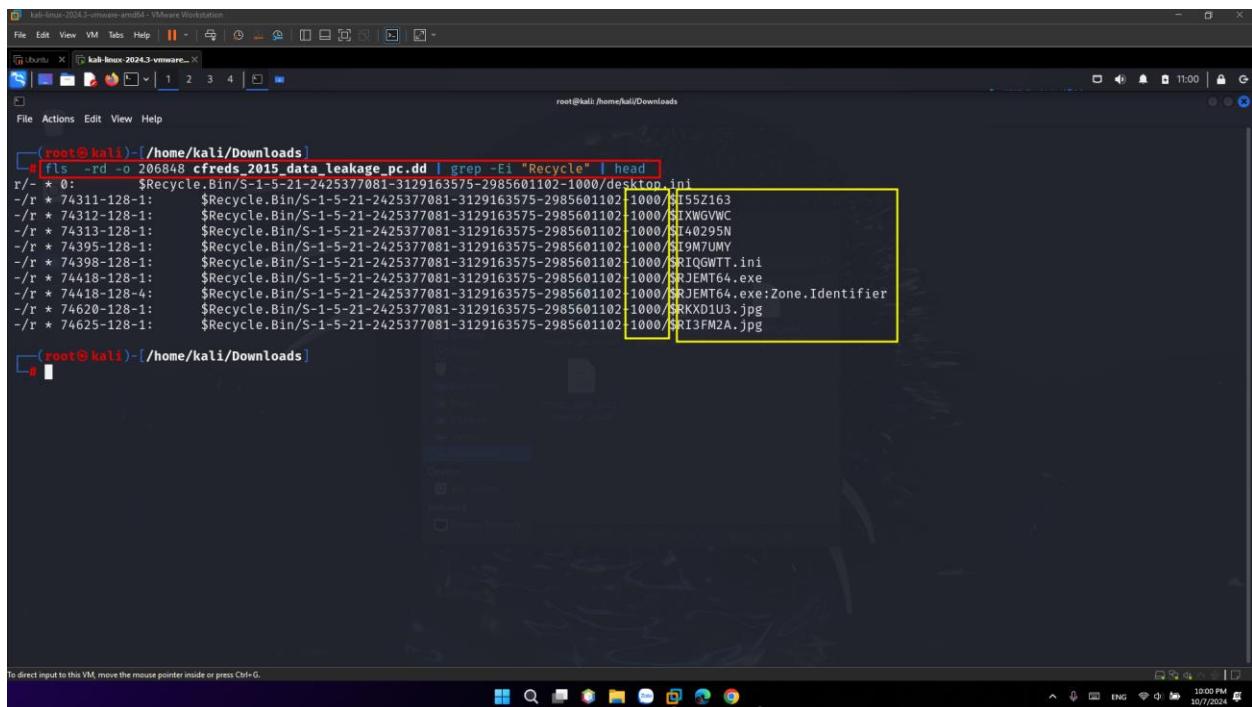


Lab 7: Recycle Bin and Anti-forensics

Group: CyberSec_N00b

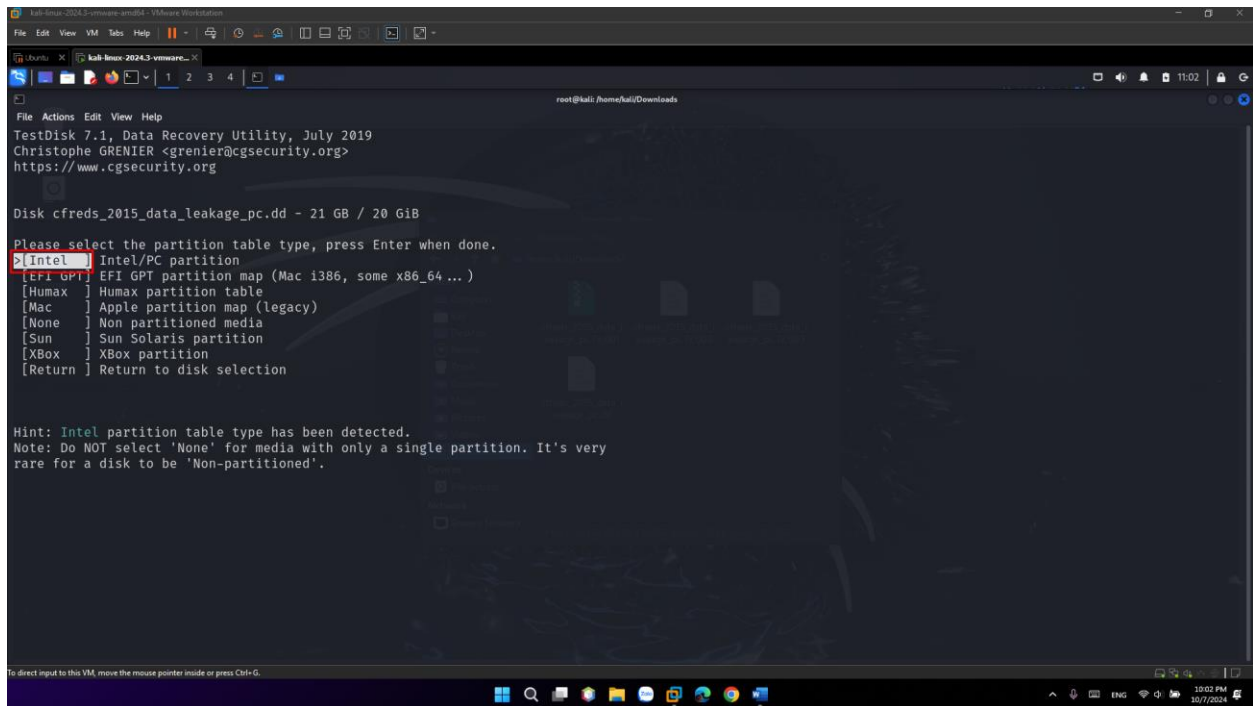
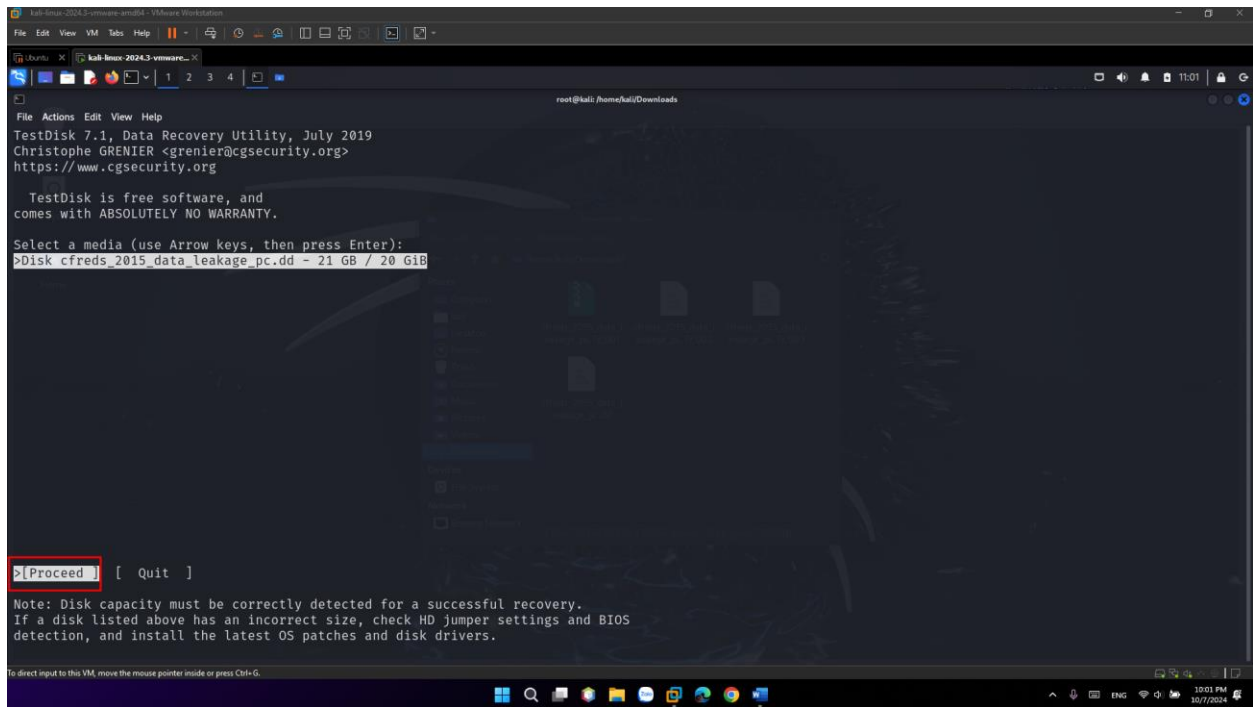
Member:

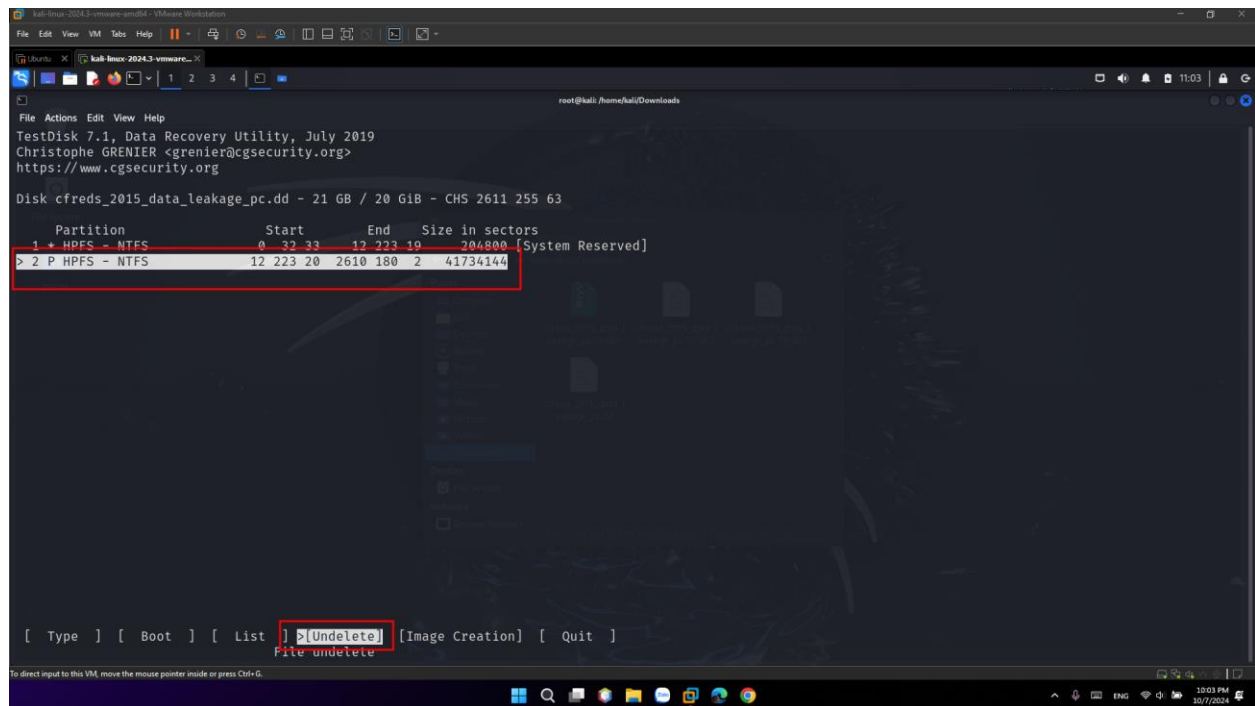
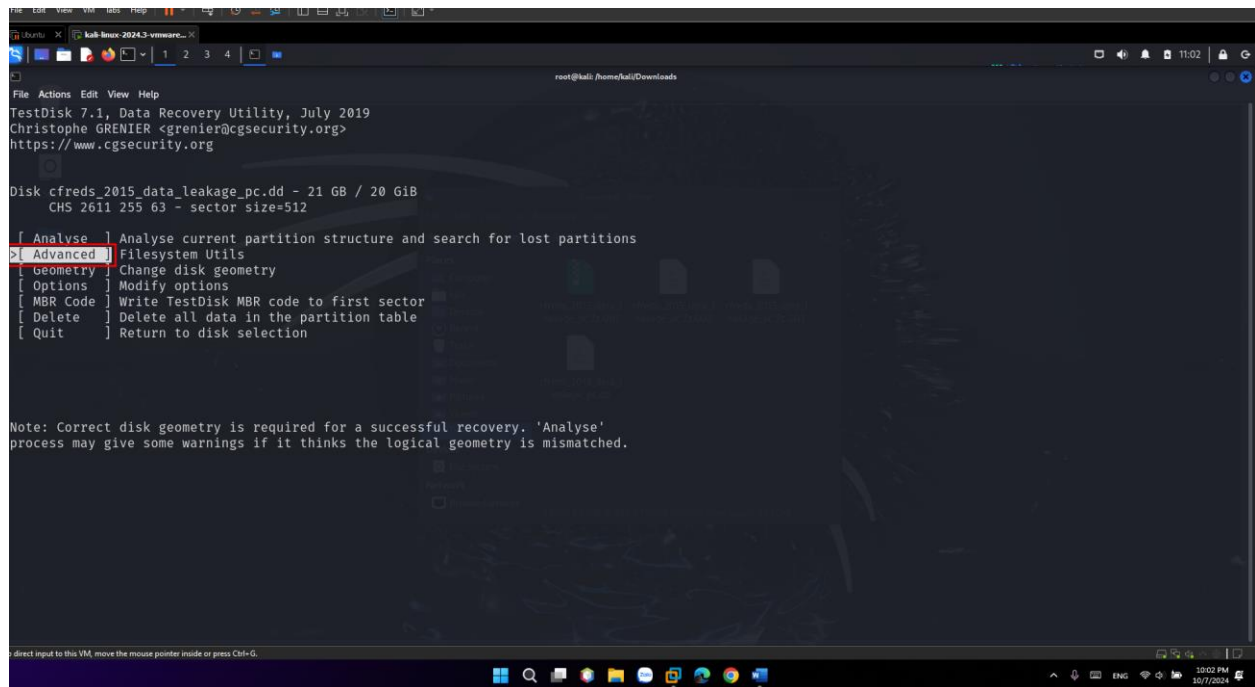
- Huỳnh Ngọc Quang (SE181838)
- Hồ Tài Liên Vy Kha (SE181818)
- Hoàng Kim Long (DE180860)
- Phạm Thành Long (SE181692)
- Nguyễn Lê Hoàng Thông (SE182533)



```
root@kali:~/Downloads
# find -r -d -o 206848 cfreds_2015_data_leakage_pc.dd | grep -Ei "Recycle" | head
r/- * 0: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/desktop.ini
-r * 74311-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SI552163
-r * 74312-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SIXWGVWC
-r * 74313-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SI40295N
-r * 74395-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SI9M7UMY
-r * 74398-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SRIQWTT.ini
-r * 74418-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SRJEMT64.exe
-r * 74418-128-4: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SRJEMT64.exe:Zone.Identifier
-r * 74620-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SRKXD1U3.jpg
-r * 74625-128-1: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/SRI3FM2A.jpg

root@kali:~/Downloads
```





```
kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali: ~/Downloads

(kali@kali)~/Downloads
$ ls S-1-5-21-2425377081-3129163575-2985601102-1000 -l
total 64
-rw-r--r-- 1 root root 544 Mar 24 2015 '$I40295N'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$I508CBB.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$I55Z163'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$I8YP3XK.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$I9M7UMY'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$I00I3HE.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$IFVCH5V.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$II3FH2A.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$IIQGWTT.ini'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$IJEMT64.exe'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$IXKD1U3.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$IU3FKWI.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$IX538VH.jpg'
-rw-r--r-- 1 root root 544 Mar 24 2015 '$IXWGVWC'
-rw-r--r-- 1 root root 174 Mar 24 2015 '$RIQGWTT.ini'
-rw-r--r-- 1 root root 26 Dec 13 1901 '$RJEMT64.exe:Zone.Identifier'

(kali@kali)~/Downloads
$
```

```
kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali: ~/Downloads

(kali@kali)~/Downloads
$ strings -h
Usage: strings [option(s)] [file(s)]
Display printable strings in [file(s)] (stdin by default)
The options are:
-a --all Scan the entire file, not just the data section [default]
-d --data Only scan the data sections in the file
-f --print-file-name Print the name of the file before each string
-n <number> Locate & print any sequence of at least <number>
displayable characters. (The default is 4).
-t --radix={o,d,x} Print the location of the string in base 8, 10 or 16
-w --include-all-whitespace Include all whitespace as valid string characters
-o An alias for --radix=o
-T --target=<BFDNAME> Specify the binary file format
-e --encoding={s,S,b,l,B,L} Select character size and endianness:
s = 7-bit, S = 8-bit, {b,l} = 16-bit, {B,L} = 32-bit
--unicode={default|show|invalid|hex|escape|highlight}
-U {a|s|l|x|h} Specify how to treat UTF-8 encoded unicode characters
-s --output-separator=<string> String used to separate strings in output.
@<file> Read options from <file>
-h --help Display this information
-v --version Print the program's version number
strings: supported targets: elf64-x86-64 elf32-i386 elf32-iamcu elf32-x86-64 pei-i386 pe-x86-64 pei-x86-64 elf64-little elf64-big elf32-little elf32-big pe-i386 pe-x86-64 pe-i386 pdb srec symbolsrec verilog tekhex binary ihex plugin
Report bugs to <https://sourceware.org/bugzilla/>

(kali@kali)~/Downloads
$ strings -e -f S-1-5-21-2425377081-3129163575-2985601102-1000/$I508CBB.jpg
S-1-5-21-2425377081-3129163575-2985601102-1000/$I508CBB.jpg: C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg

(kali@kali)~/Downloads
$
```