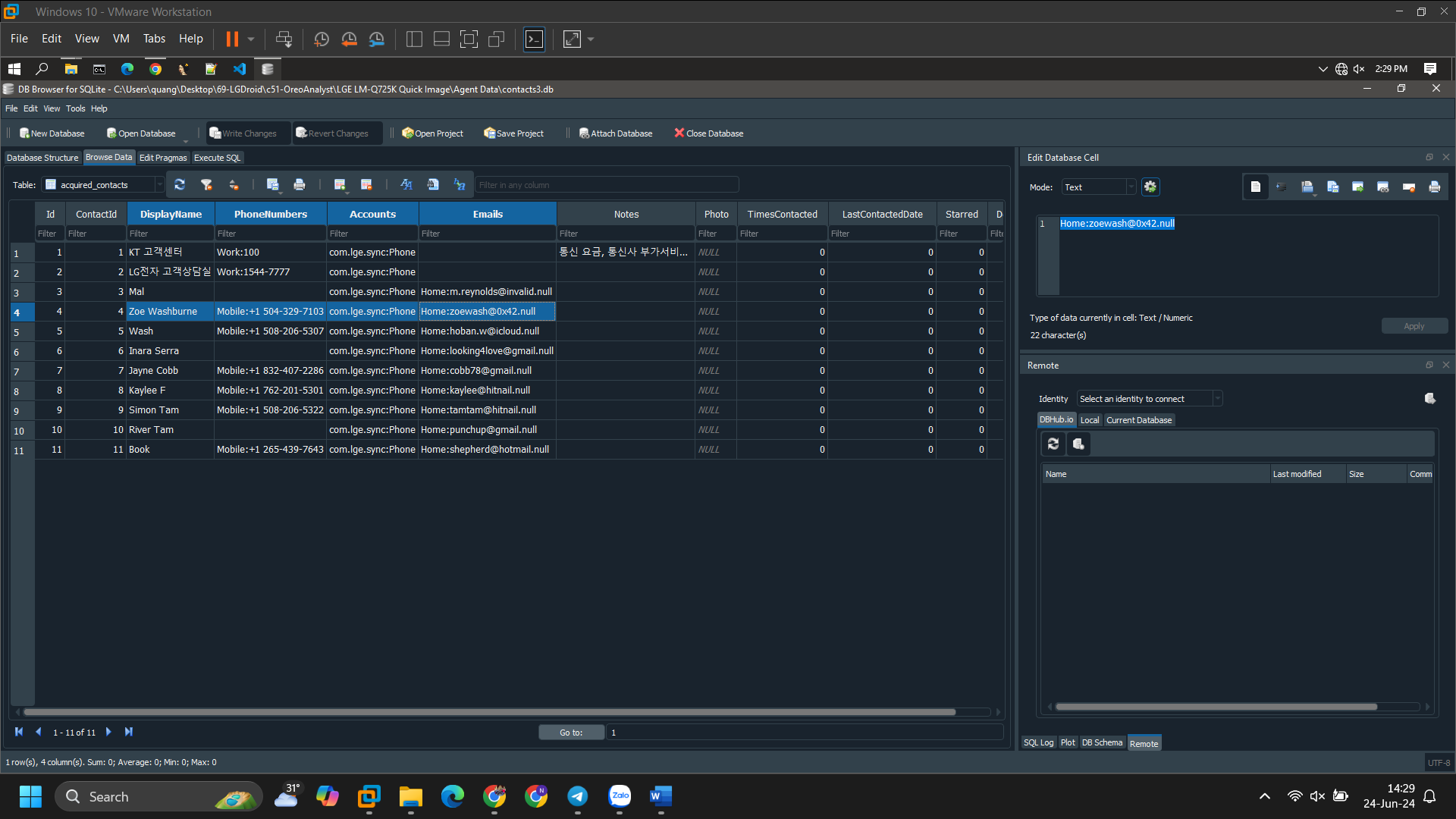
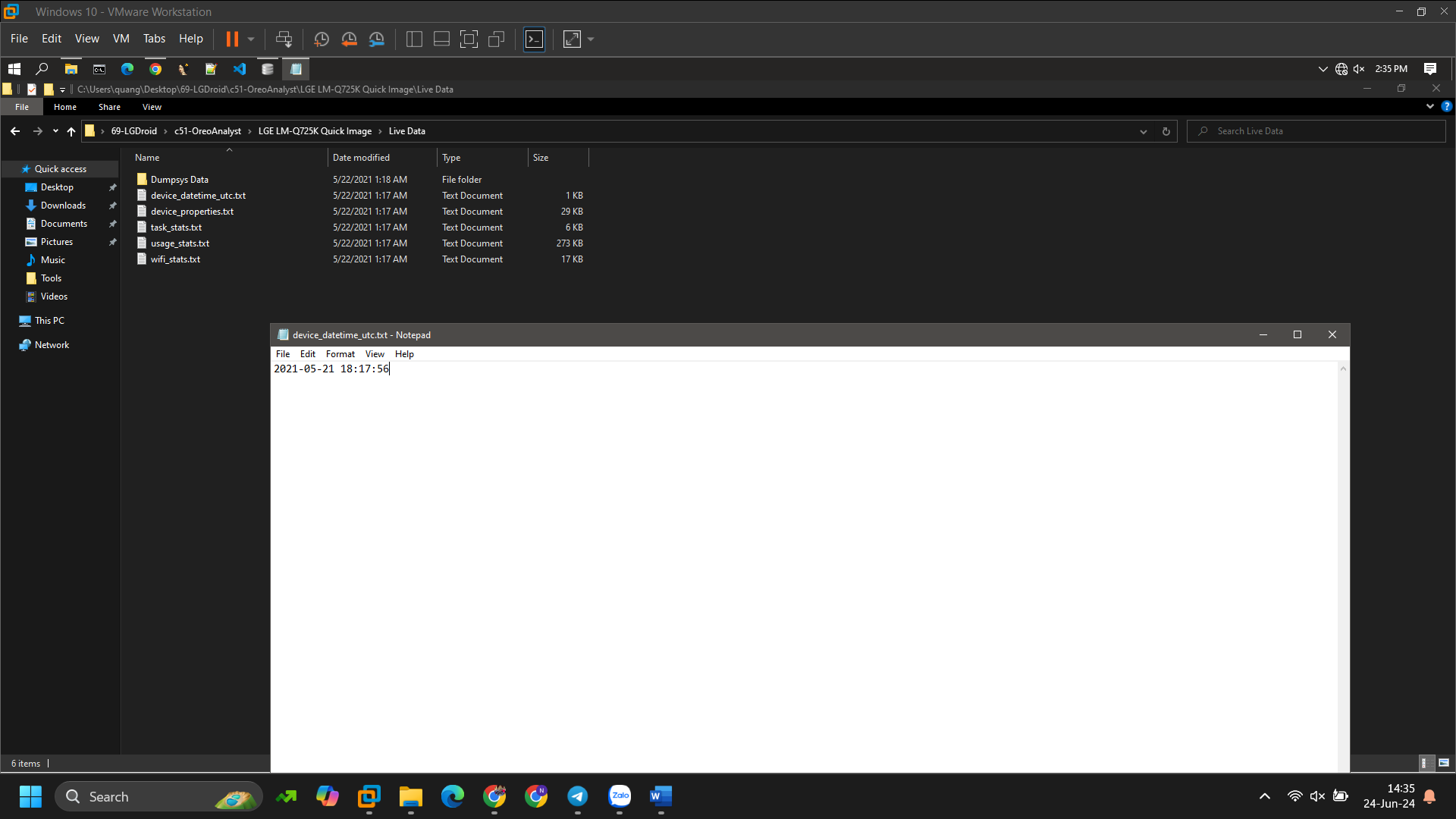
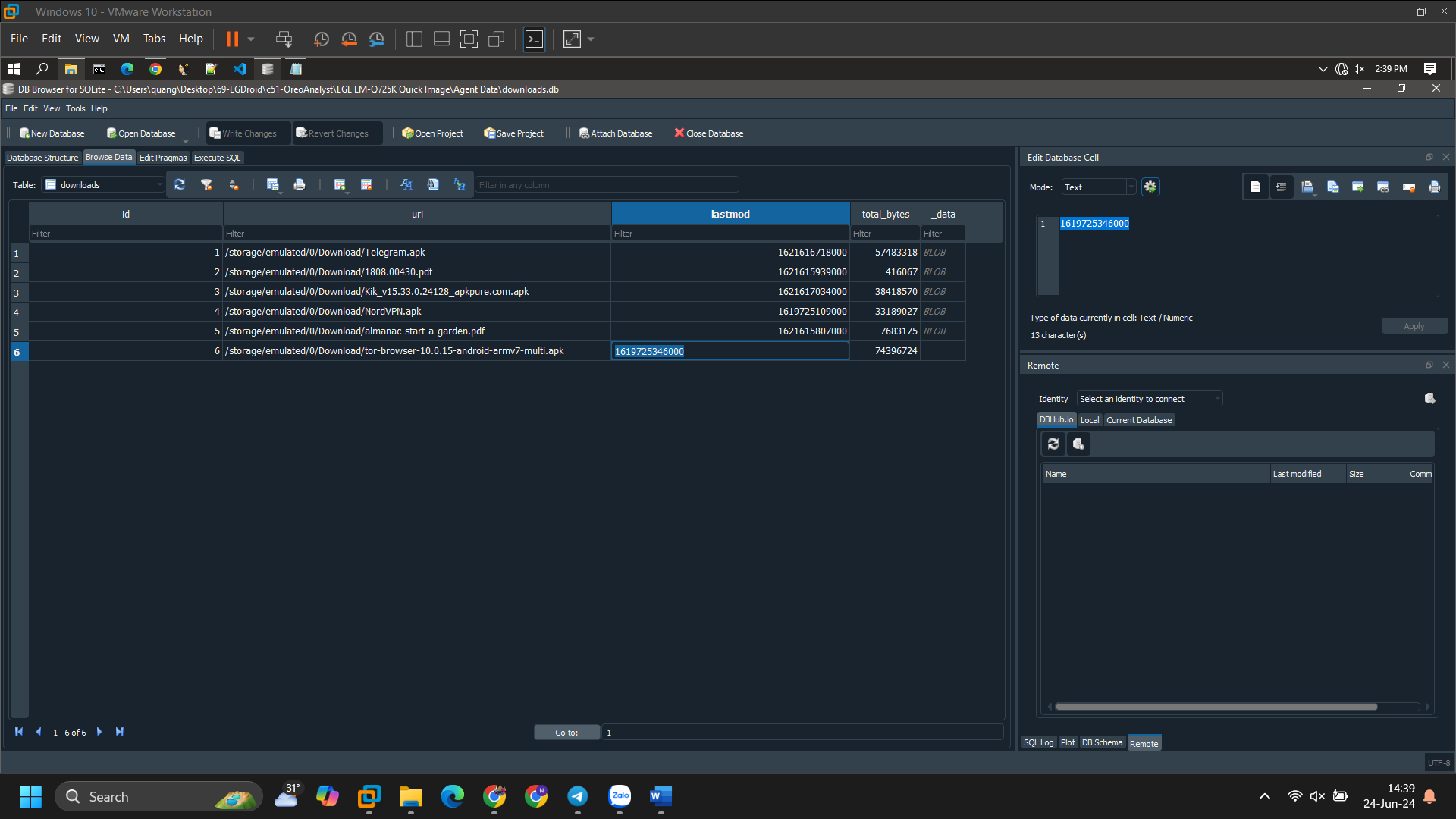
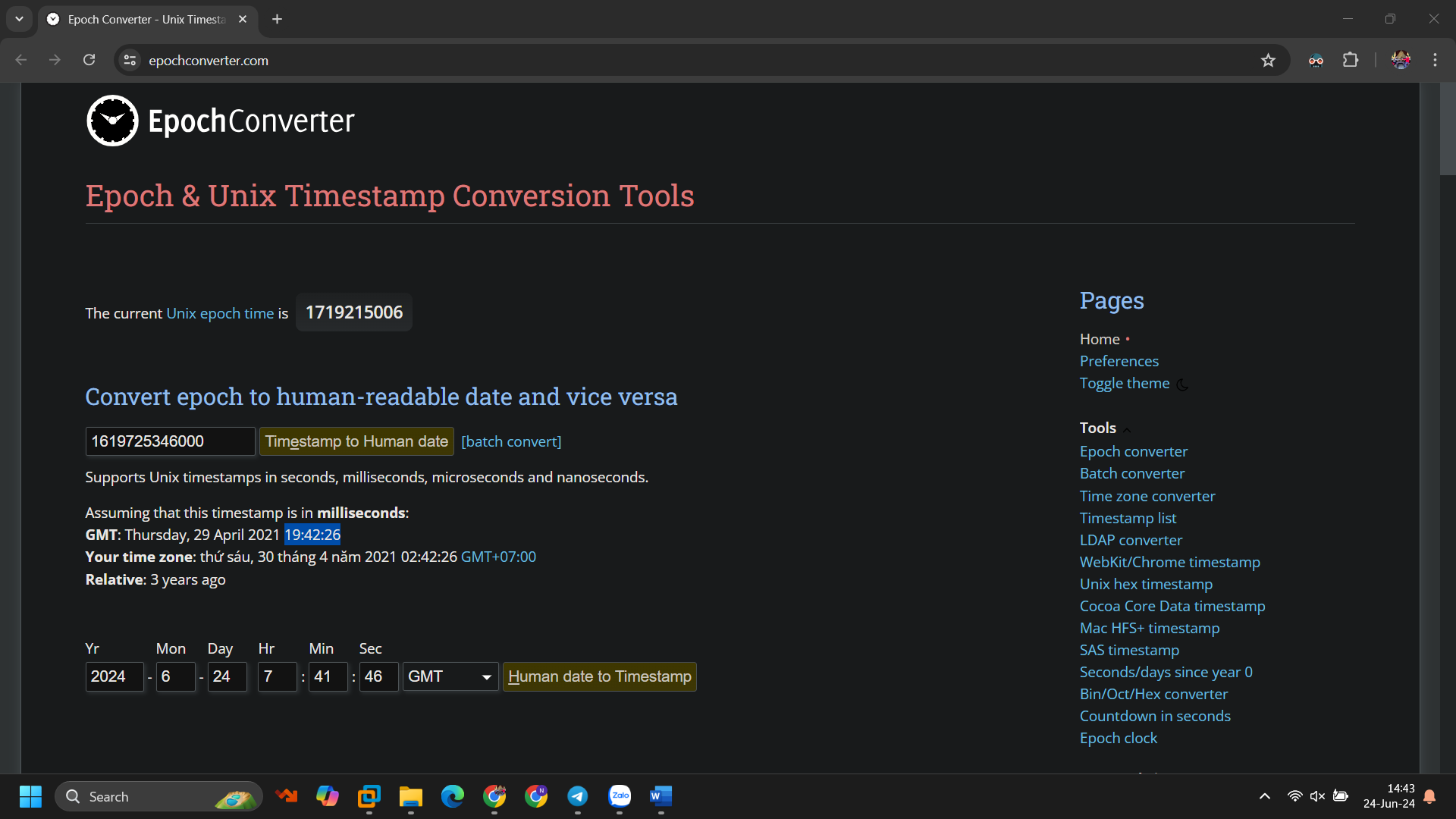
<https://cyberdefenders.org/blueteam-ctf-challenges/lgdroid/>

Q1. Địa chỉ email của Zoe Washburne là zoewash@0x42.null.  
Dựa vào thông tin, dữ liệu cá nhân được lưu trong cơ sở dữ liệu SQLite có tên Agent Data\Contacts3d.db.  


Q2. Thời gian của thiết bị ở UTC tại thời điểm thu lại lại là 18:17:56.  
Thời gian của thiết bị được lưu lại trong file Live Data\device\_datetime\_utc.txt. Thông tin trong file là 2021-05-21 18:17:56.  


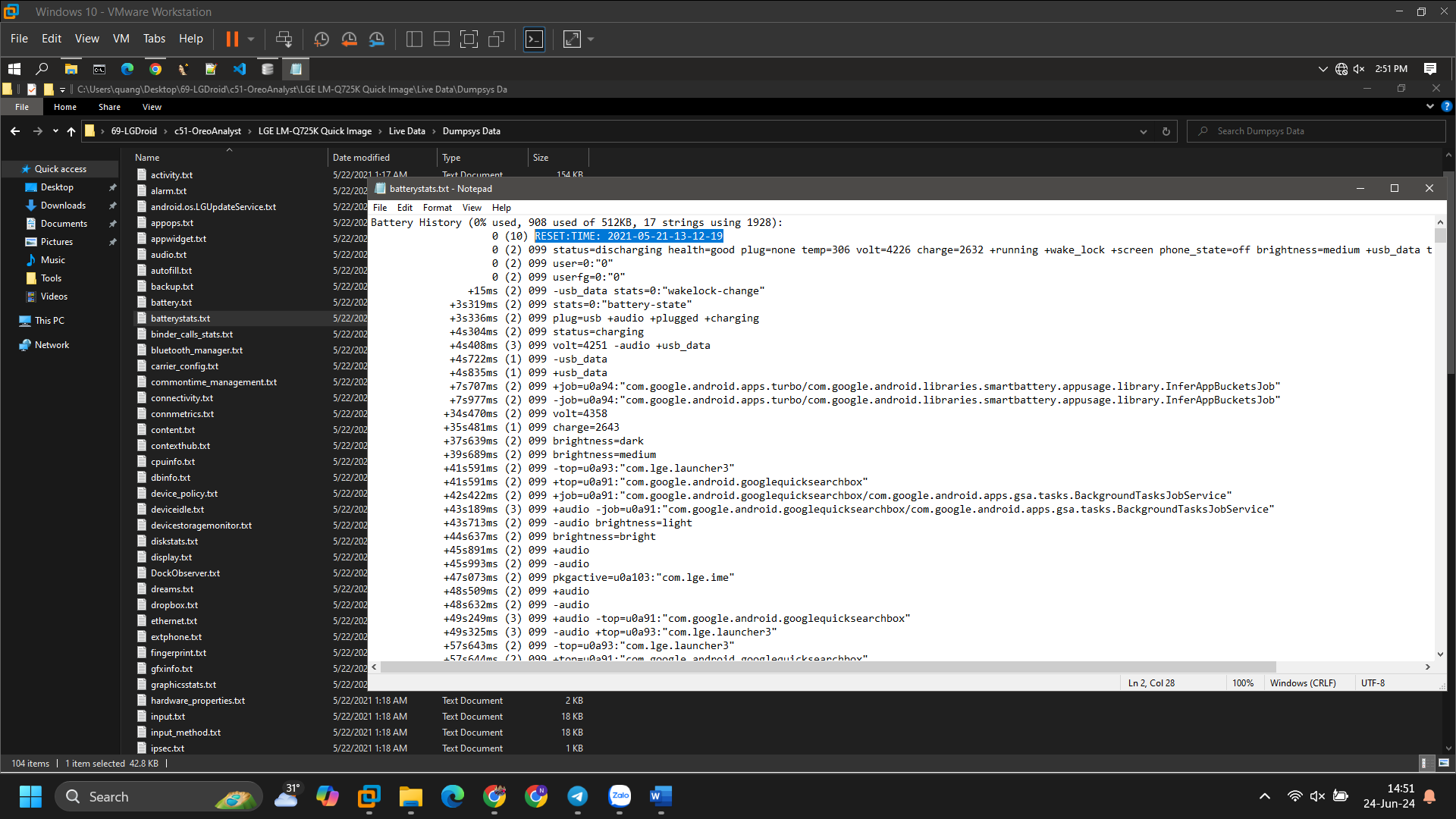
Q3. Tor Browser được tải xuống lúc 19:42:26 theo giờ UTC.

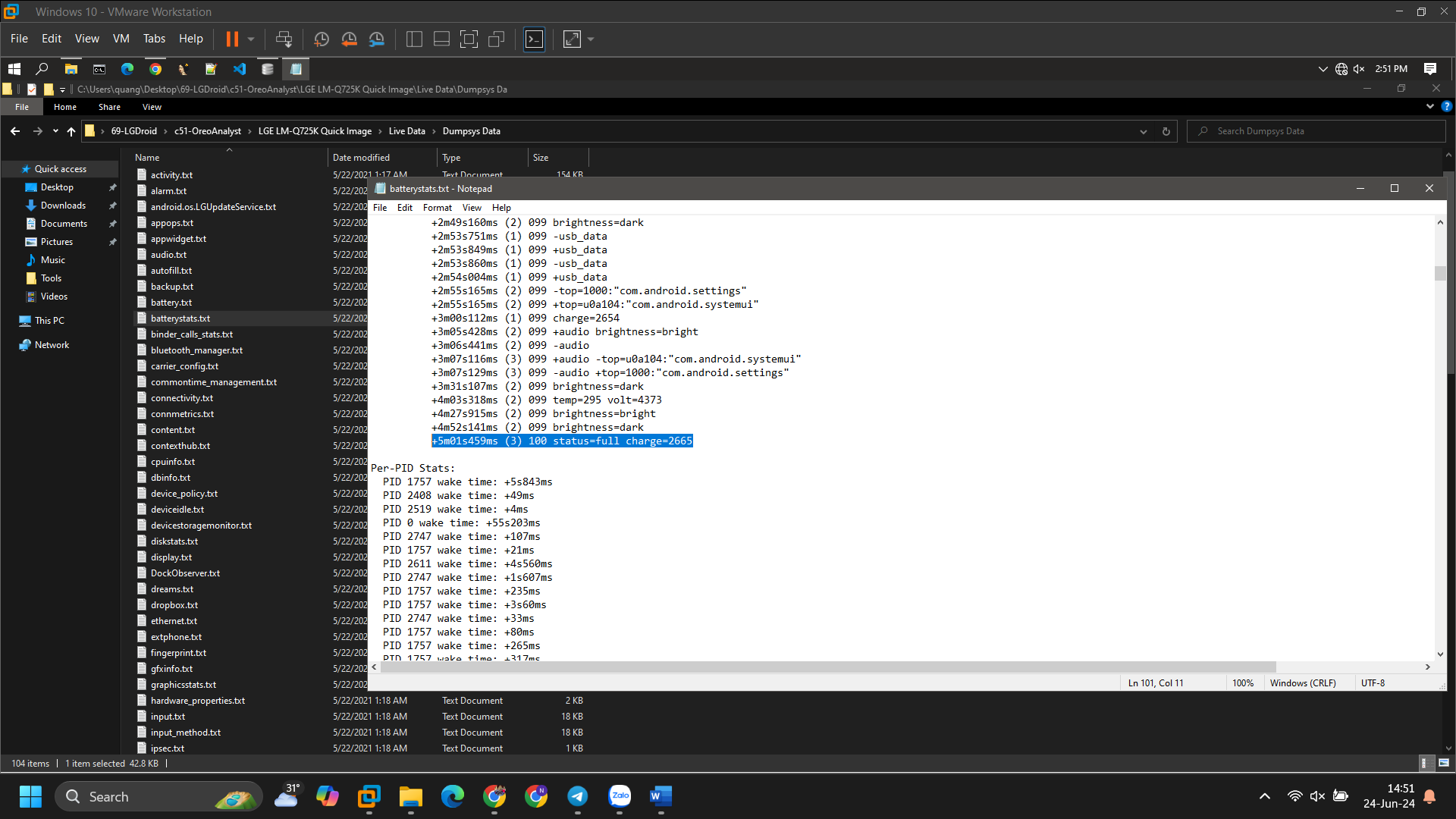
Dựa vào thông tin, thông tin các mục tải xuống của thiết bị được lưu trong cơ sở dữ liệu SQLite có tên Agent Data\downloads.db. Trong bảng downloads, cột lastmod (thời gian) của Tor Browser đã bị mã hóa thành 1619725346000.  


Để xem thời gian tải xuống của Tor Browser 1619725346000, ta sử dụng <https://www.epochconverter.com/> để xem thời gian, kết quả là 19:42:26.   


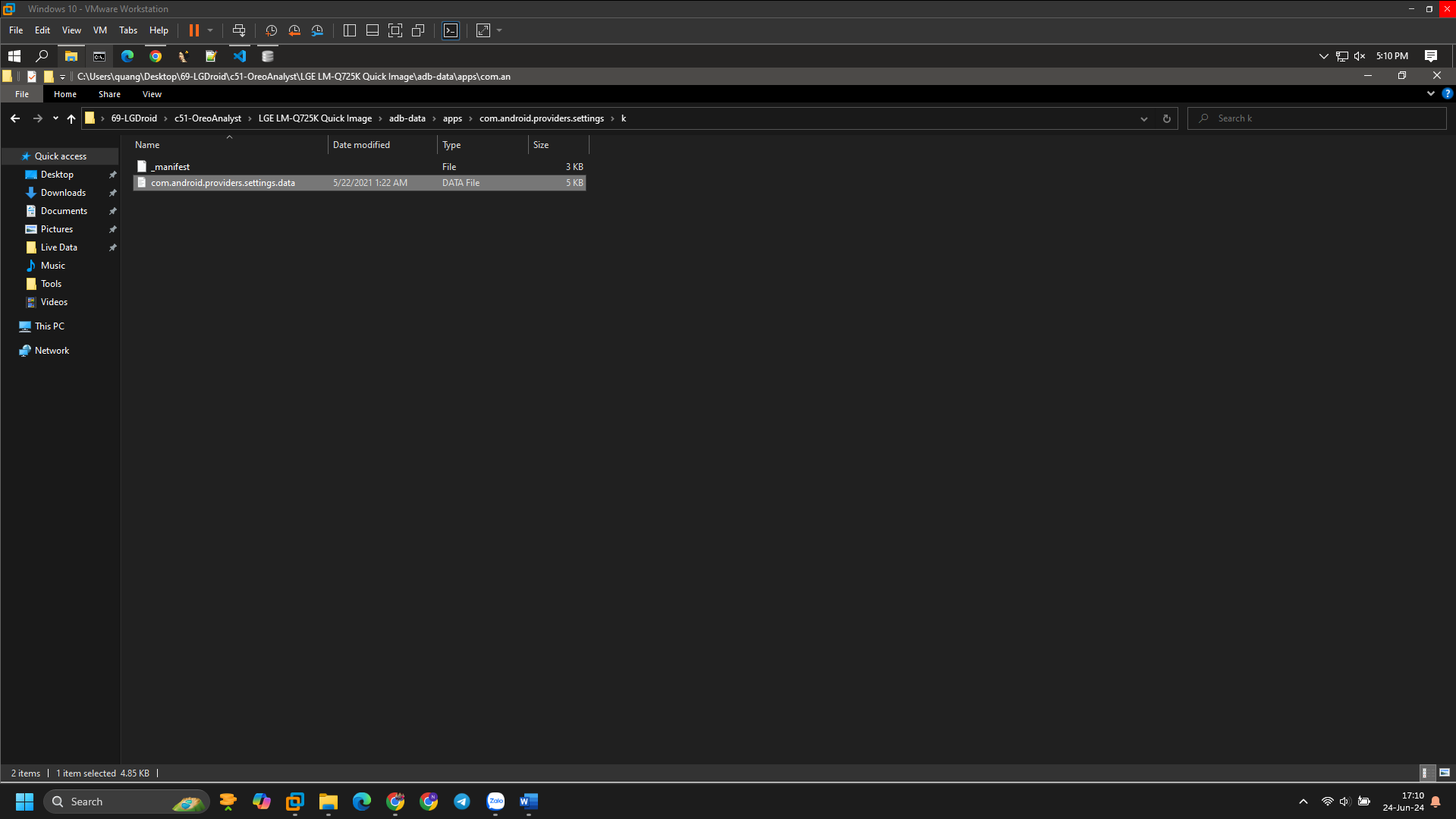
Q4. Điện thoại đã sạc đến 100% vào lúc 13:17:20 sau lần đặt lại cuối cùng.

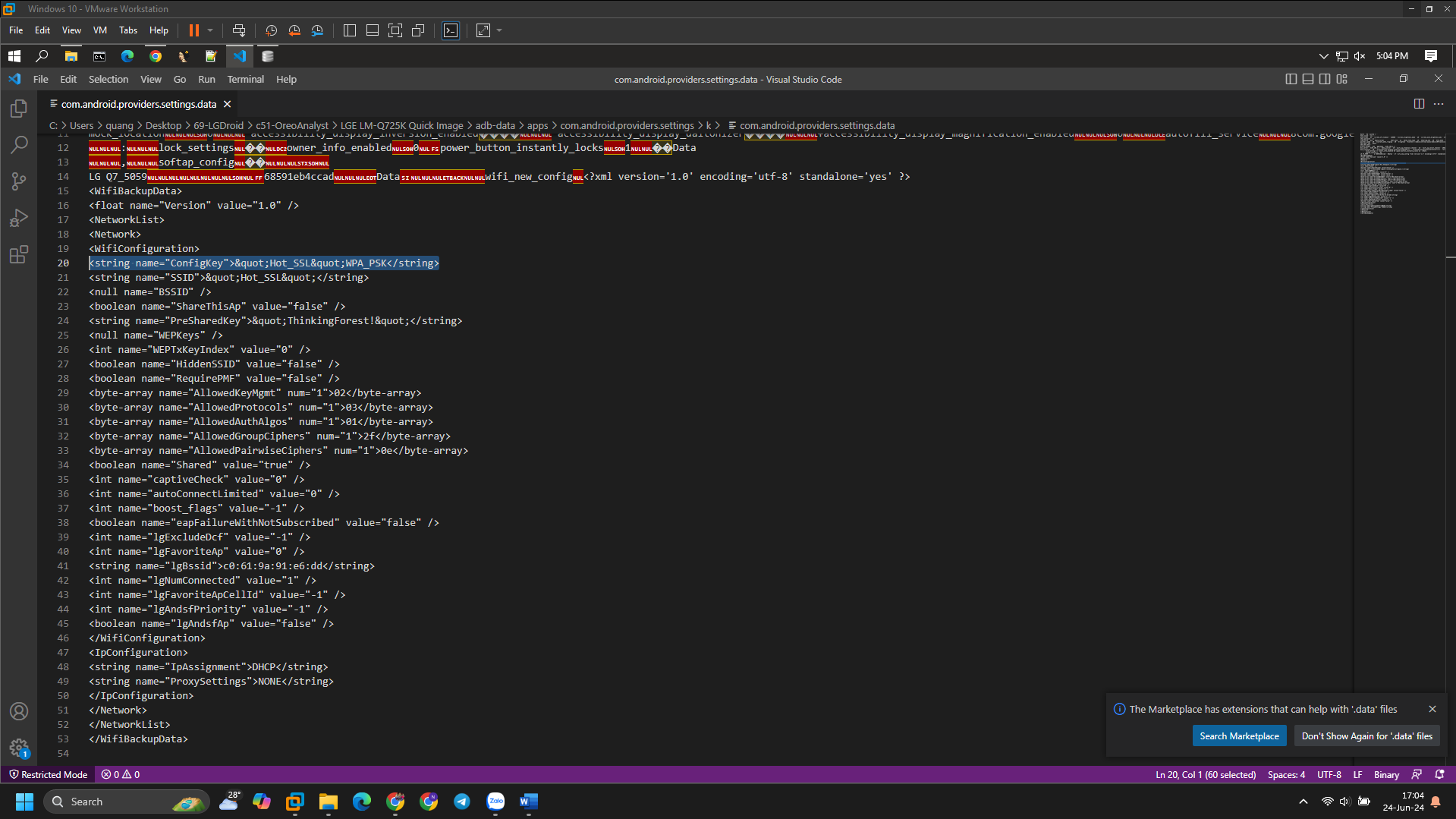
Kiểm tra file Live Data\Dumpsys Data\batterystats.txt. Tìm tới mục RESET:TIME: để xem thời gian thiết bị được cắm sạc sau khi bị sập nguồn và pin xuống 0%: RESET:TIME: 2021-05-21-13-12-19.

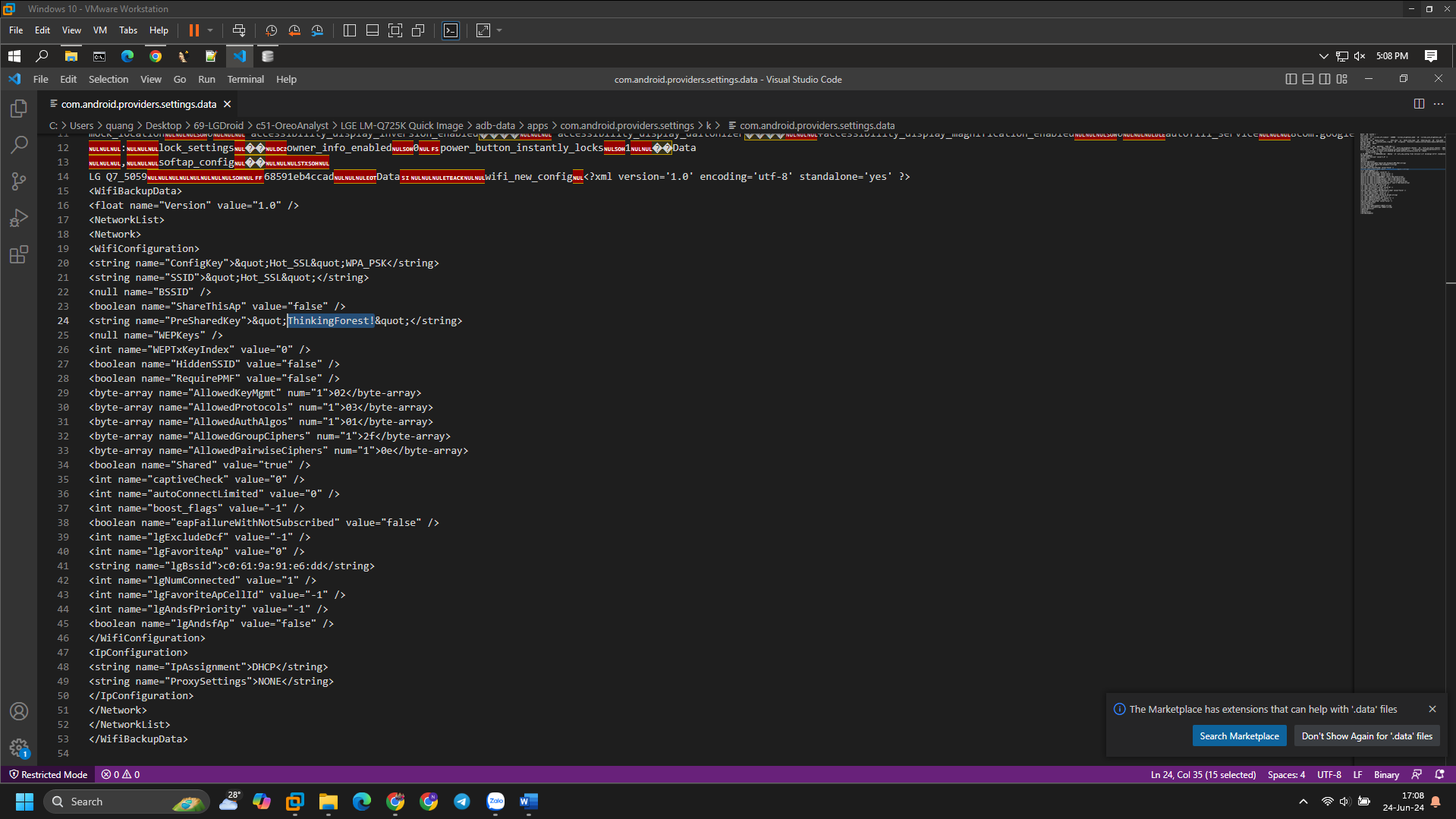


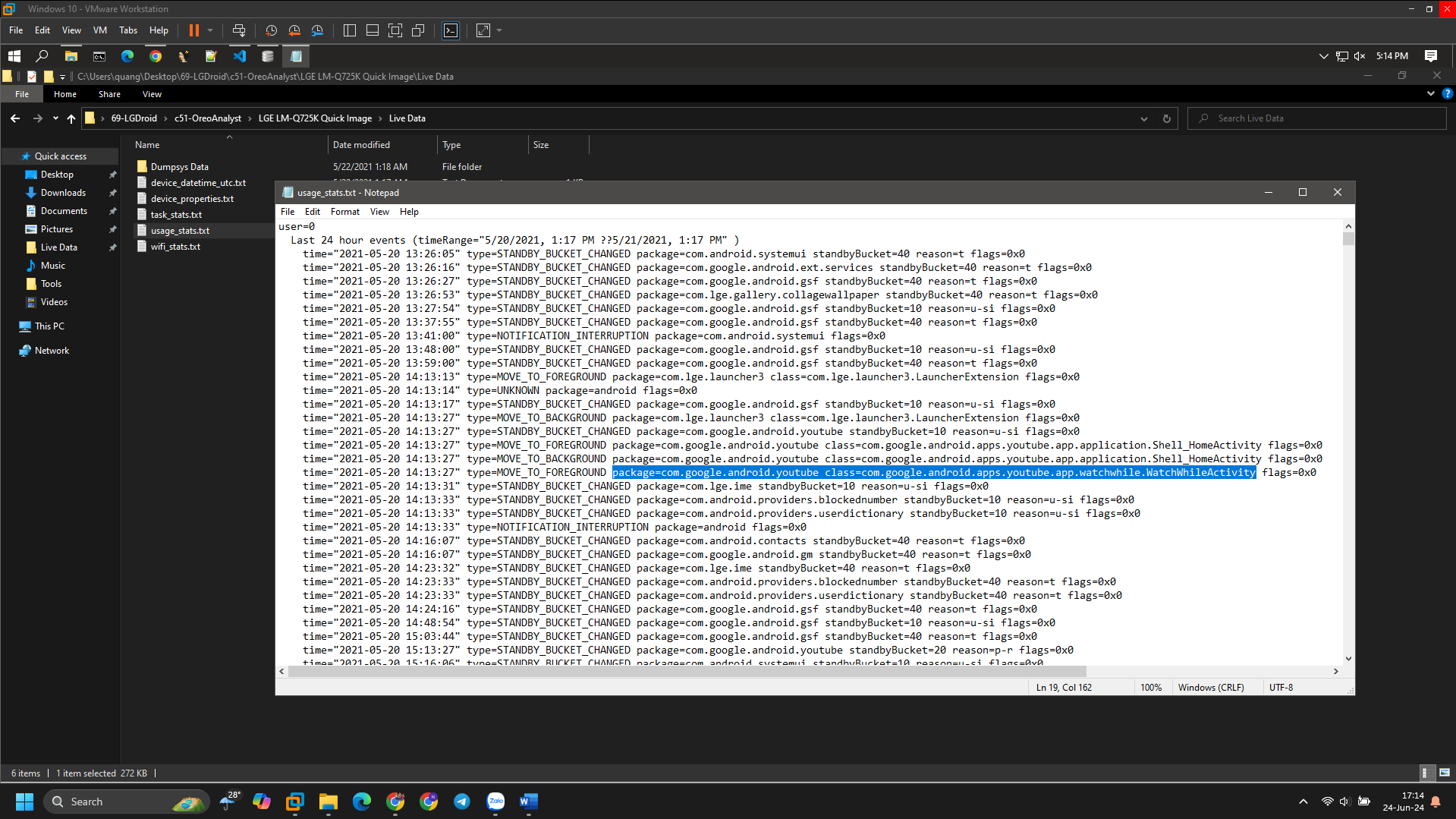
Tìm tới mục status=full để xem thời gian điện thoại được sạc lên 100%: 00:05:01. Từ đó lấy thời gian cắm sạc cộng với thời gian được sạc lên 100% là 13:17:20.  


Q5. Thông tin liên quan tới WIFI được lưu lại ở 3 file:  
Live Data/wifi\_status.txt ; Live Data/Dumpsys Data/wifi.txt ; Live Data/Dumpsys Data/wifip2p.txt. Tuy nhiên 3 file đó không phải là mục tiêu chúng ta hướng tới. Dựa theo <https://stackoverflow.com/questions/14964305/where-does-android-store-system-settings-such-as-wifi-networks>, chúng ta hướng tới đường dẫn adb-data\apps\com.android.providers.settings\k\com.android.providers.settings.data.



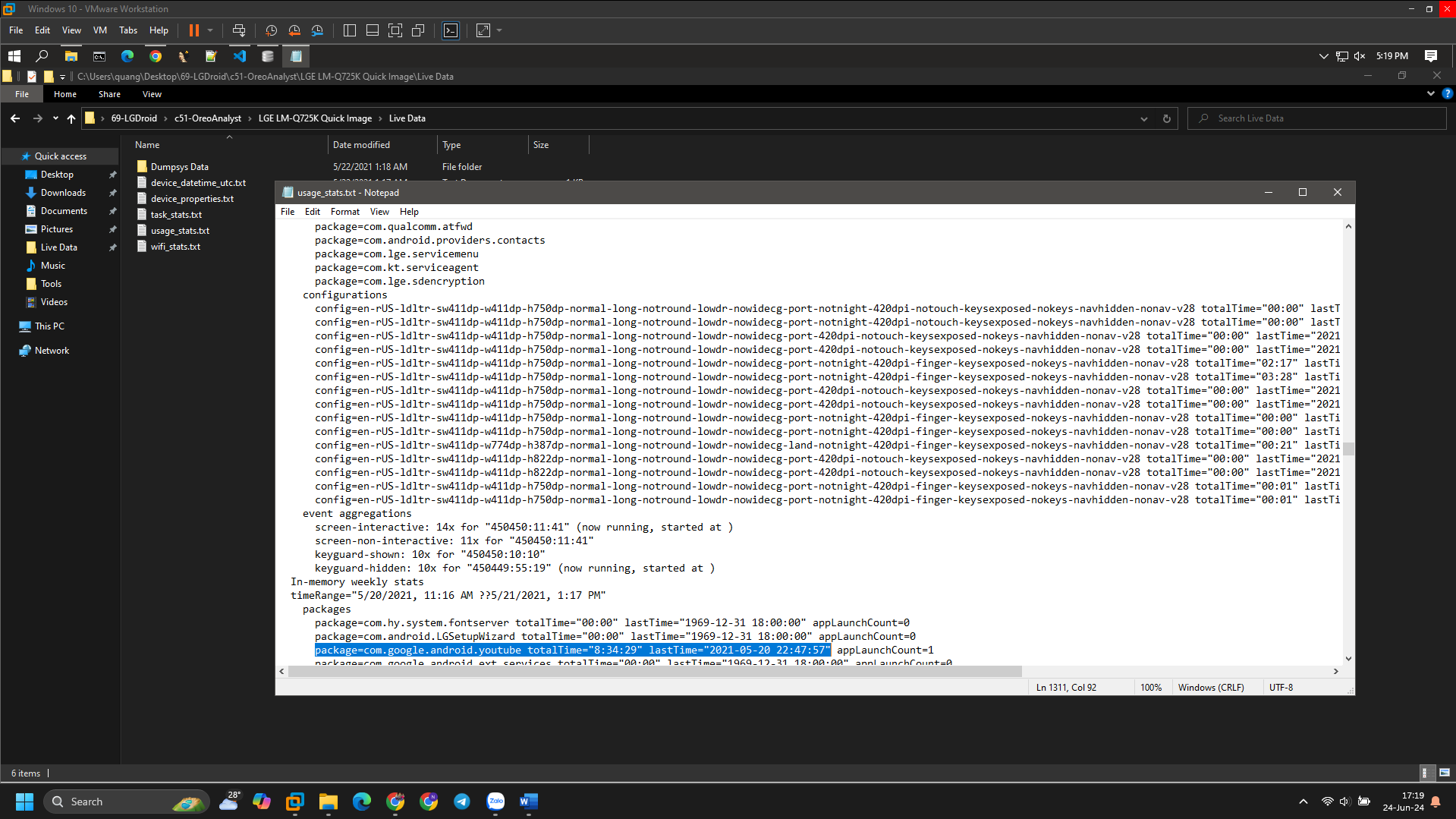
Ở trong file com.android.providers.settings.data, WIFI này sử dụng WPA\_PSK. Khi tìm kiếm trên Google với WPA\_PSK để biết đâu là mật khẩu WIFI, WPA\_PSK là phương thức bảo mật được sử dụng với PreSharedKey, và PreSharedKey chính là mật khẩu WIFI.  


Ở mục PreSharedKey, chúng ta thấy có đoạn chuỗi ký tự “ThinkingForest!”. Từ đó cho thấy “ThinkingForest” chính là mật khẩu WIFI.  


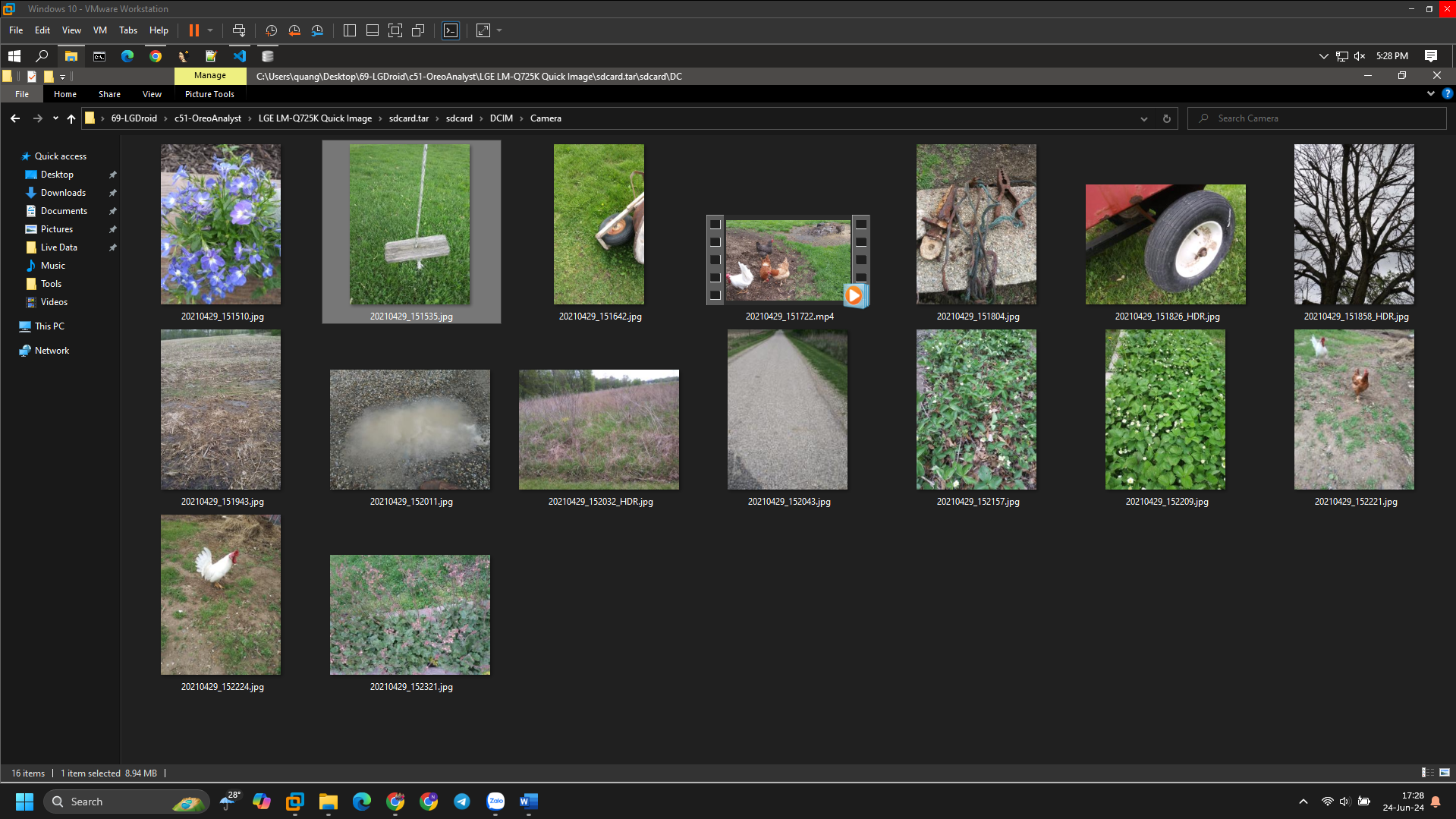
Q6. Người dùng tập trung vào ứng dụng YouTube vào lúc 20/05/2021 14:13:27.  
Thông tin và thời gian sử dụng các chương trình/ứng dụng của thiết bị được lưu lại trong file Live Data\usage\_stats.txt. Với thời gian 20/05/2021 14:13:27, package=com.google.android.youtube class=com.google.android.apps.youtube.app.watchwhile.WatchWhileActivity đã được sử dụng.  


Q7. YouTube đã được sử dụng trong 8:34:29 giờ vào ngày 20/05.2021.

Thông tin và thời gian sử dụng các chương trình/ứng dụng của thiết bị được lưu lại trong file Live Data\usage\_stats.txt. Tìm kiếm totalTime với mục YouTube, ta thấy totalTime="8:34:29" lastTime="2021-05-20 22:47:57".



Q8. suspicious.jpg: Số liệu về độ tương tự về cấu trúc của hình ảnh này so với hình ảnh tương tự về mặt hình ảnh được chụp bằng điện thoại di động là gì?

Hình ảnh tương tự với suspicious.jpg là 20210429\_151535.jpg trong mục sdcard.tar\sdcard\DCIM\Camera. sdcard.tar\sdcard\DCIM\Camera là nơi lưu trữ những ảnh đã chụp.  


Sử dụng script Python <https://ourcodeworld.com/articles/read/991/how-to-calculate-the-structural-similarity-index-ssim-between-two-images-with-python> để tính SSIM giữa 2 file ảnh, với câu lệnh python3 script.py --first 20210429\_151535.jpg --second suspicious.jpg. Hoặc sử dụng tool <https://darosh.github.io/image-ms-ssim-js/test/browser_test.html> trên website. Kết quả là 0.99.  
