Họ tên: Trần Trí Dũng

MSSV: HE190680

Lớp: IA1901

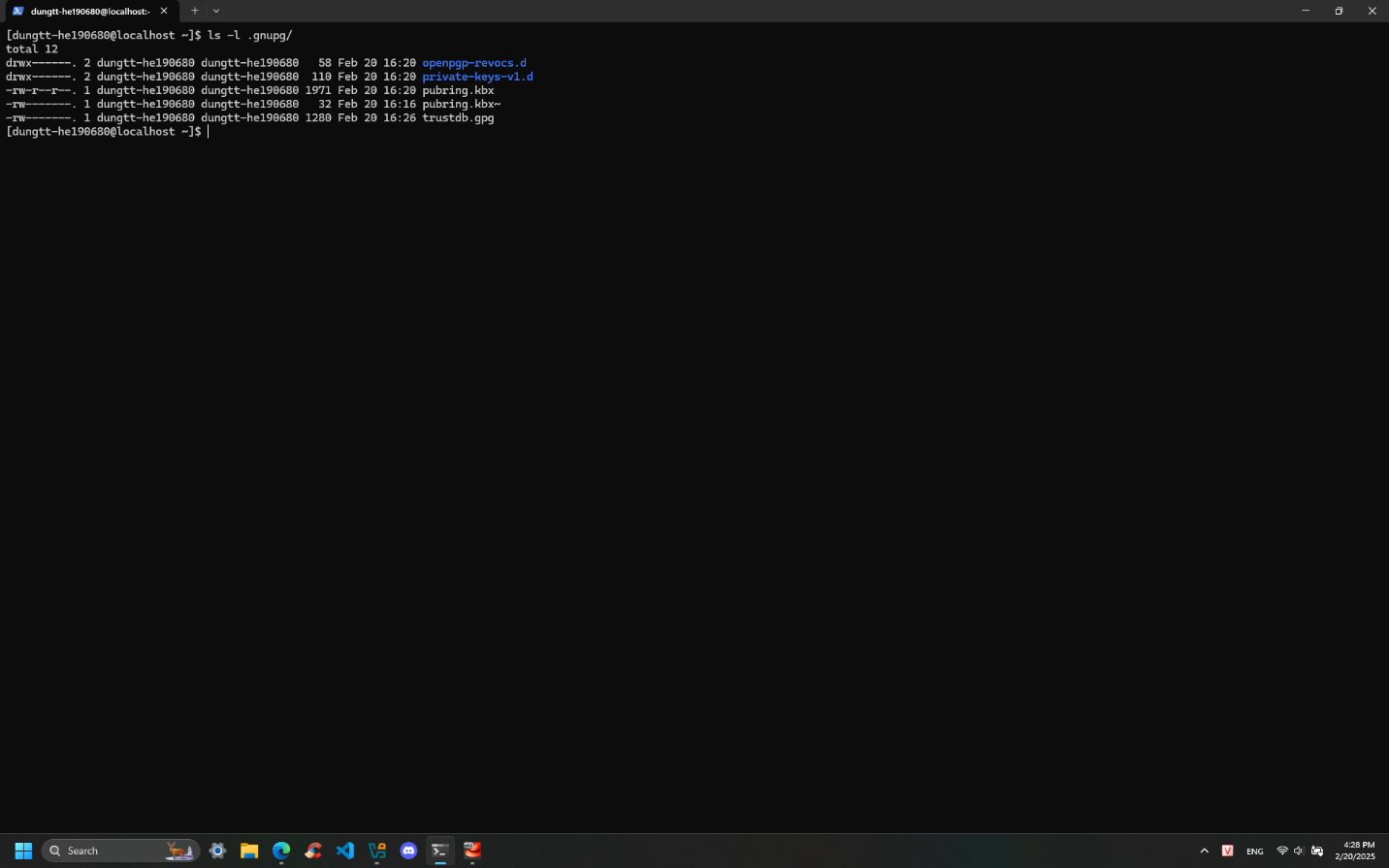
5.1 – Creating your GPG keys

Các file và thư mục được tạo ra:

* openpgp-revocs.d: Thư mục chứa chứng chỉ thu hồi
* private-keys-v1.d: Thư mục chứa khóa riêng tư
* pubring.kbx: File chứa khóa công khai
* pubring.kbx~: File backup của khóa công khai
* trustdb.gpg: Cơ sở dữ liệu về độ tin cậy của các khóa

Phân quyền:

* Các thư mục có quyền drwx------ (700): chỉ chủ sở hữu có toàn quyền
* File pubring.kbx có quyền -rw-r--r-- (644): mọi người có thể đọc
* Các file còn lại có quyền -rw------- (600): chỉ chủ sở hữu có thể đọc/ghi



5.2 – Symmetrically encrypting your own files

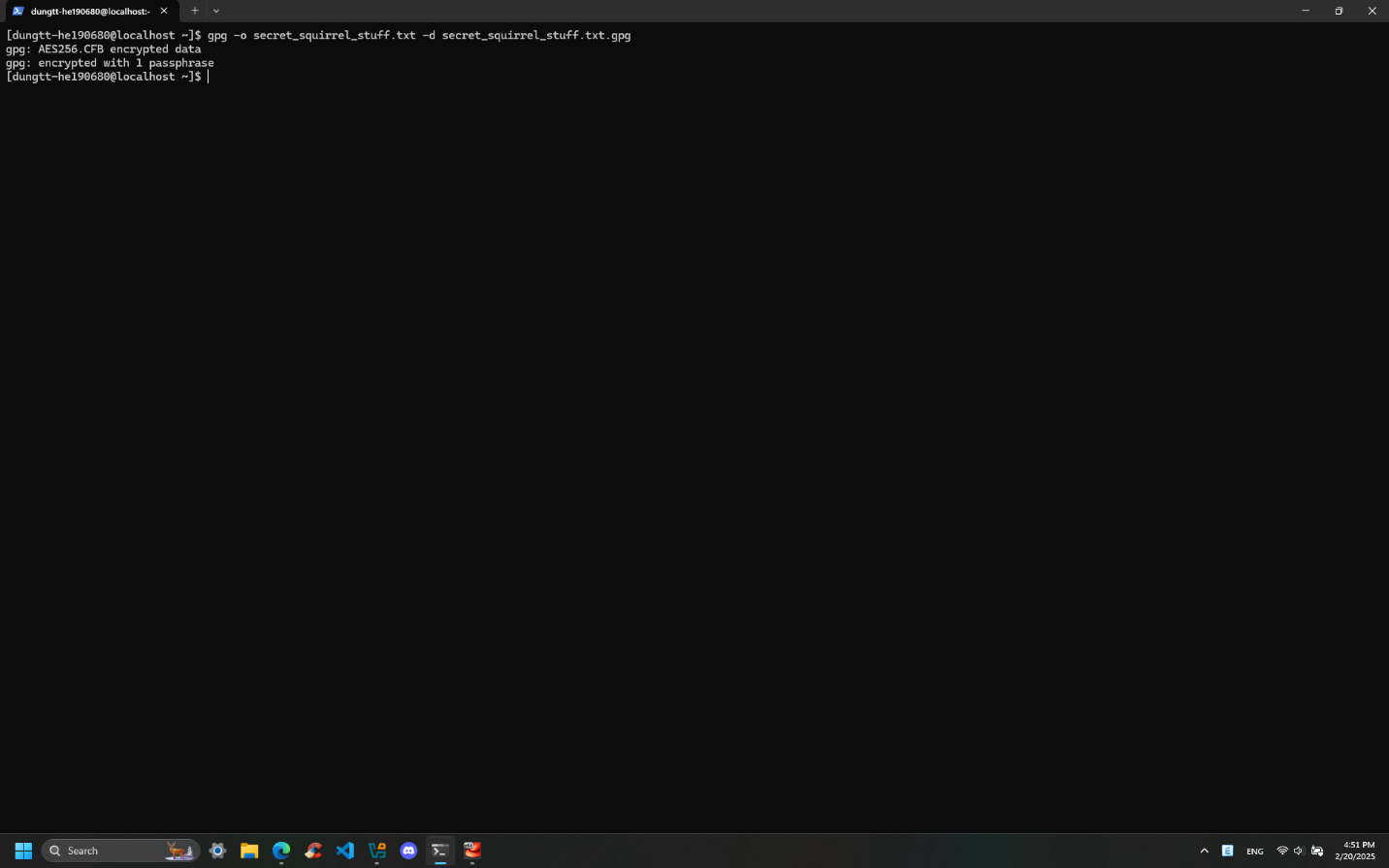
Đây là lệnh giải mã file GPG, trong đó:

* -o secret\_squirrel\_stuff.txt: Chỉ định tên file output sau khi giải mã
* -d: Option để giải mã (decrypt)
* secret\_squirrel\_stuff.txt.gpg: File đã được mã hóa cần giải mã

Kết quả hiển thị:

* gpg: AES256.CFB encrypted data: Cho biết file được mã hóa bằng thuật toán AES-256 ở chế độ CFB
* gpg: encrypted with 1 passphrase: File được mã hóa bằng 1 passphrase (mật khẩu)

Lệnh này sẽ tạo ra một file giải mã mới có tên secret\_squirrel\_stuff.txt từ file mã hóa secret\_squirrel\_stuff.txt.gpg



5.3 – Encrypting files with public keys

Thông tin mã hóa:

* File được mã hóa bằng khóa RSA3072
* ID khóa: EE3167DB83EFB500
* Được tạo ngày: 2025-02-28
* Người nhận: "Frank <frank@gmail.com>"

Nội dung giải mã:

This is TOP SECRET stuff that only Frank can see!!!!!

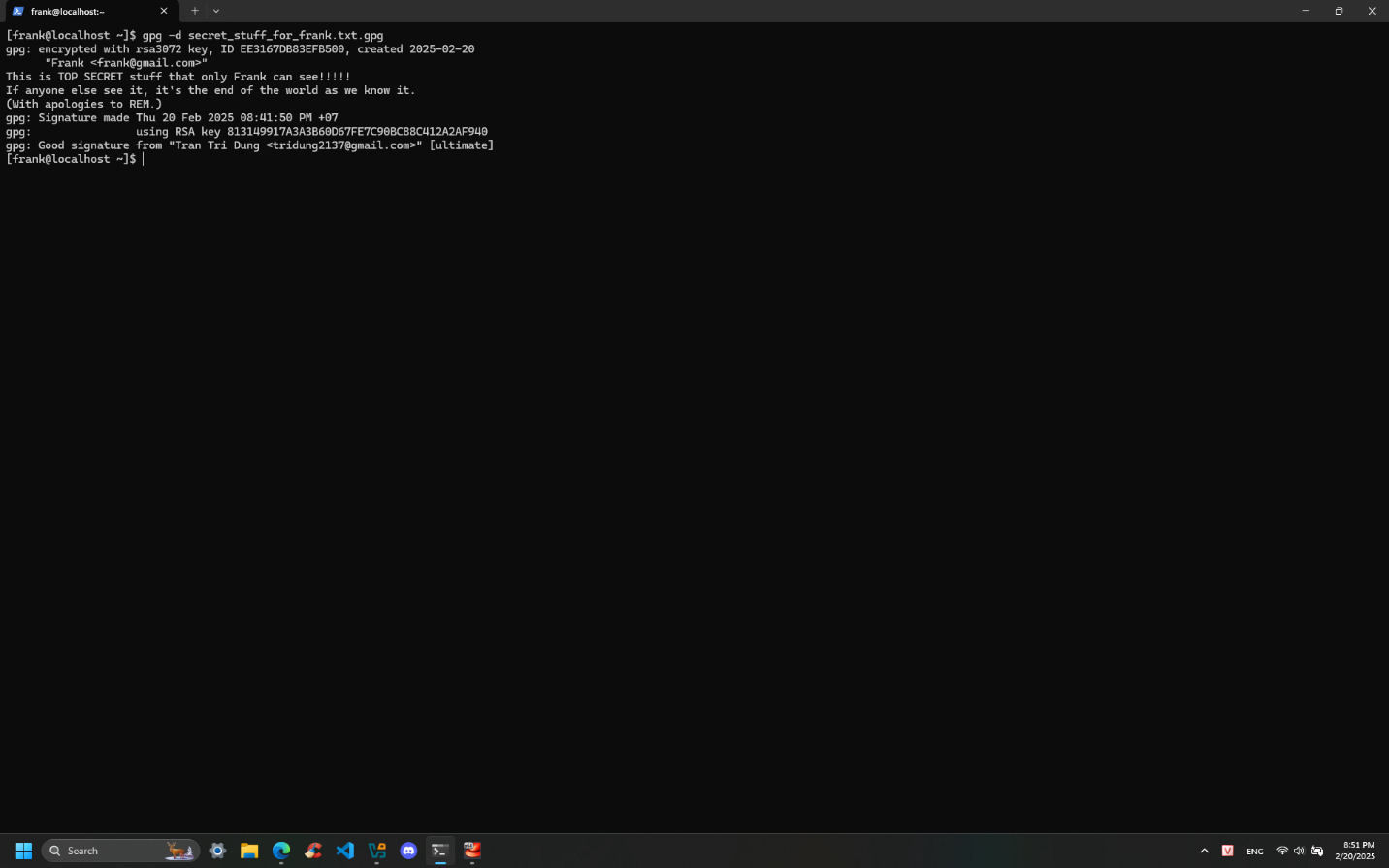
If anyone else see it, it's the end of the world as we know it.

(With apologies to REM.)

Thông tin chữ ký số:

* Thời gian ký: Thu 20 Feb 2025 08:41:58 PM +07
* Sử dụng khóa RSA: 813149917A3A3860D67FE7C90BC88C412A2AF949
* Chữ ký từ: "Tran Tri Dung <tridung2137@gmail.com>"
* Trạng thái: Good signature [ultimate] (chữ ký hợp lệ và được tin cậy hoàn toàn)

Điều này cho thấy:

* File chỉ có thể được giải mã bởi người nhận (Frank)
* Có chữ ký số để xác thực người gửi (Tran Tri Dung)
* Chữ ký được xác nhận là đáng tin cậy (ultimate trust)

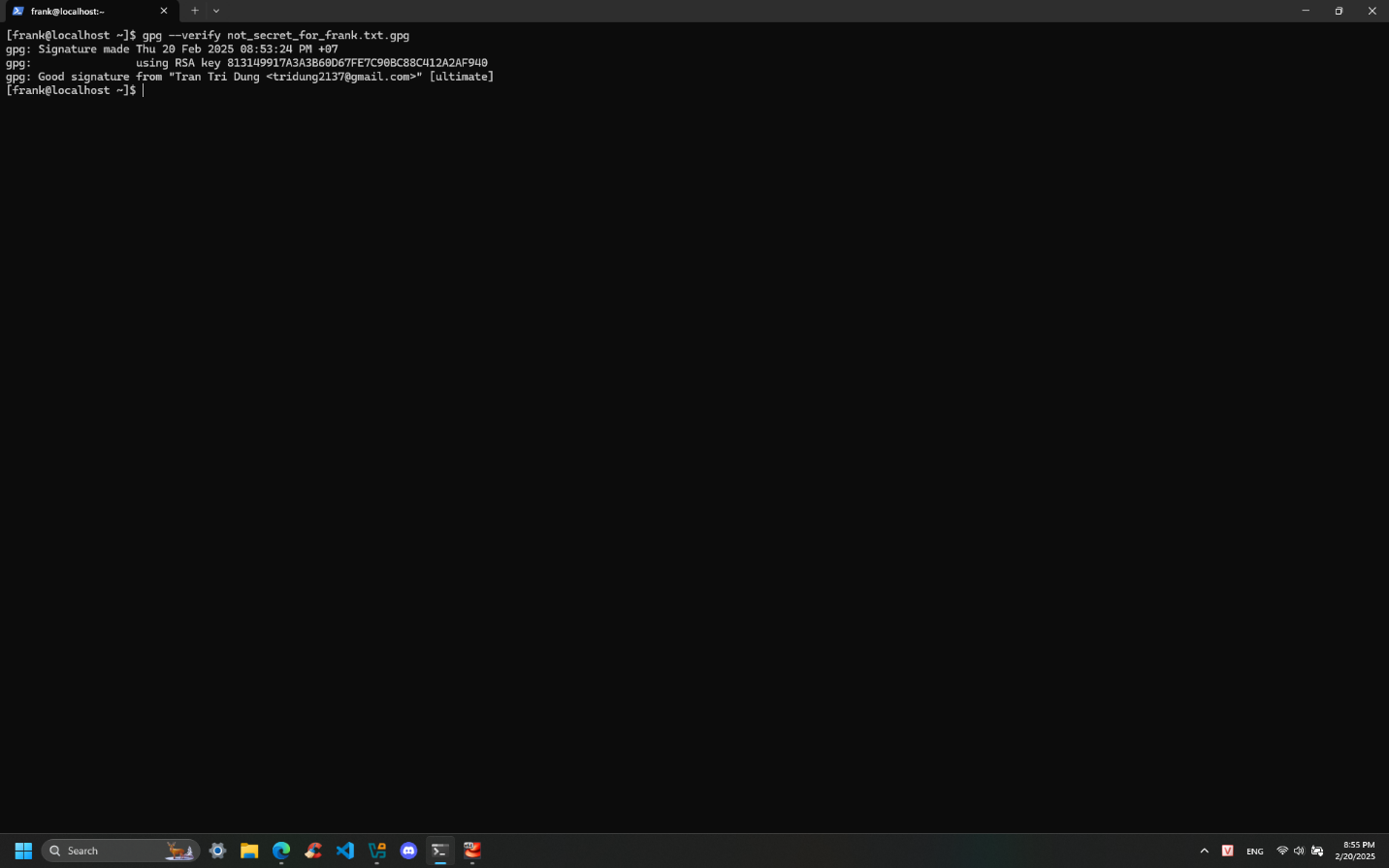
5.4 – Signing a file without encryption

Thông tin chữ ký:

* Thời gian ký: Thu 20 Feb 2025 08:53:24 PM +07
* Sử dụng khóa RSA: 813149917A3A3860D67FE7C90BC88C412A2AF949
* Chữ ký từ: "Tran Tri Dung <tridung2137@gmail.com>"
* Trạng thái: Good signature [ultimate] (chữ ký hợp lệ và được tin cậy hoàn toàn)

Điều này cho thấy:

* File không được mã hóa nhưng có chữ ký số để đảm bảo tính xác thực và toàn vẹn
* Chữ ký số được xác nhận là hợp lệ và đến từ người gửi đáng tin cậy (Tran Tri Dung)
* Việc xác minh chữ ký hoạt động chính xác, đảm bảo file không bị thay đổi kể từ khi được ký
* Không như lệnh -d trước đó, lệnh này không giải mã nội dung file mà chỉ xác minh chữ ký

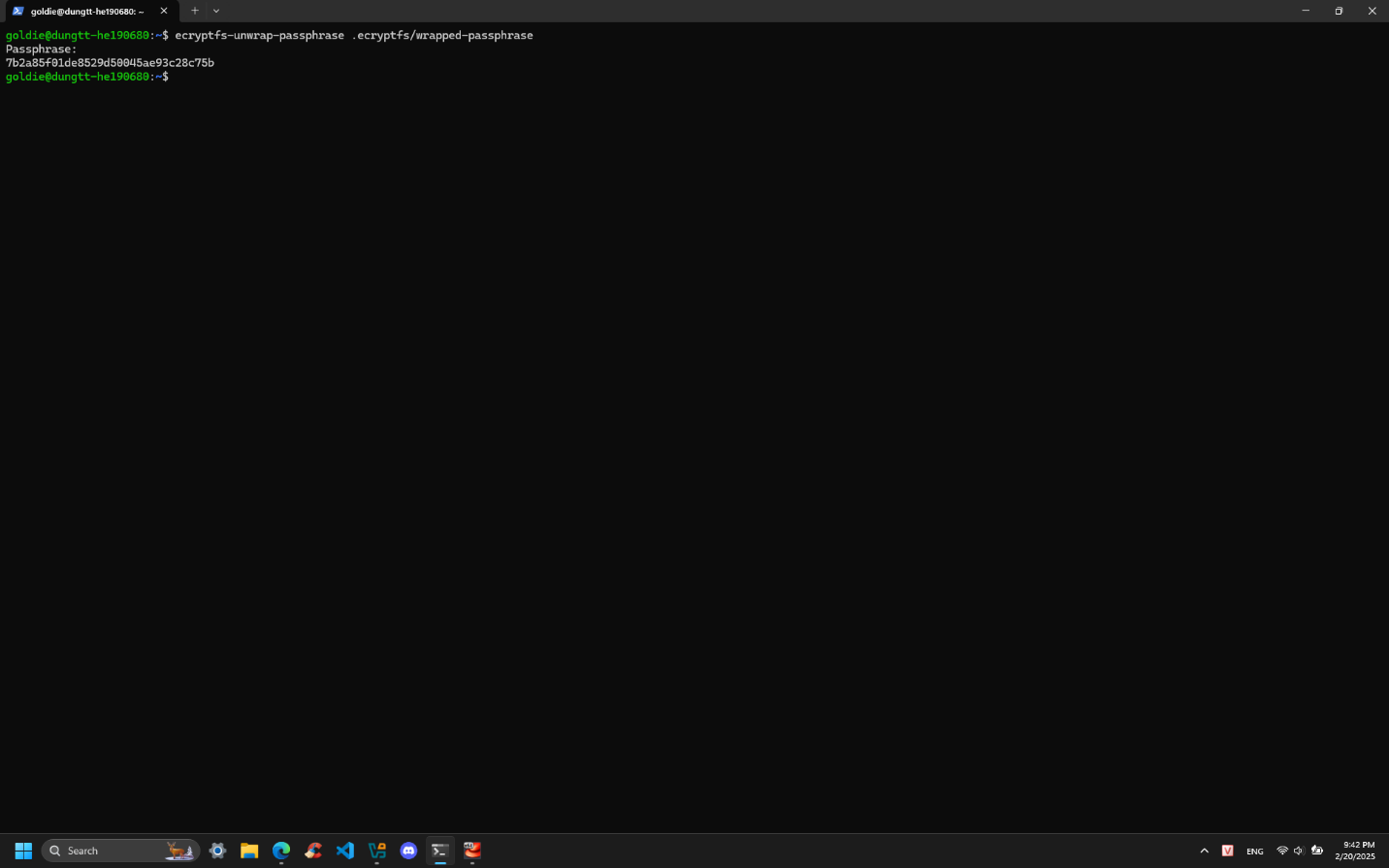


5.7 – Encrypting a home directory for a new user account

Kết quả hiển thị: Passphrase: 7b2a85f01de8529d50045ae93c28c75b

Đây là quá trình lấy passphrase được mã hóa (wrapped) cho thư mục mã hóa của người dùng Goldie:

* Lệnh ecryptfs-unwrap-passphrase được sử dụng để giải mã và hiển thị mount passphrase
* File .ecryptfs/wrapped-passphrase chứa passphrase được mã hóa
* Passphrase này được dùng để khôi phục dữ liệu nếu thư mục mã hóa bị hỏng, là chìa khóa để truy cập dữ liệu mã hóa trong thư mục home



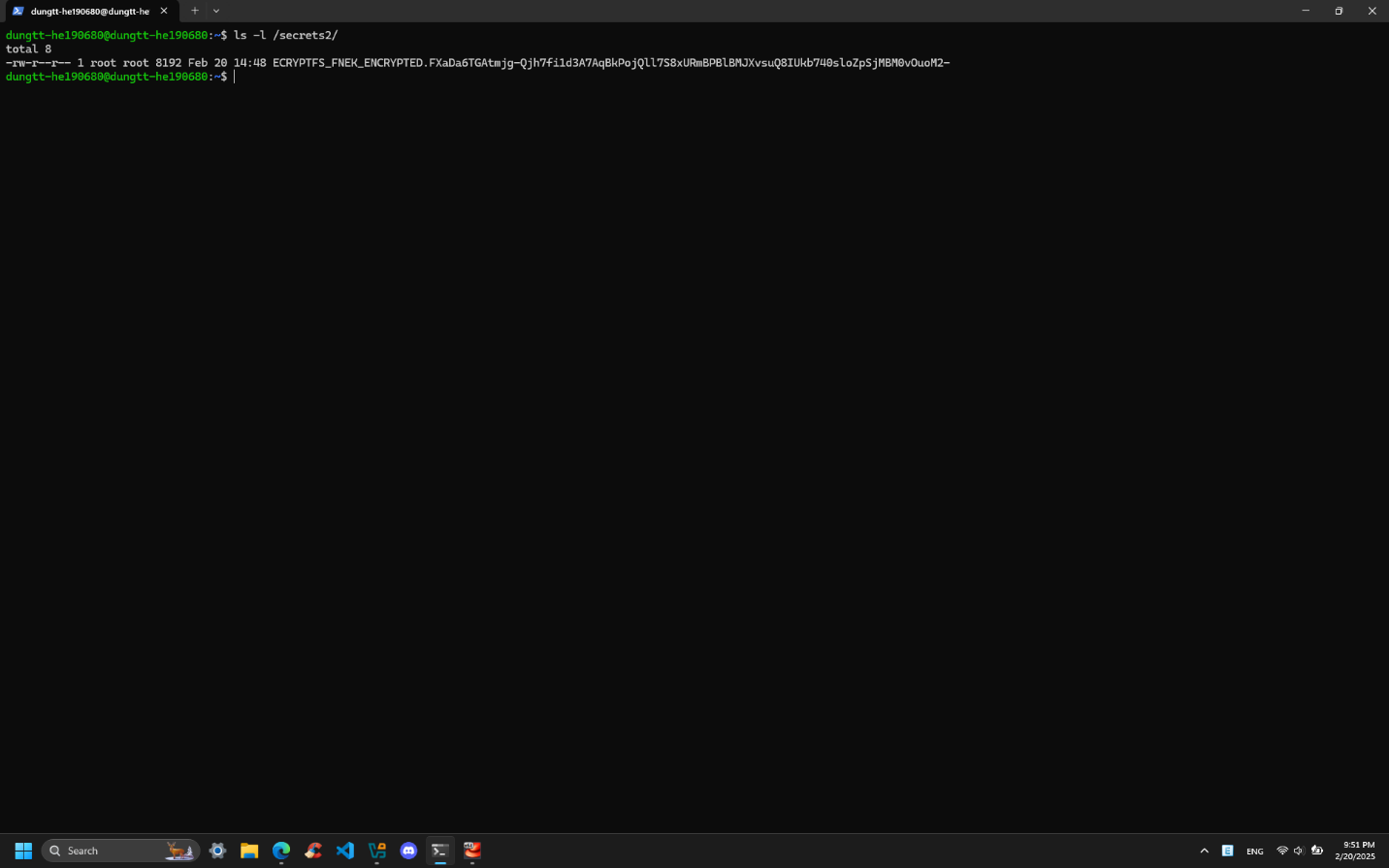
5.8 – Encrypting other directories with eCryptfs

Trạng thái thư mục:

* Thư mục /secrets2/ đang ở trạng thái unmounted
* Tên file được hiển thị ở dạng mã hóa (encrypted filename)
* Prefix "ECRYPTFS\_FNEK\_ENCRYPTED" cho biết đây là file được mã hóa bởi eCryptfs với tính năng mã hóa tên file (FNEK - Filename Encryption Key)

Tính năng bảo mật:

* Tên file được mã hóa hoàn toàn, không thể biết được tên file gốc
* Nội dung file cũng được mã hóa
* Cần mount thư mục với passphrase chính xác để xem được tên và nội dung file gốc



5.10 – Creating and mounting a VeraCrypt volume in console mode

Thông tin volume được mount:

* Đường dẫn container: /home/dungtt-he190680/good\_stuff
* Device mapper: /dev/mapper/veracrypt1
* Mount point: /home/dungtt-he190680/good\_stuff\_dir

Điều này cho thấy:

* Container VeraCrypt được tạo tại thư mục home của user dungtt-he190680
* Được mount thông qua device mapper của Linux
* Có thể truy cập nội dung đã giải mã tại thư mục good\_stuff\_dir
* Volume đang trong trạng thái mounted và sẵn sàng sử dụng
* Người dùng có thể truy cập và làm việc với dữ liệu đã được giải mã trong thư mục good\_stuff\_dir
* Khi không cần sử dụng nữa, có thể unmount volume để bảo vệ dữ liệu

