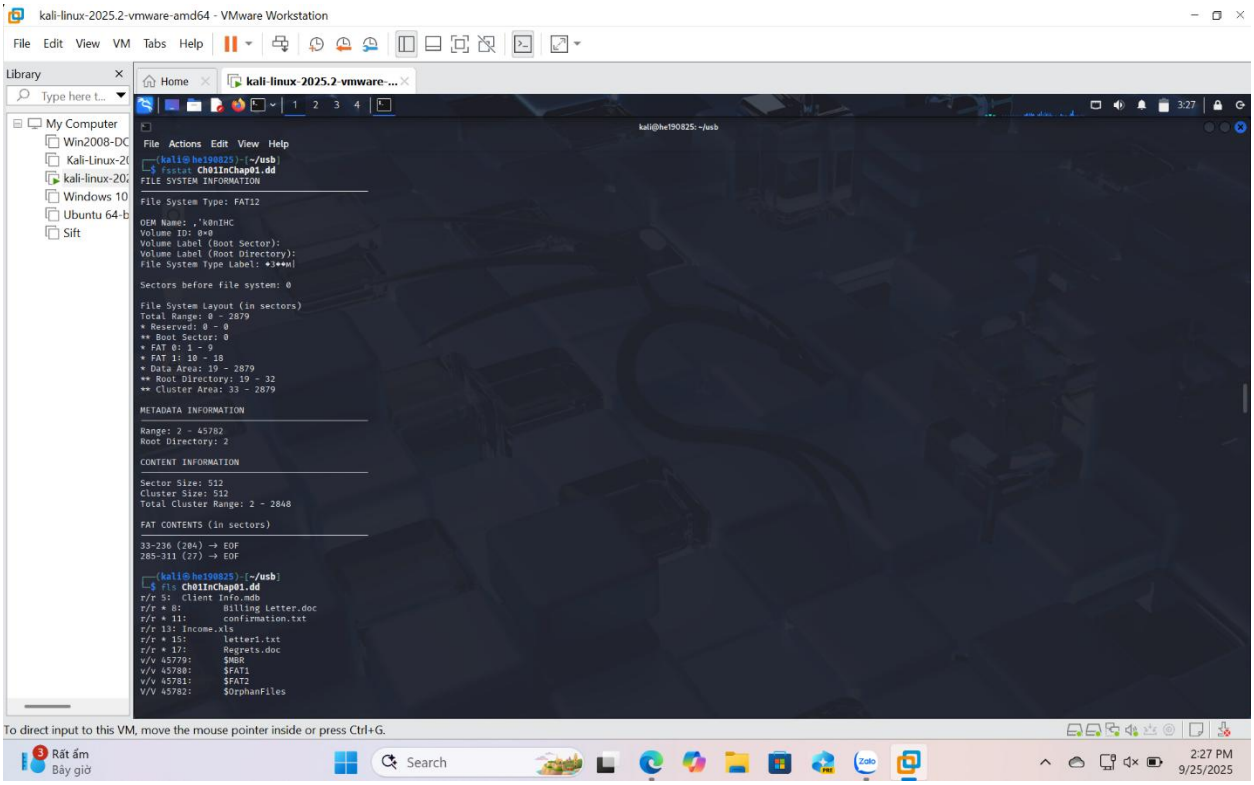
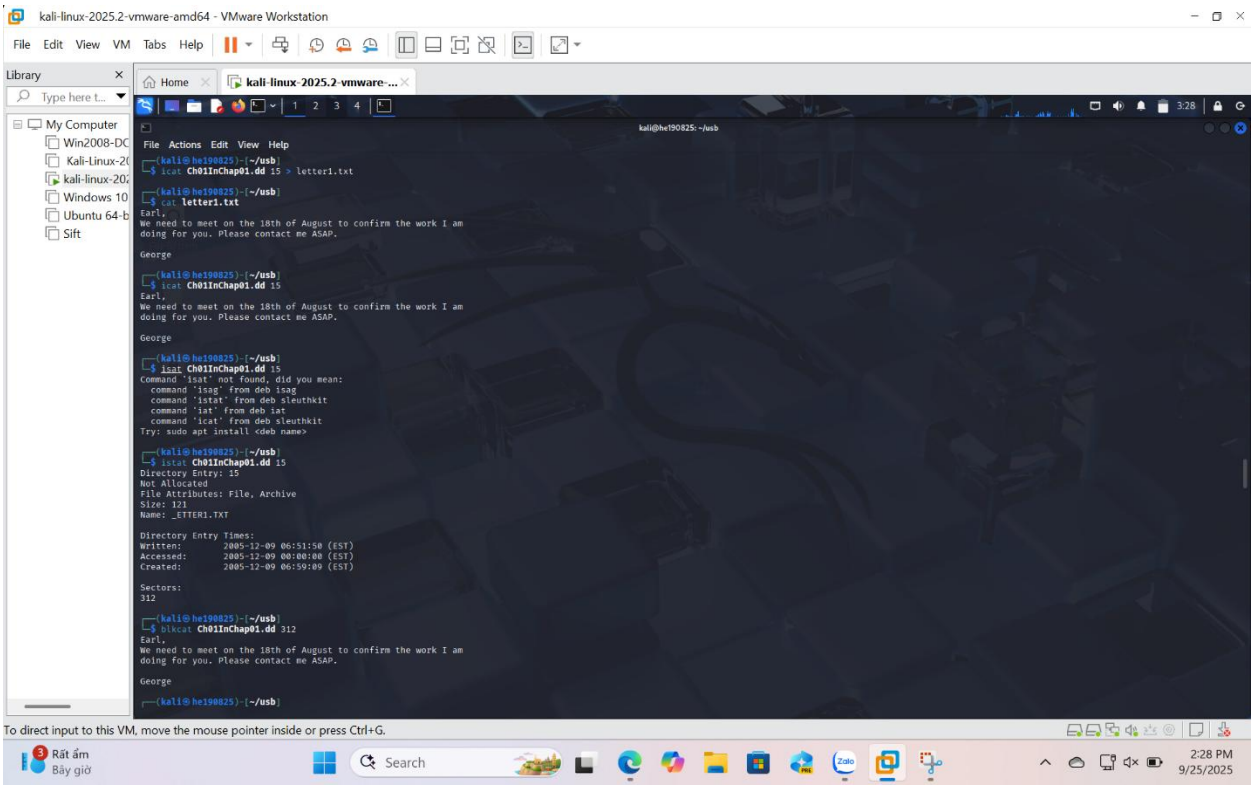
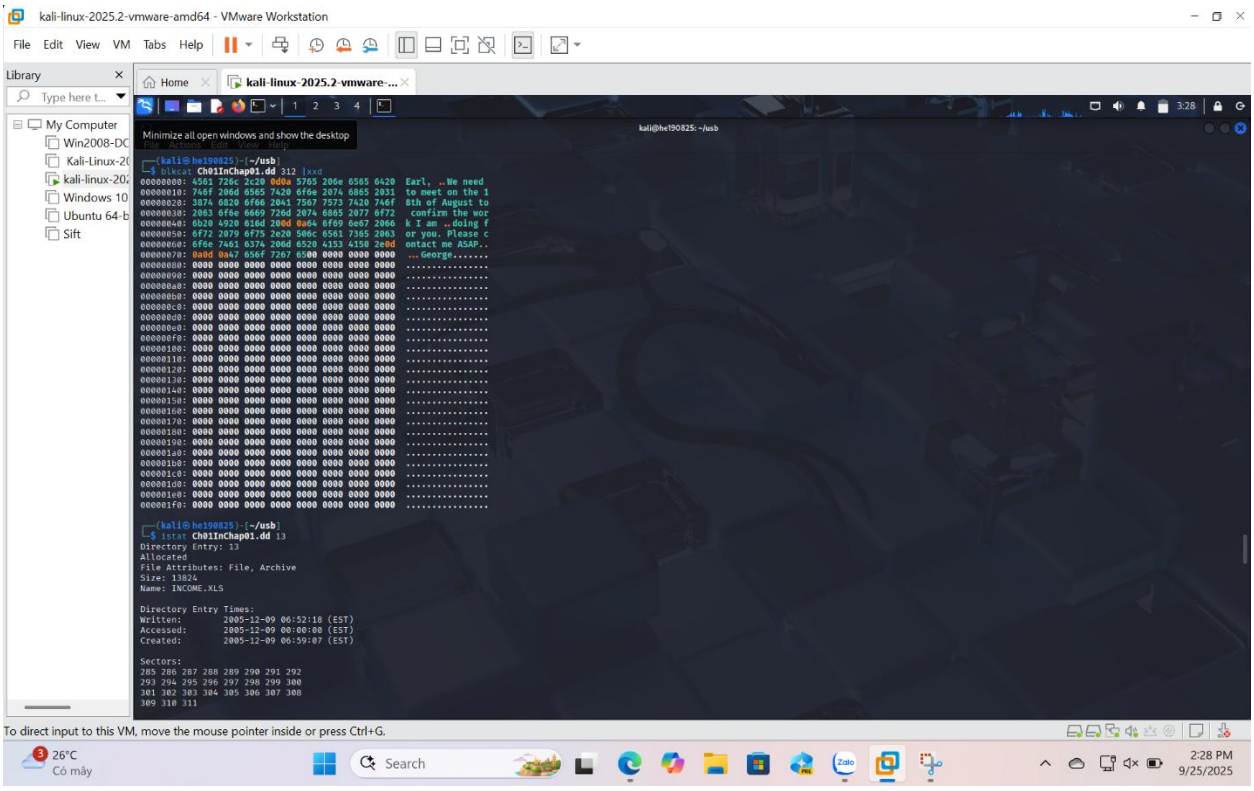
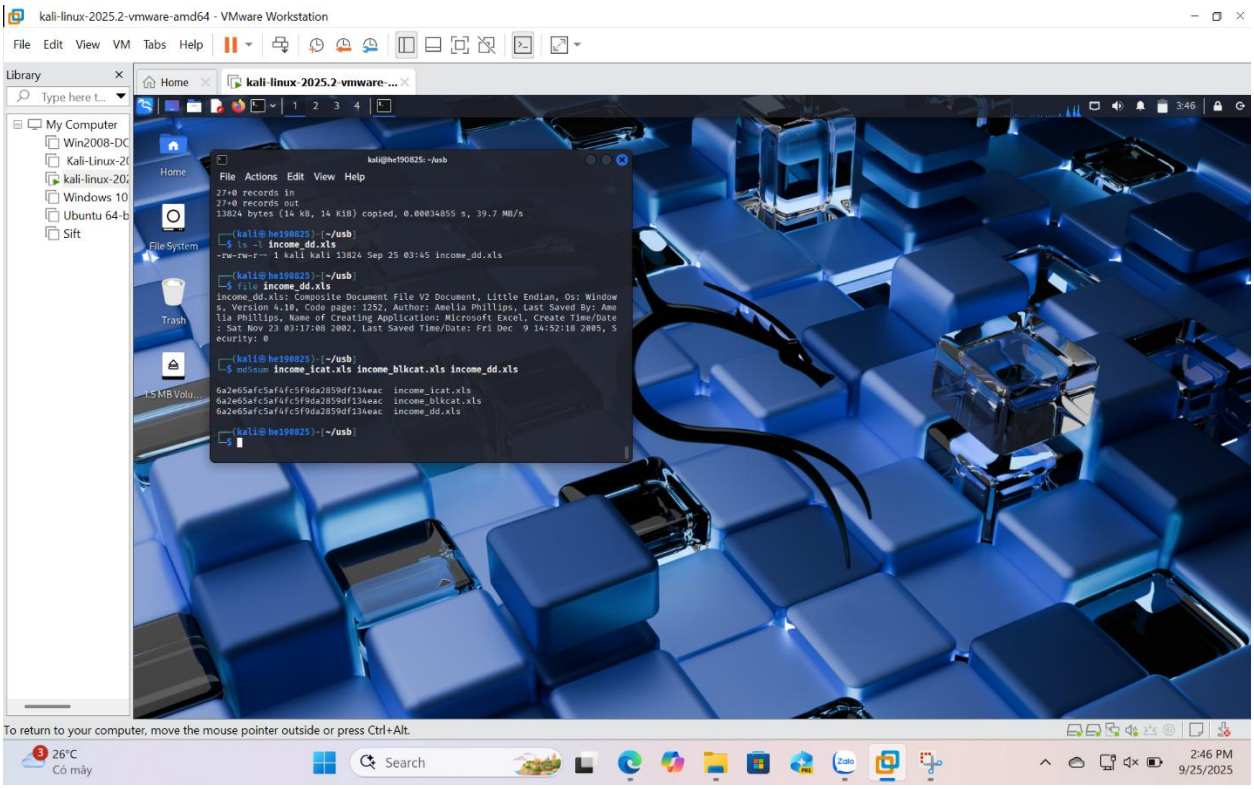
BÁO CÁO LAB 4-FRS

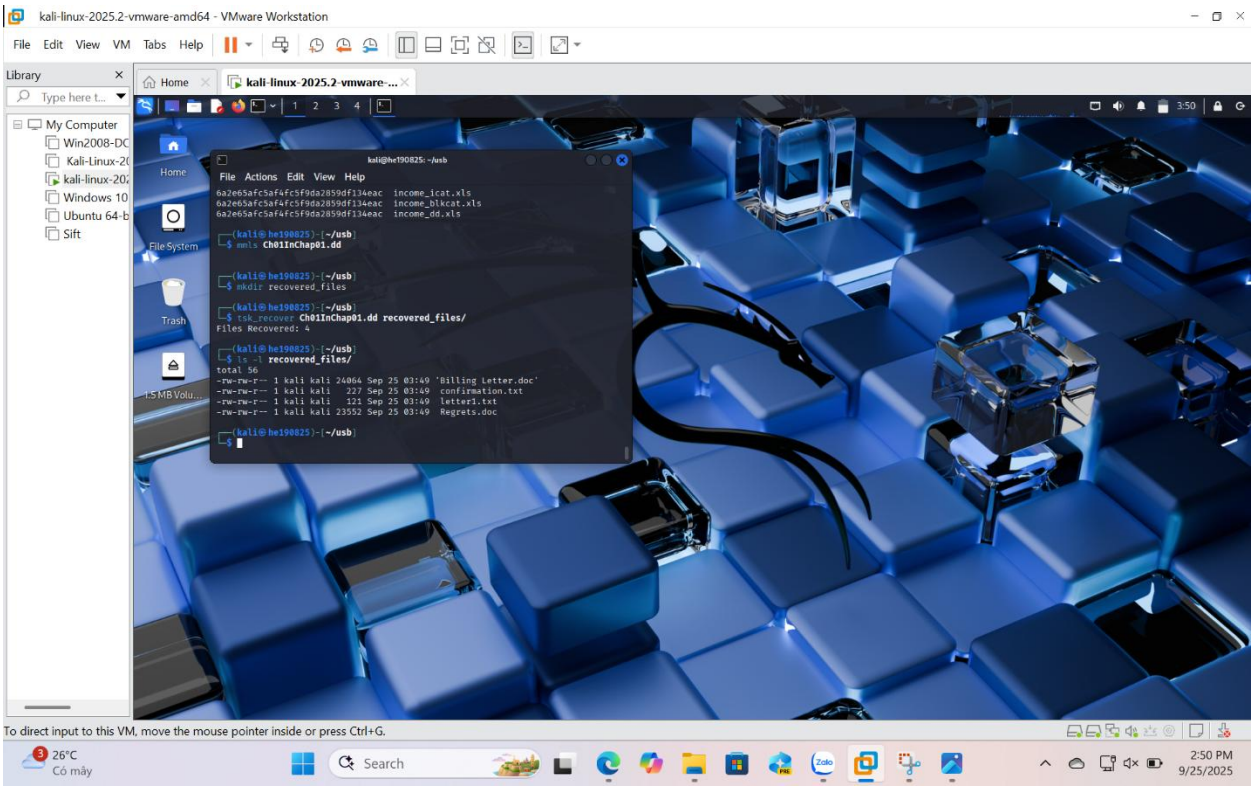
Họ và tên: Hoàng Đình Lâm
MSSV: He190825
Lớp: IA1905




kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-20
kali-linux-202
Windows 10
Ubuntu 64-b
Sift
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/usb
File Actions Edit View Help
(kali㉿he190825)-[~/usb]
$ icat Ch01InChap01.dd 15 > letter1.txt
$ cat letter1.txt
Earl,
We need to meet on the 18th of August to confirm the work I am
doing for you. Please contact me ASAP.
George
$ icat Ch01InChap01.dd 15
$ isat Ch01InChap01.dd 15
Command 'isat' not found, did you mean:
command 'isag' from deb isag
command 'istat' from deb sleuthkit
command 'iat' from deb iat
command 'icat' from deb sleuthkit
Try: sudo apt install <deb name>
$ istat Ch01InChap01.dd 15
Directory Entry: 15
Not Allocated
File Attributes: File, Archive
Size: 121
Name: _ETTER1.TXT
Directory Entry Times:
Written: 2005-12-09 06:51:50 (EST)
Accessed: 2005-12-09 00:00:00 (EST)
Created: 2005-12-09 06:59:09 (EST)
Sectors:
312
$ blkcat Ch01InChap01.dd 312
Earl,
We need to meet on the 18th of August to confirm the work I am
doing for you. Please contact me ASAP.
George
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
2:28 PM
9/25/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
Kali-Linux-20
kali-linux-202
Windows 10
Ubuntu 64-b
Sift
Home
kali-linux-2025.2-vmware-...
Minimize all open windows and show the desktop
kali@he190825: ~/usb
$ blkcat Ch01InChap01.dd 312 |xxd
00000000: 4561 726c 2c20 0d0a 5765 206e 6565 6420 Earl, ..We need
00000010: 746f 206d 6565 7420 6f6e 2074 6865 2031 to meet on the 1
00000020: 3874 6820 6f66 2041 7567 7573 7420 746f 8th of August to
00000030: 2063 6f6e 6669 726d 2074 6865 2077 6f72 confirm the wor
00000040: 6b20 4920 616d 200d 0a64 6f69 6e67 2066 k I am ..doing f
00000050: 6f72 2079 6f75 2e20 506c 6561 7365 2063 or you. Please c
00000060: 6f6e 7461 6374 206d 6520 4153 4150 2e0d ontact me ASAP..
00000070: 0a0d 0a47 656f 7267 6500 0000 0000 0000 ...George.....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000100: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000110: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000120: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000130: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000140: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000150: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000160: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000170: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000190: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001b0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001c0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001d0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001f0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
$ istat Ch01InChap01.dd 13
Directory Entry: 13
Allocated
File Attributes: File, Archive
Size: 13824
Name: INCOME.XLS
Directory Entry Times:
Written: 2005-12-09 06:52:18 (EST)
Accessed: 2005-12-09 00:00:00 (EST)
Created: 2005-12-09 06:59:07 (EST)
Sectors:
285 286 287 288 289 290 291 292
293 294 295 296 297 298 299 300
301 302 303 304 305 306 307 308
309 310 311
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Có mây
Search
2:28 PM
9/25/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-20
kali-linux-202
Windows 10
Ubuntu 64-b
Sift
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/usb
File Actions Edit View Help
27+0 records in
27+0 records out
13824 bytes (14 kB, 14 KiB) copied, 0.00034855 s, 39.7 MB/s
(kali㉿he190825)-[~/usb]
$ ls -l income_dd.xls
-rw-rw-r-- 1 kali kali 13824 Sep 25 03:45 income_dd.xls
(kali㉿he190825)-[~/usb]
$ file income_dd.xls
income_dd.xls: Composite Document File V2 Document, Little Endian, Os: Windows, Version 4.10, Code page: 1252, Author: Amelia Phillips, Last Saved By: Amelia Phillips, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Nov 23 03:17:08 2002, Last Saved Time/Date: Fri Dec 9 14:52:18 2005, Security: 0
(kali㉿he190825)-[~/usb]
$ md5sum income_icat.xls income_blkcat.xls income_dd.xls
6a2e65afc5af4fc5f9da2859df134eac income_icat.xls
6a2e65afc5af4fc5f9da2859df134eac income_blkcat.xls
6a2e65afc5af4fc5f9da2859df134eac income_dd.xls
(kali㉿he190825)-[~/usb]
$
File System
Trash
1.5 MB Volu...
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
26°C
Có mây
Search
2:46 PM
9/25/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-20
kali-linux-202
Windows 10
Ubuntu 64-b
Sift
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/usb
File Actions Edit View Help
6a2e65afc5af4fc5f9da2859df134eac income_icat.xls
6a2e65afc5af4fc5f9da2859df134eac income_blkcat.xls
6a2e65afc5af4fc5f9da2859df134eac income_dd.xls
(kali㉿he190825)-[~/usb]
$ mmls Ch01InChap01.dd
(kali㉿he190825)-[~/usb]
$ mkdir recovered_files
(kali㉿he190825)-[~/usb]
$ tsk_recover Ch01InChap01.dd recovered_files/
Files Recovered: 4
(kali㉿he190825)-[~/usb]
$ ls -l recovered_files/
total 56
-rw-rw-r-- 1 kali kali 24064 Sep 25 03:49 'Billing Letter.doc'
-rw-rw-r-- 1 kali kali 227 Sep 25 03:49 confirmation.txt
-rw-rw-r-- 1 kali kali 121 Sep 25 03:49 letter1.txt
-rw-rw-r-- 1 kali kali 23552 Sep 25 03:49 Regrets.doc
(kali㉿he190825)-[~/usb]
$
File System
Trash
1.5 MB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Có mây
Search
2:50 PM
9/25/2025