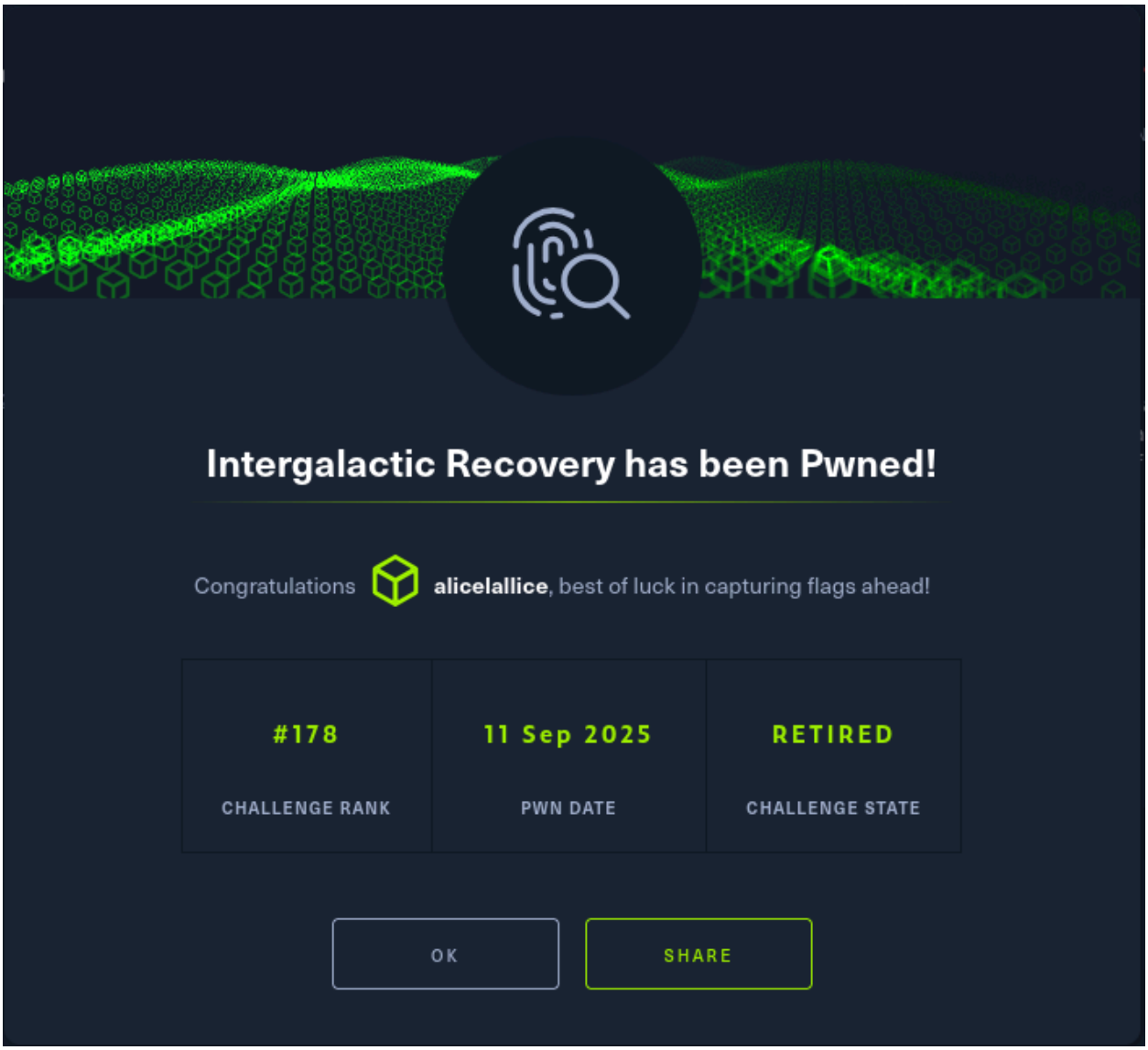
Intergalactic Recovery

Types	forensic
CTF	HTB



You’re handed three disk images from a degraded RAID 5 array. Your goal: reassemble the array, mount it read-only, and recover a hidden PDF — even if the

filesystem appears empty.

🔧 Step 1: Map the Loop Devices

bash

```
sudo losetup /dev/loop0 fef0d1cd.img
sudo losetup /dev/loop1 0c584923.img
sudo losetup /dev/loop2 06f98d35.img
```

> ⚠️ loop1 may throw a warning due to non-standard sector alignment — ignore it unless it blocks RAID creation.

Step 2: Zero Out Old RAID Metadata

bash

```
sudo mdadm --zero-superblock /dev/loop0
sudo mdadm --zero-superblock /dev/loop2
```

> Skip loop1 — it's only 3K and not usable.

🛠️ Step 3: Create a Degraded RAID Array

bash

```
sudo mdadm --create /dev/md0 --level=5 --raid-devices=3 /dev/loop0 missing /dev/loop2
```

Confirm with:

bash

```
cat /proc/mdstat
```

> Look for [U_U] — two active disks, one missing.

📂 Step 4: Mount the Array Read-Only

bash

```
sudo mkdir -p raid
sudo mount -o ro /dev/md0 raid/
ls -la raid/
```

> The filesystem may appear empty — time to pivot into raw carving.

🔍 Step 5: Locate PDF Signatures

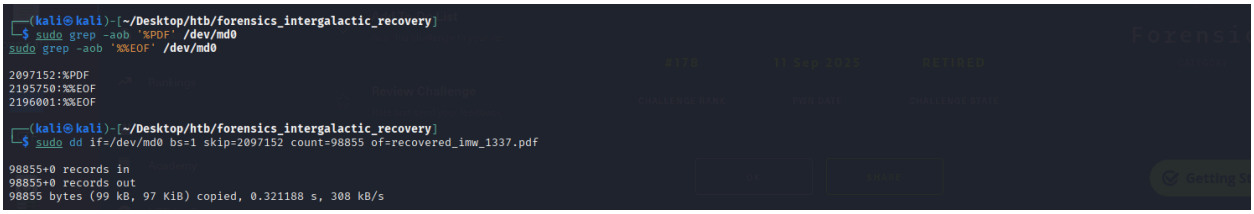
bash

```
sudo grep -aob '%PDF' /dev/md0
sudo grep -aob '%%EOF' /dev/md0
```

> Example output:

Code

```
%PDF at offset: 2097152
%%EOF at offset: 2196007
```



✂️ Step 6: Carve the PDF

bash

```
sudo dd if=/dev/md0 bs=1 skip=2097152 count=98855 of=recovered_imw_1337.pdf
```

> Adjust skip and count based on your actual offsets.

open the pdf and you will see the flag