

Feb 11, 2026

Hands On Activity 3

Team 5 (pizza winning team 🍕 🍕) : Mathys Gouzènes, Alexis Rochefort, Rezaul Haque

USB Steganography Exercise - Recap

Files

File 1

An image (cockroach picture).

We manually edited it using Notepad and added a hidden message in the file:

"myboysaid:67" (flag)

The image still opens normally because PNG files ignore extra data appended at the end.

File 2 (new-york.jpg)

A (sadly corrupted) image, edited via Notepad, three randomly generated passwords:

- A
- B
- C

Files 3 to 6

These are normal image files used as **carriers**:

- File 3 - maxresdefault.jpg
- File 4 - spacedog.png
- File 5 - pizzawarfare.bmp
- File 6 - natureimage8k.bmp

We used **OpenPuff** to hide File 1 inside these images.

We enabled **decoy mode** during the process.

File 7 (Decoy Password) (password=password.txt)

File 7 name contains the fake password A used for the decoy extraction ("password"). This was intentionally placed to mislead someone into thinking they found the correct password. If they use it, they only recover fake data.

Steganography Setup

- **File 1 was embedded inside Files 3-6.**
- Passwords A, B, and C are required to extract the real hidden content.
- A decoy was also configured inside.

If someone tries extracting using fake password A, they will get decoy content instead of the real hidden file.

Folder Hiding

We used the Windows command:

attrib +h +s myfolder

This hides the folder from the normal view in File Explorer.

This method is only cosmetic. It does not provide real security, but it prevents casual users from immediately seeing the folder.

Final Structure on USB

```
|— myfolder (hidden)
|   |— maxresdefault.jpg
|   |— natureimage8k.bmp
|   |— pizzawarfare.bmp
|   |— spacedog.png
|— new-york.jpg
|— password=password.txt
```

Visible:

- File 2
- File 7

Hidden folder (*myfolder*):

- File 1
- Files 3-6