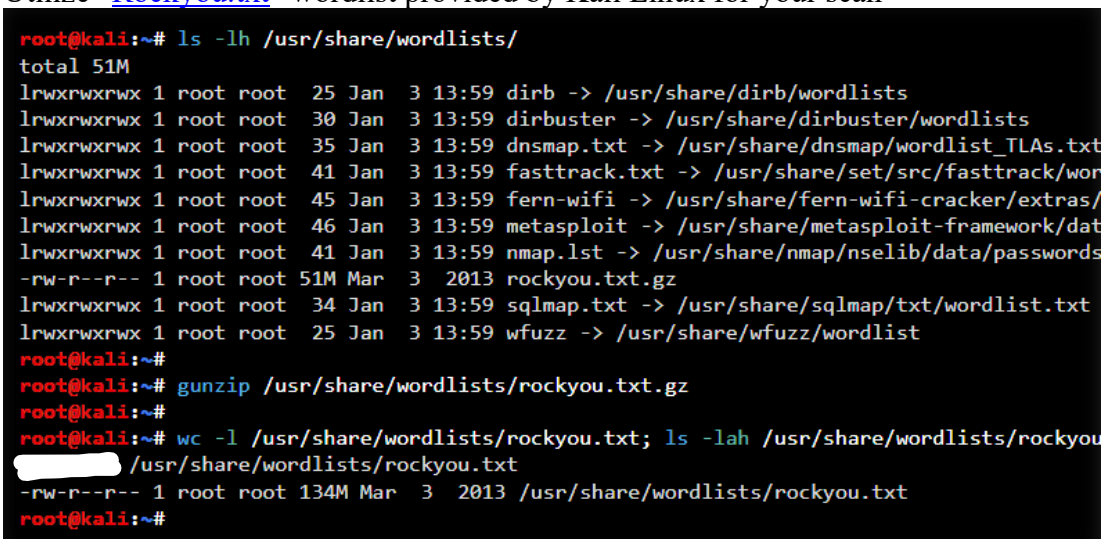
    b. Scan for Wi-Fi networks (ie. Active)

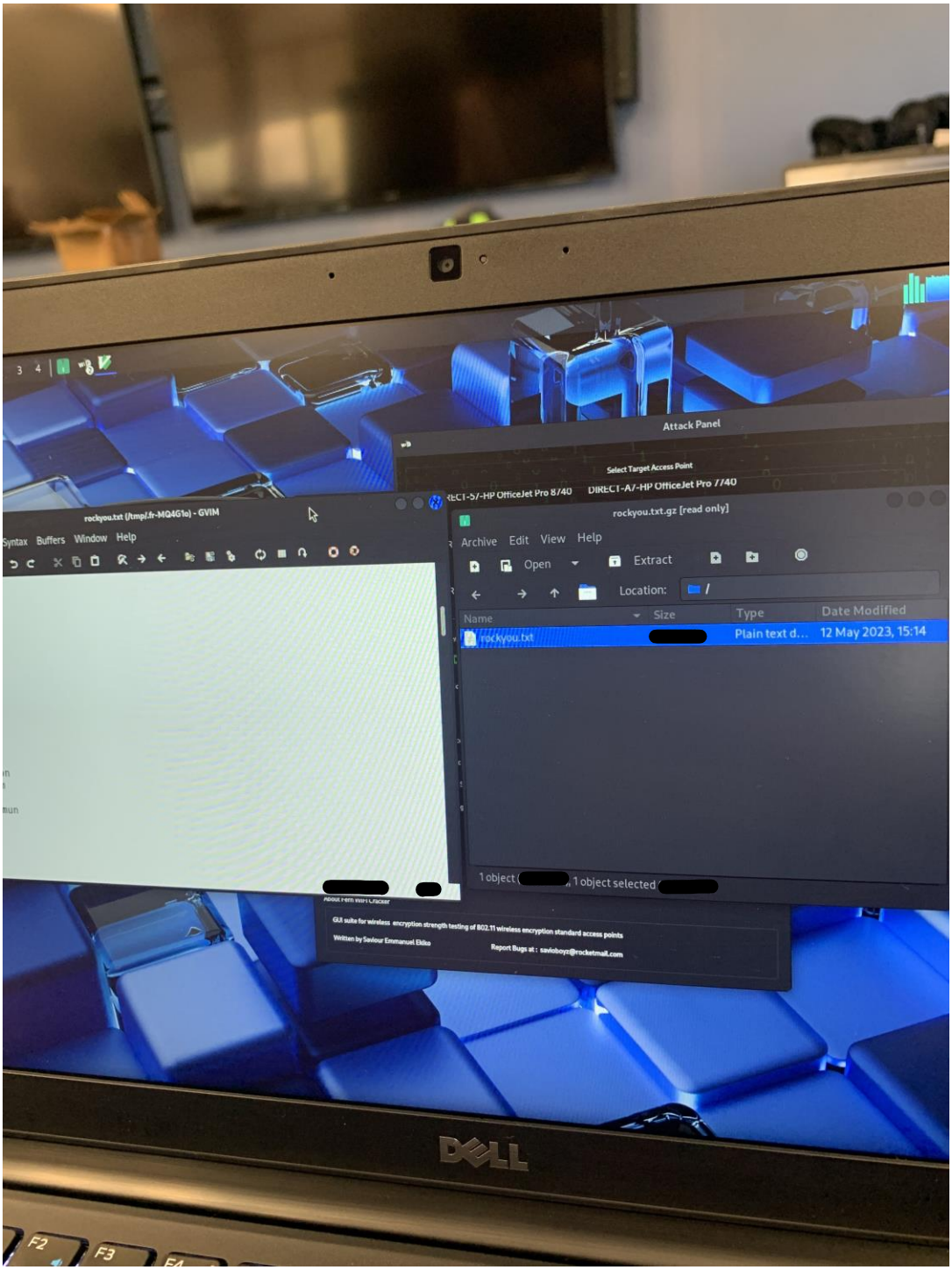
c. View Wi-Fi networks utilizing WPA

d. Select the SSID provided by another group (ready to be attacked)

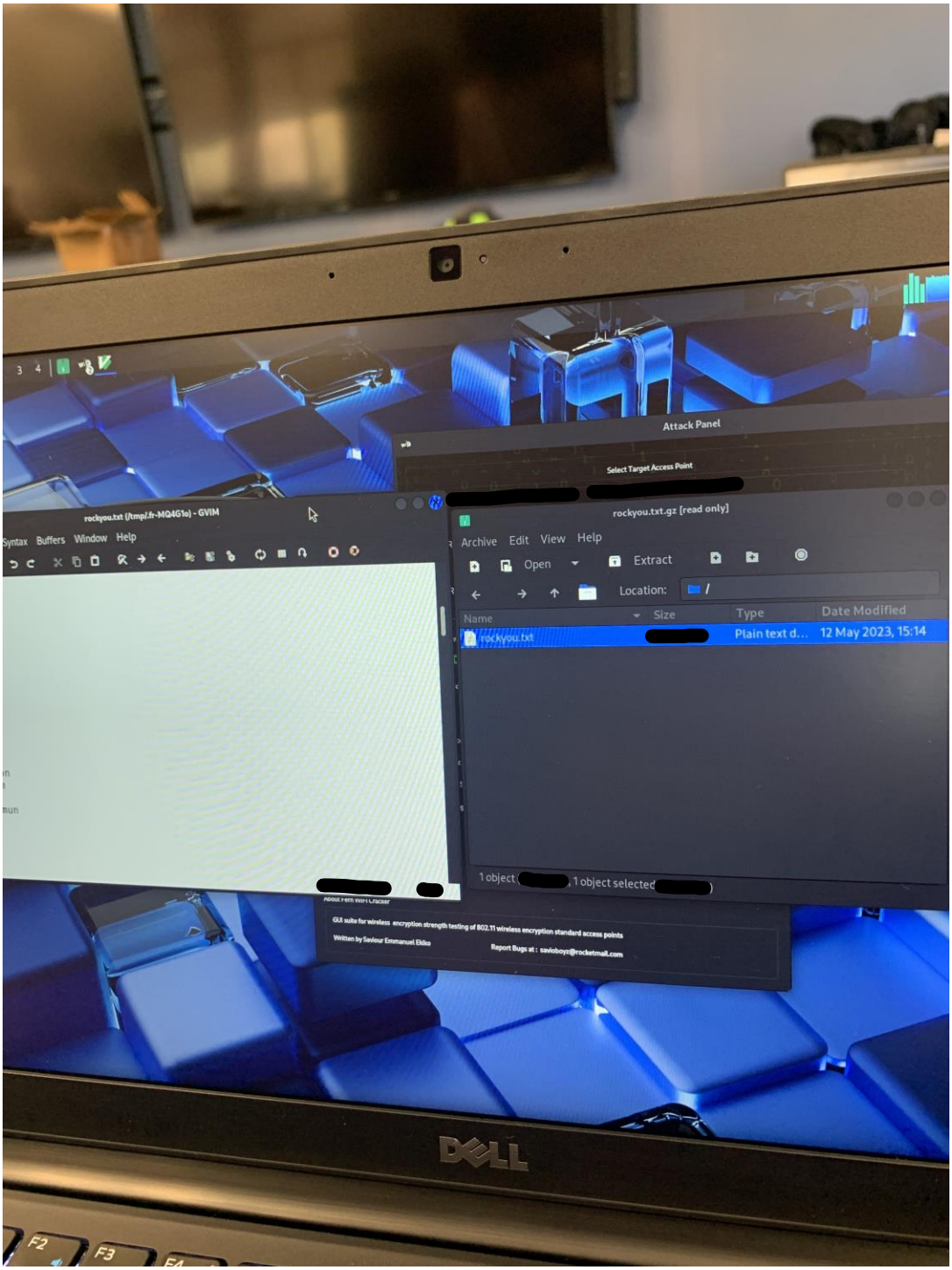


e. Utilize "Rockyou.txt" wordlist provided by Kali Linux for your scan





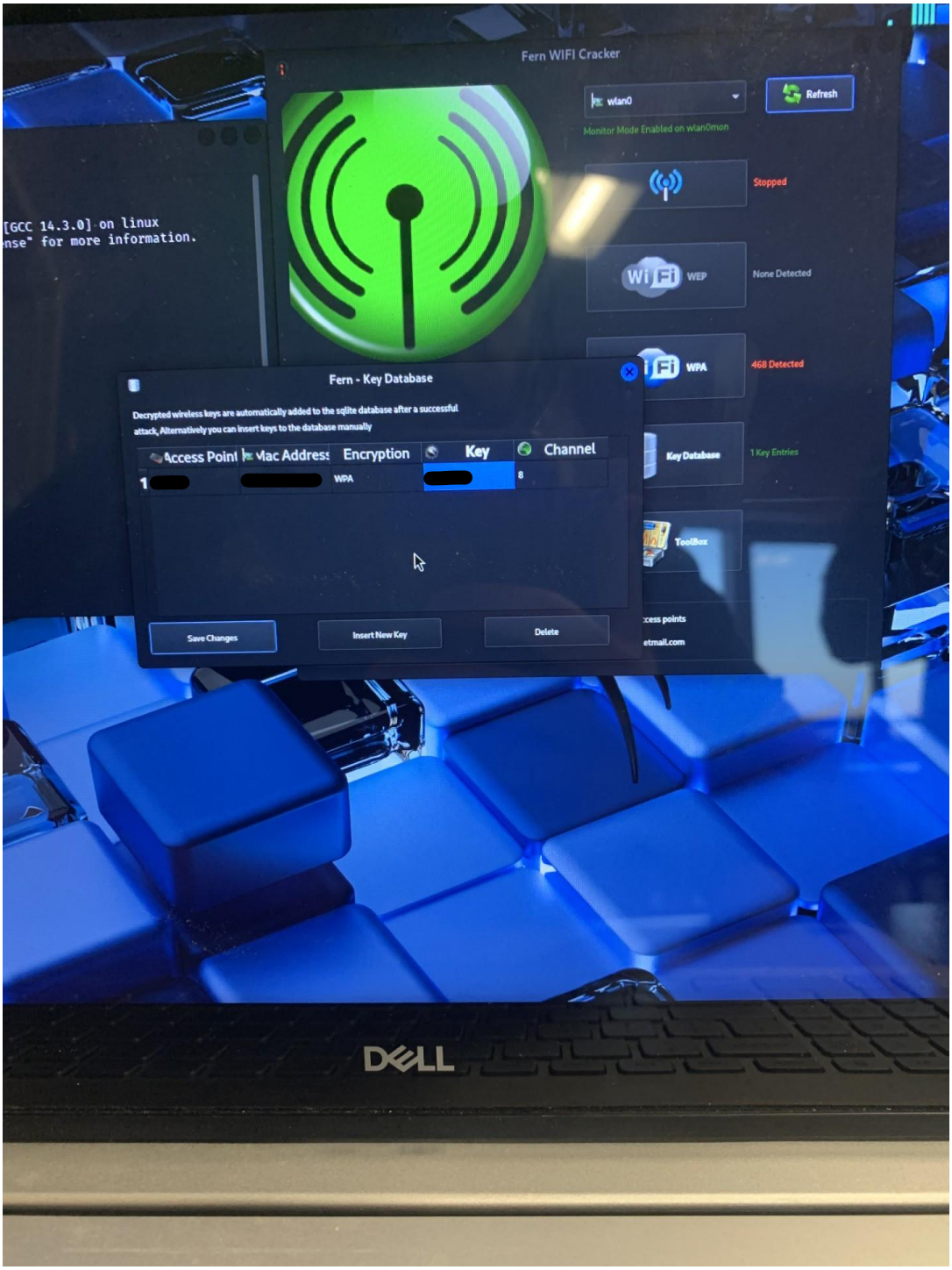
f. View the text file. How large is the rockyou.txt file?

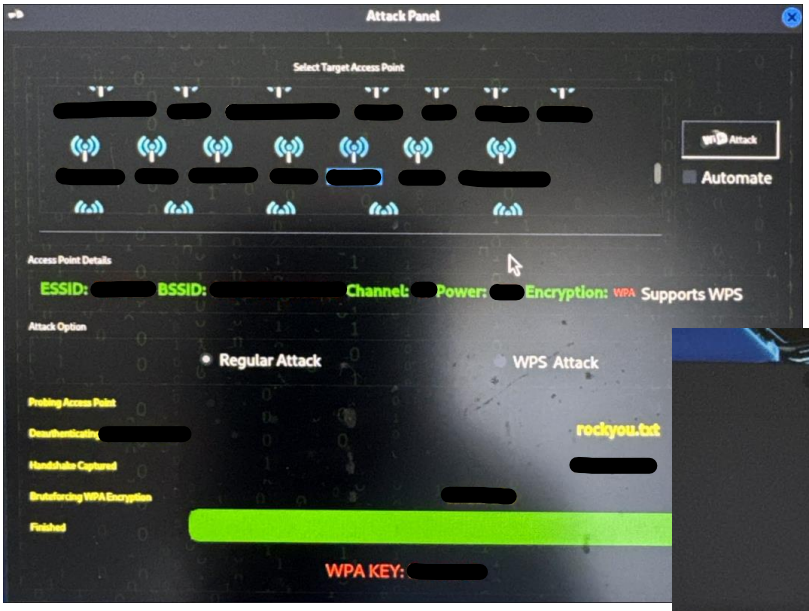


[redacted]

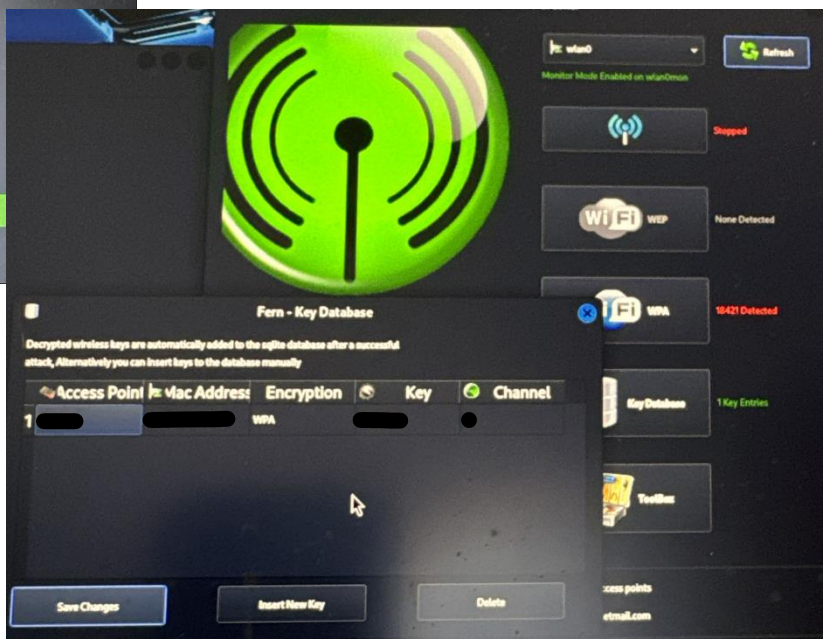
g. Begin scan / attack

h. What is the pass phrase? Is it stored in the Key Database


Fern WIFI Cracker
wlan0
Refresh
Monitor Mode Enabled on wlan0mon
Stopped
WEP
None Detected
WPA
468 Detected
Key Database
1 Key Entries
ToolBox
[GCC 14.3.0] on linux
nse" for more information.
Fern - Key Database
Decrypted wireless keys are automatically added to the sqlite database after a successful attack, Alternatively you can insert keys to the database manually
Access Point
Mac Address
Encryption
Key
Channel
WPA
8
Save Changes
Insert New Key
Delete
DELL



Example showing WPA cracked



Example showing pass phrased stored in Key Database

HARDEN Wireless Router / AP (5 points)

1. What steps will you take to harden the wireless router / AP (Wi-Fi Network) to make it more difficult to gain access?
   The first would be to use a password that was not involved in a massive data leak. And with that, use a password that is more complex and original, following a minimum of 14 characters along with a special character and upper and lowercase letter. If possible, use https management that limits accessing it on specific LAN IPs if possible to reduce the attack area.

Zach Jon Shi