Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Leandro Delgado	114416241	As Posted	6%

Name	Lab2

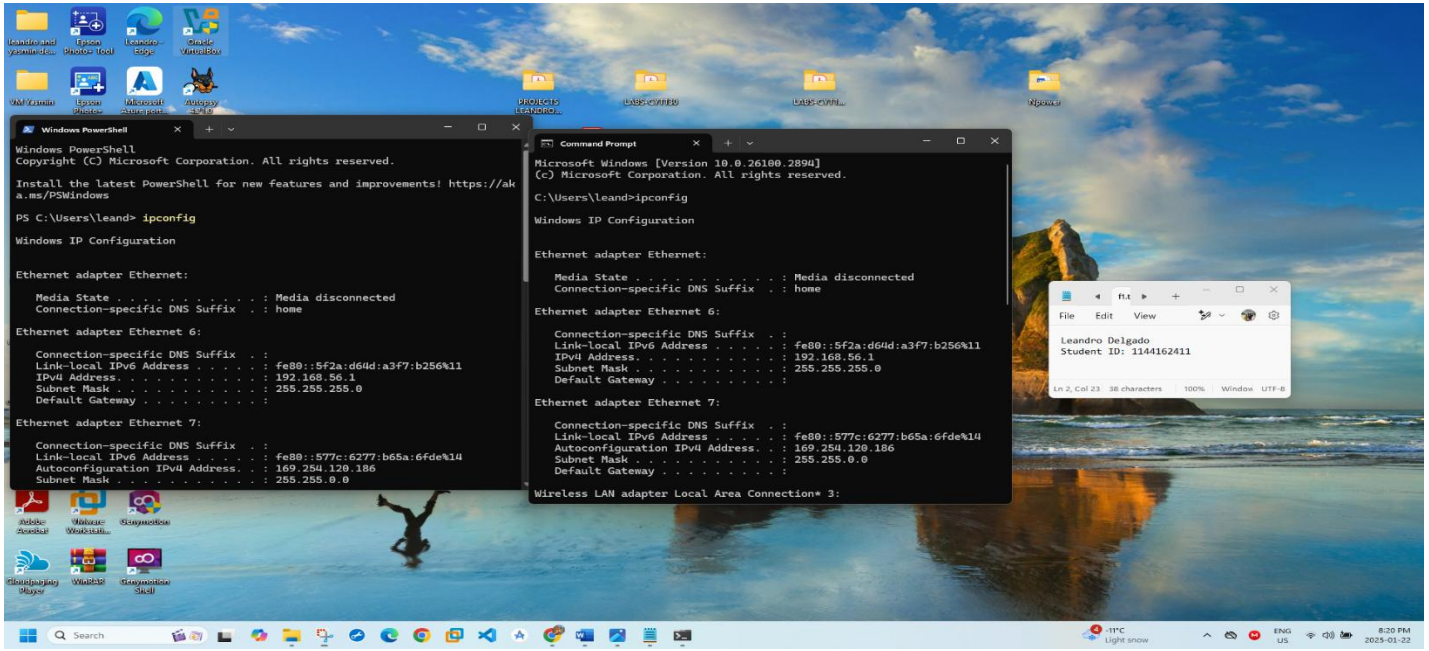
Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above.
	• Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.
	• Attach the main screenshots of your work performed and write your own analysis & findings of your activities.
	• Include Links & References, if applicable
	• Show your genuine signs of your work is done on your machine. This includes:
	  ○ Screenshots that show your desktop background with Date/Time
	  ○ Show a pop-up bx that shows "your name + Student ID"
	  ○ Show your logged account when applicable.
	  ○ Optional: Your photo.
	• Submit your report name: CYT215-Lab1-Student Name & ID

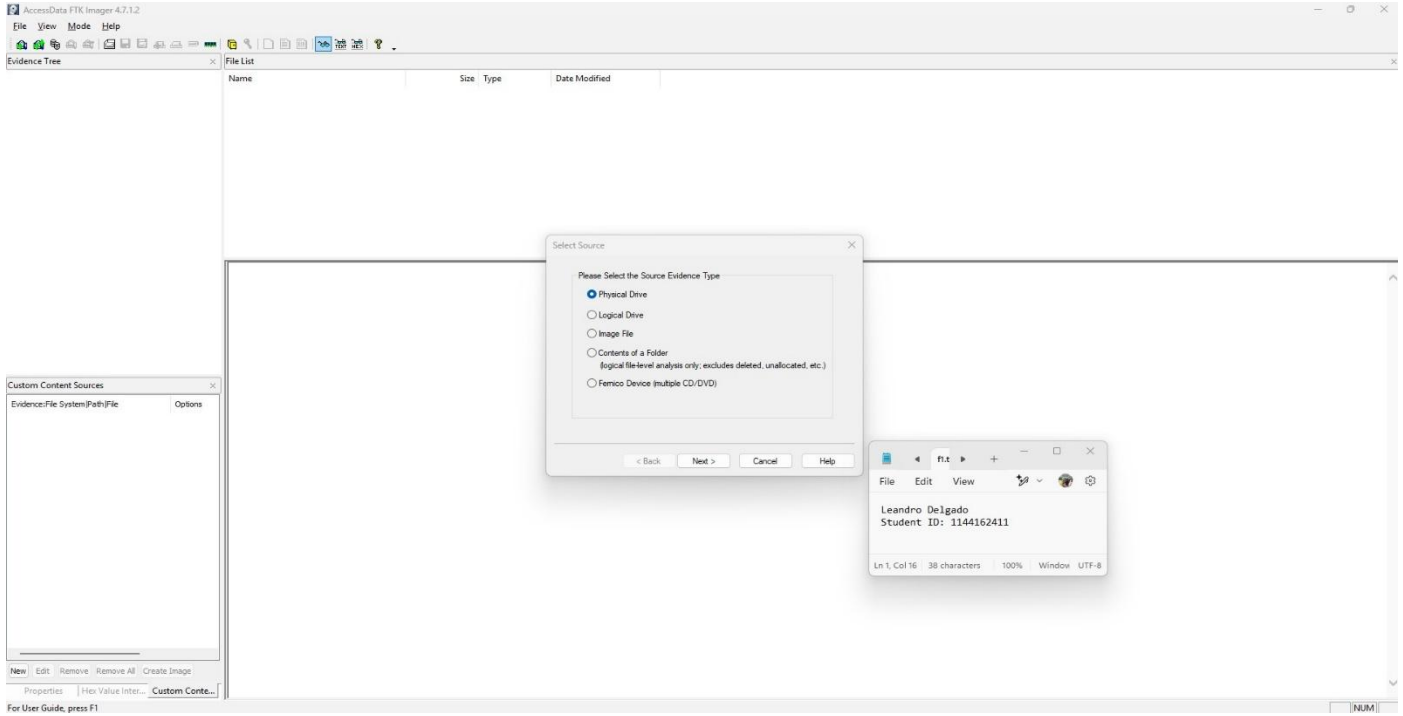
Students Work
 	
Activity 1
	• Go to Read https://www.hackingarticles.in/multiple-ways-to-create-image-file-for-forensics-investigation/. You will see that there are 4 popular relevant tools:
	  1. FTK Imager
	  2. Belkasoft Acquisition Tool
	  3. Encase Imager
	  4. Forensic Imager
	• Download & install any 2 tools (upon your wish) for example the following 2 tools:
	  1. FTK Imager https://www.exterro.com/ftk-imager
	  2. Forensic imager https://getdataforensics.com/product/fex-imager/
	• Make disk image of your machine using your chosen 2 tools, i.e. A disk image for every tool (The image is typically mounted by or 'loaded into' forensics software, such as FTK Imager, for analysis which usually involves searching various areas on the disk for evidence of malicious activity or presence of malware.)
	• Take screenshots of your works.
	• Keep your images for future coming labs.
	• Briefly write your experience and answer the following.:
	  ○ Which tool you found is good & easy to use?

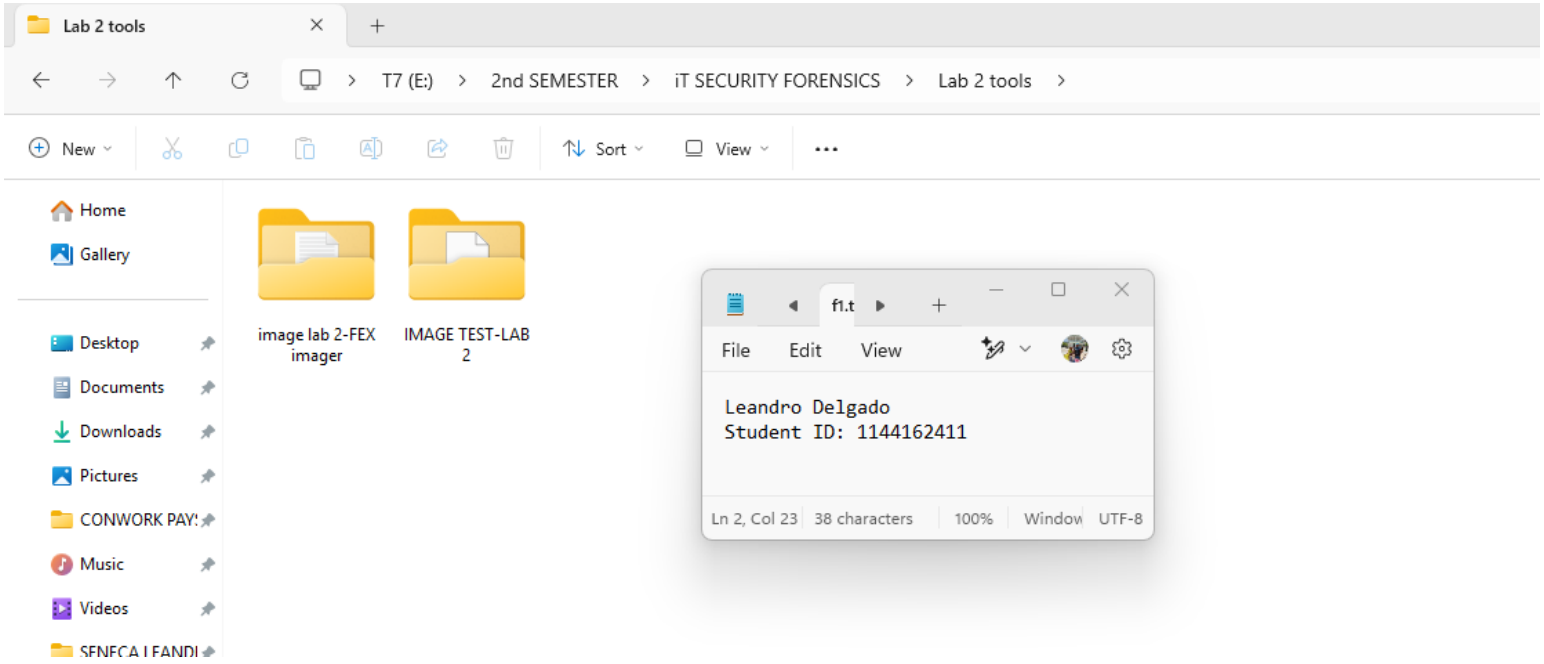
0	Introduction: It's important to setup your case files in an organized and consistent manner. Not long into an investigation you'll be dealing with large numbers of files, and it can be easy to lose track of what you've done and what your next steps are. An organized folder layout will help control the growing complexity of your case. In this next lab you will setup your workspace inside the SIFT virtual machine and re-familiarize yourself with some simple Linux commands. If you do not have a copy of SIFT or a copy of VMWare Player installed, you will need to get/install those before continuing with this lab. Please refer to following link for more information. https://digital-forensics.sans.org/community/downloads One thing to always keep in mind when working through these labs, whenever possible try to write a script to execute your commands rather than typing them every time. This allows others to repeat your process and hopefully produce the same results, in fact an accurate repeatable process is a keystone of good forensic analysis. It can also allow you to recreate your work product should you accidentally loose it due to a processing error. There are a number of" cheat sheets" available that document common processes in the SIFT virtual machine. They are available through the SIFT download site at http://computer-forensics.sans.org/community/downloads. Tools and Utilities: The following list of Linux command line tools are used or referenced in this tutorial. As a reminder, most Linux command line tools have man page documentation. Simply type man followed by the name of the tool to read the documentation. • mkdir - For creating directories. • ln - For creating shortcuts. • tree - For displaying your working directory tree. • cp - For copying files. • dc3dd - For creating forensic bit-stream images of devices. • mount - For mounting imaged devices for processing. • sudo - For performing commands as the super-user. • file - For determining what general type of category a file belongs to. • egrep - For searching through text data for specific patterns. • cut - For cutting/pasting columns of text output as a result of a Linux command. • losetup - For configuring loop devices.

	• mmls - Assists in determining the partition layout of a volume. Helpful when looking for the starting sector of various file systems. A quick note before we begin, variable names are used throughout this tutorial to demonstrate general patterns for commands. You should replace any italicized variable names with real values. Ex. tree -d directory name could be changed to tree -d /home/user/Desktop/cases/CYT215-2023-0001 Login 1. Start VMWare and load the SIFT virtual machine. 2. Ensure that sharing has been enabled between the host and guest operating system so that you can transfer files to and from your image. These settings are located under: " Edit virtual machine settings" ->" Options" ->" Shared Folders". 3. Start the SIFT virtual machine in VMWare. 4. Login using username sansforensics and password forensics. 1. Open a command terminal and navigate to the sansforensics user's Desktop/cases directory. 2. Create the directory tree shown below using the mkdir command. This structure suits itself well to a case with a single custodian. A custodian is an entity (ex. a person, server, department, company) that was in possession of some ESI at the time it was seized. If the case contains multiple custodians, additional folders for organizing data on a per custodian basis should be added. The parenthesized text beside the folder names is for documentation only and should not be part of the folder name. Notice the lack of spaces in the directory names. While they are supported, working with spaces in Linux filenames is difficult and prone to error. |-- CYT215-2024-0001 (Case number) | |-- admin | |-- coc (Chain of Custody Documents) | |-- databases (For databases generated during or used in analysis) | |-- dec (Digital Evidence Collection Documents) | |-- keywords (Keyword lists and other search parameters) | |-- logs (For any program output and reports) | `-- scripts (For scripts you write during your processing)
	--

	email |-- dd (Email with duplicates removed, DeDuplicated) |-- kwf (Filtered email, KeyWord Filtered) `-- raw (Raw extracted email data from your images) |  |--  files |  |-- dd (File data with duplicates removed) |  |-- kwf (Filtered files) |  `-- raw (Raw extracted file data) | |-- images (Image files) You can generate the hierarchical view above by using the tree -d directory name command. Your deliverable for this part of lab is the screenshot showing the output of the tree command which shows your whole case folder structure.
Grading Alerts	• Use the provided template • Show your account real name • Show your machine desktop background (with date & time) • Write in your own words and do not copy from other resources


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\leand> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : home
Ethernet adapter Ethernet 6:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5f2a:d64d:a3f7:b256%11
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter Ethernet 7:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::577c:6277:b65a:6fde%14
Autoconfiguration IPv4 Address. . : 169.254.120.186
Subnet Mask . . . . . : 255.255.0.0
Command Prompt
Microsoft Windows [Version 10.0.26100.2894]
(c) Microsoft Corporation. All rights reserved.
C:\Users\leand>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : home
Ethernet adapter Ethernet 6:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5f2a:d64d:a3f7:b256%11
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter Ethernet 7:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::577c:6277:b65a:6fde%14
Autoconfiguration IPv4 Address. . : 169.254.120.186
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 3:
File Edit View
Leandro Delgado
Student ID: 1144162411


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1
NUM
File Edit View
Leandro Delgado
Student ID: 1144162411


Lab 2 tools
T7 (E:) > 2nd SEMESTER > iT SECURITY FORENSICS > Lab 2 tools >
New
Sort
View
Home
Gallery
Desktop
Documents
Downloads
Pictures
CONWORK PAY!
Music
Videos
SENECA LEANDI
image lab 2-FEX imager
IMAGE TEST-LAB 2
f1.t
File
Edit
View
Leandro Delgado
Student ID: 1144162411
Ln 2, Col 23
38 characters
100%
Window
UTF-8

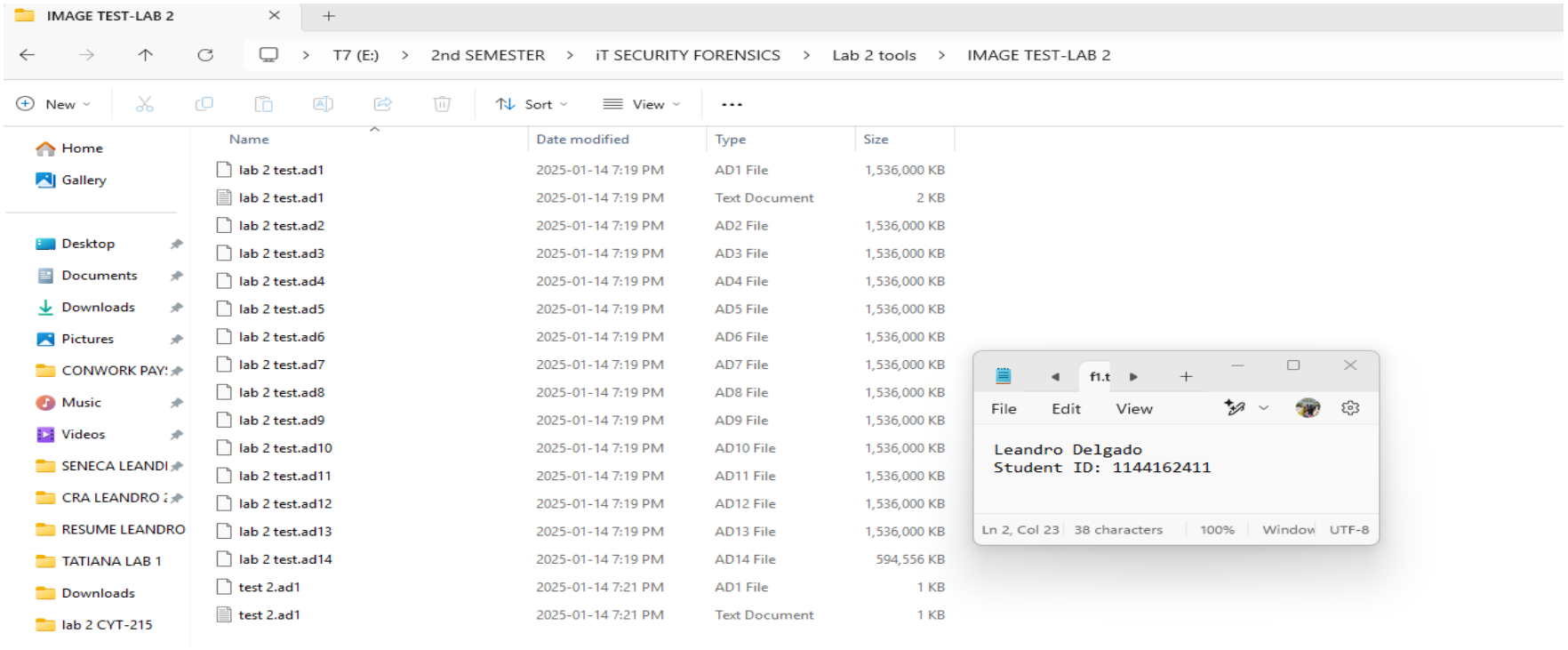
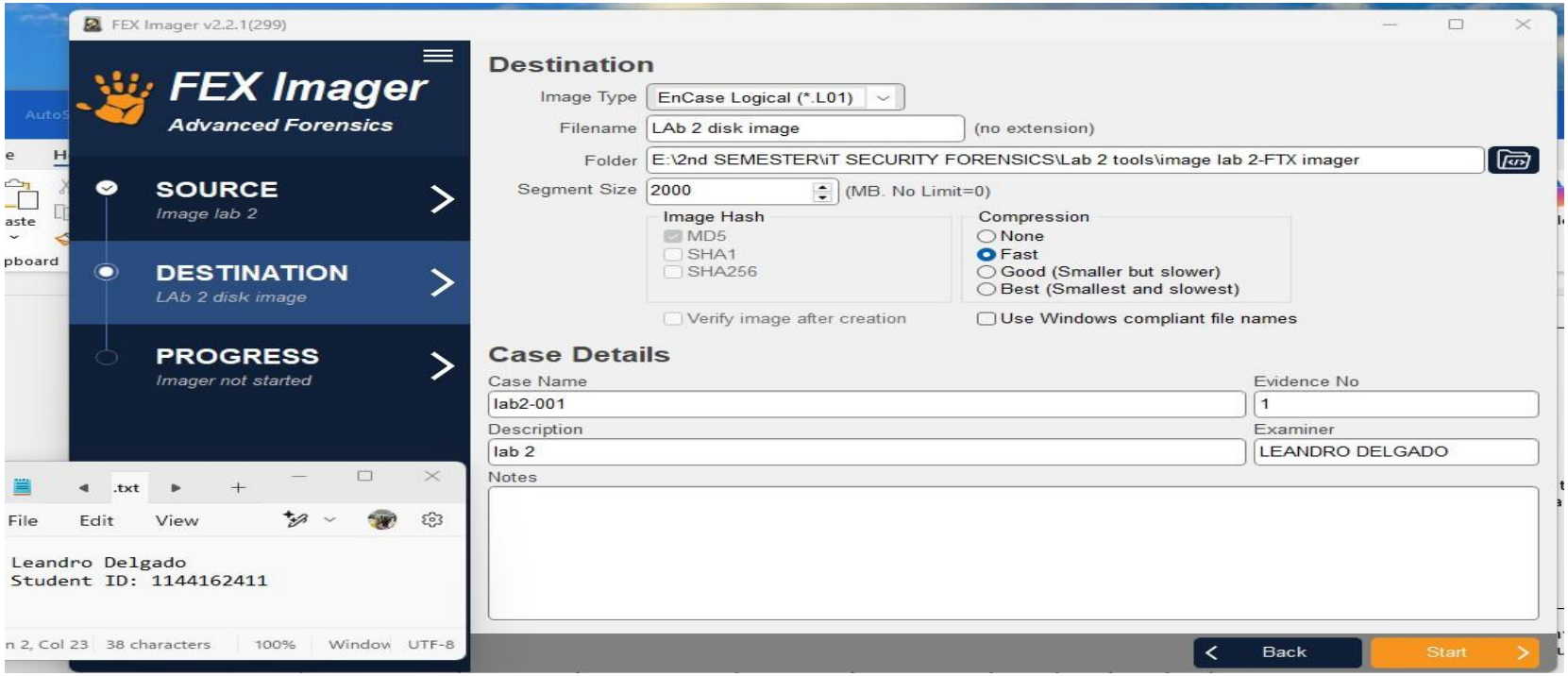
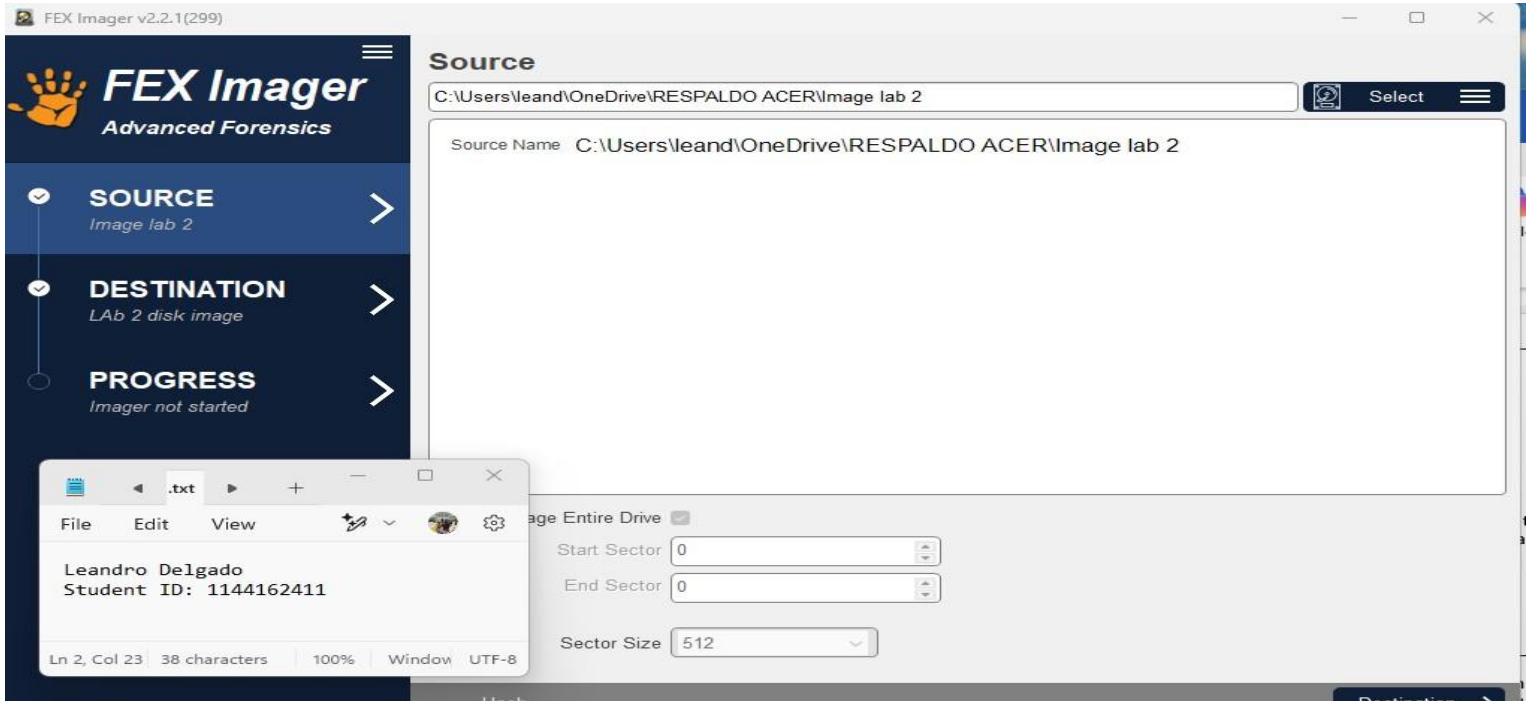
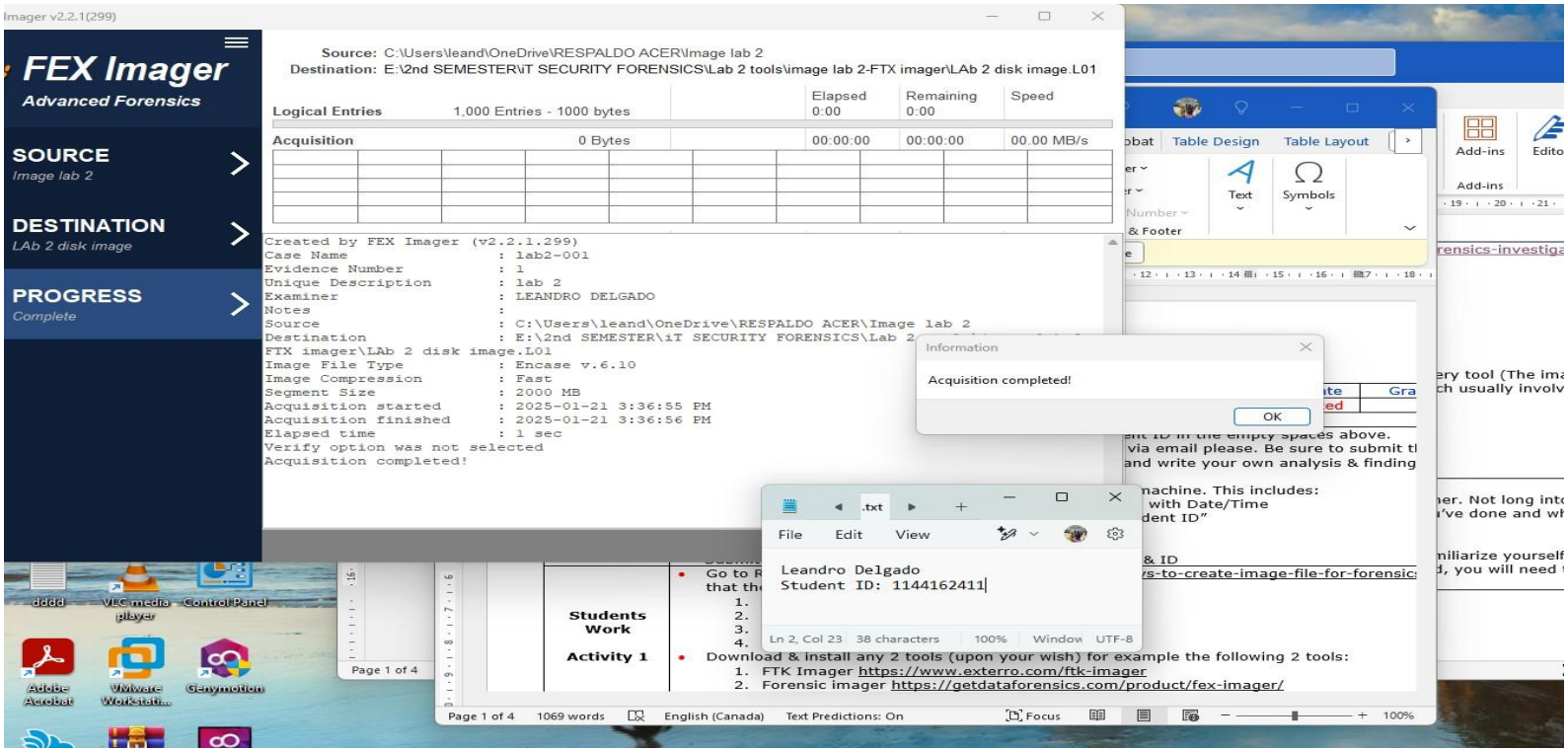


IMAGE TEST-LAB 2
T7 (E:) > 2nd SEMESTER > iT SECURITY FORENSICS > Lab 2 tools > IMAGE TEST-LAB 2
New
Sort
View
Home
Gallery
Desktop
Documents
Downloads
Pictures
CONWORK PAY!
Music
Videos
SENECA LEANDI
CRA LEANDRO
RESUME LEANDRO
TATIANA LAB 1
Downloads
lab 2 CYT-215
Name
Date modified
Type
Size
lab 2 test.ad1 2025-01-14 7:19 PM AD1 File 1,536,000 KB
lab 2 test.ad1 2025-01-14 7:19 PM Text Document 2 KB
lab 2 test.ad2 2025-01-14 7:19 PM AD2 File 1,536,000 KB
lab 2 test.ad3 2025-01-14 7:19 PM AD3 File 1,536,000 KB
lab 2 test.ad4 2025-01-14 7:19 PM AD4 File 1,536,000 KB
lab 2 test.ad5 2025-01-14 7:19 PM AD5 File 1,536,000 KB
lab 2 test.ad6 2025-01-14 7:19 PM AD6 File 1,536,000 KB
lab 2 test.ad7 2025-01-14 7:19 PM AD7 File 1,536,000 KB
lab 2 test.ad8 2025-01-14 7:19 PM AD8 File 1,536,000 KB
lab 2 test.ad9 2025-01-14 7:19 PM AD9 File 1,536,000 KB
lab 2 test.ad10 2025-01-14 7:19 PM AD10 File 1,536,000 KB
lab 2 test.ad11 2025-01-14 7:19 PM AD11 File 1,536,000 KB
lab 2 test.ad12 2025-01-14 7:19 PM AD12 File 1,536,000 KB
lab 2 test.ad13 2025-01-14 7:19 PM AD13 File 1,536,000 KB
lab 2 test.ad14 2025-01-14 7:19 PM AD14 File 594,556 KB
test 2.ad1 2025-01-14 7:21 PM AD1 File 1 KB
test 2.ad1 2025-01-14 7:21 PM Text Document 1 KB
f1.t
File
Edit
View
Leandro Delgado
Student ID: 1144162411
Ln 2, Col 23
38 characters
100%
Window
UTF-8


FEX Imager v2.2.1(299)
FEX Imager
Advanced Forensics
SOURCE
Image lab 2
DESTINATION
LAb 2 disk image
PROGRESS
Imager not started
Destination
Image Type EnCase Logical (*.L01)
Filename LAb 2 disk image (no extension)
Folder E:\2nd SEMESTER\iT SECURITY FORENSICS\Lab 2 tools\image lab 2-FTX imager
Segment Size 2000 (MB. No Limit=0)
Image Hash
MD5
SHA1
SHA256
Compression
None
Fast
Good (Smaller but slower)
Best (Smallest and slowest)
Verify image after creation
Use Windows compliant file names
Case Details
Case Name lab2-001
Evidence No 1
Description lab 2
Examiner LEANDRO DELGADO
Notes
Back
Start
.txt
File Edit View
Leandro Delgado
Student ID: 1144162411
Ln 2, Col 23 38 characters 100% Window UTF-8


FEX Imager v2.2.1(299)
FEX Imager
Advanced Forensics
SOURCE
Image lab 2
DESTINATION
LAb 2 disk image
PROGRESS
Imager not started
Source
C:\Users\leand\OneDrive\RESPALDO ACER\Image lab 2
Select
Source Name C:\Users\leand\OneDrive\RESPALDO ACER\Image lab 2
Start Sector 0
End Sector 0
Sector Size 512
.txt
File Edit View
Leandro Delgado
Student ID: 1144162411
Ln 2, Col 23 38 characters 100% Window UTF-8


FEX Imager
Advanced Forensics
SOURCE
Image lab 2
DESTINATION
LAb 2 disk image
PROGRESS
Complete
Source: C:\Users\leand\OneDrive\RESPALDO ACER\Image lab 2
Destination: E:\2nd SEMESTER\iT SECURITY FORENSICS\Lab 2 tools\image lab 2-FTX imager\LAb 2 disk image.L01
Logical Entries 1,000 Entries - 1000 bytes
Acquisition 0 Bytes
Elapsed 0:00
Remaining 0:00
Speed
00:00:00
00:00:00
00.00 MB/s
Created by FEX Imager (v2.2.1.299)
Case Name : lab2-001
Evidence Number : 1
Unique Description : lab 2
Examiner : LEANDRO DELGADO
Notes :
Source : C:\Users\leand\OneDrive\RESPALDO ACER\Image lab 2
Destination : E:\2nd SEMESTER\iT SECURITY FORENSICS\Lab 2
FTX imager\LAb 2 disk image.L01
Image File Type : Encase v.6.10
Image Compression : Fast
Segment Size : 2000 MB
Acquisition started : 2025-01-21 3:36:55 PM
Acquisition finished : 2025-01-21 3:36:56 PM
Elapsed time : 1 sec
Verify option was not selected
Acquisition completed!
Information
Acquisition completed!
OK
File Edit View
Leandro Delgado
Student ID: 1144162411
Ln 2, Col 23 38 characters 100% Window UTF-8
Students Work
Activity 1
Download & install any 2 tools (upon your wish) for example the following 2 tools:
1. FTK Imager https://www.exterro.com/ftk-imager
2. Forensic imager https://getdataforensics.com/product/fex-imager/
Page 1 of 4 1069 words English (Canada) Text Predictions: On Focus 100%

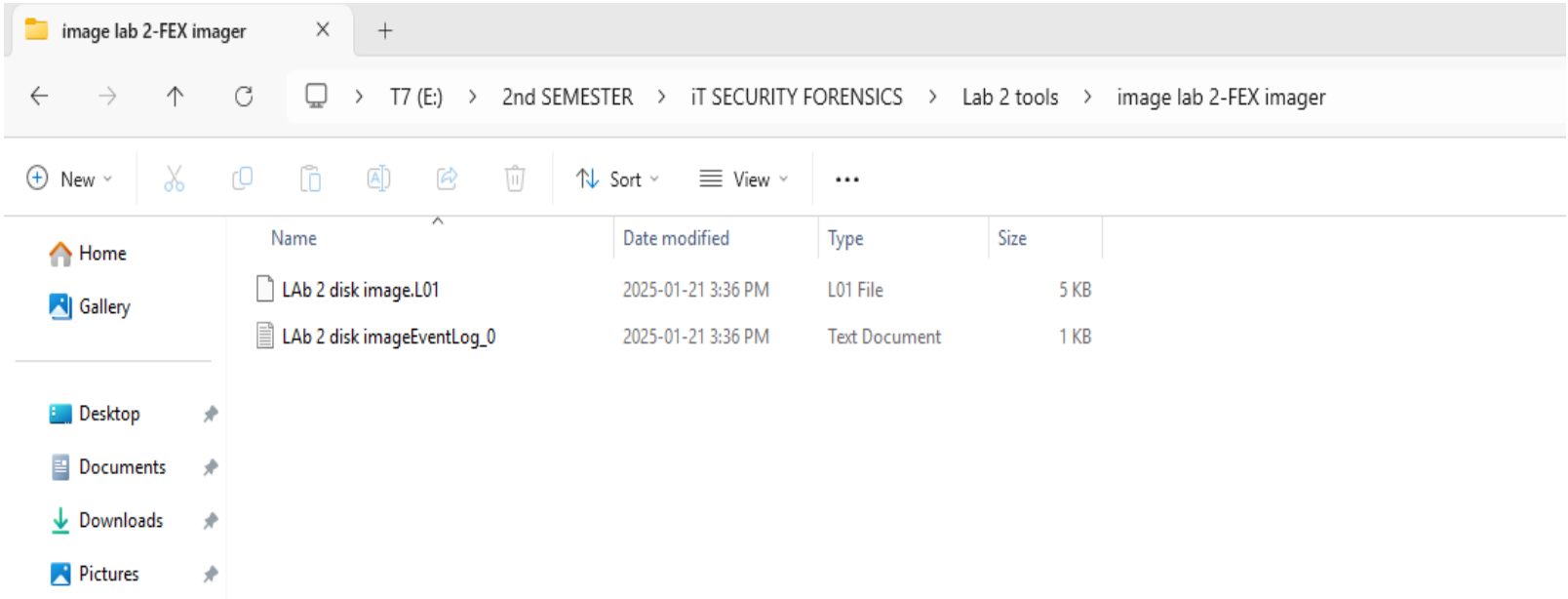
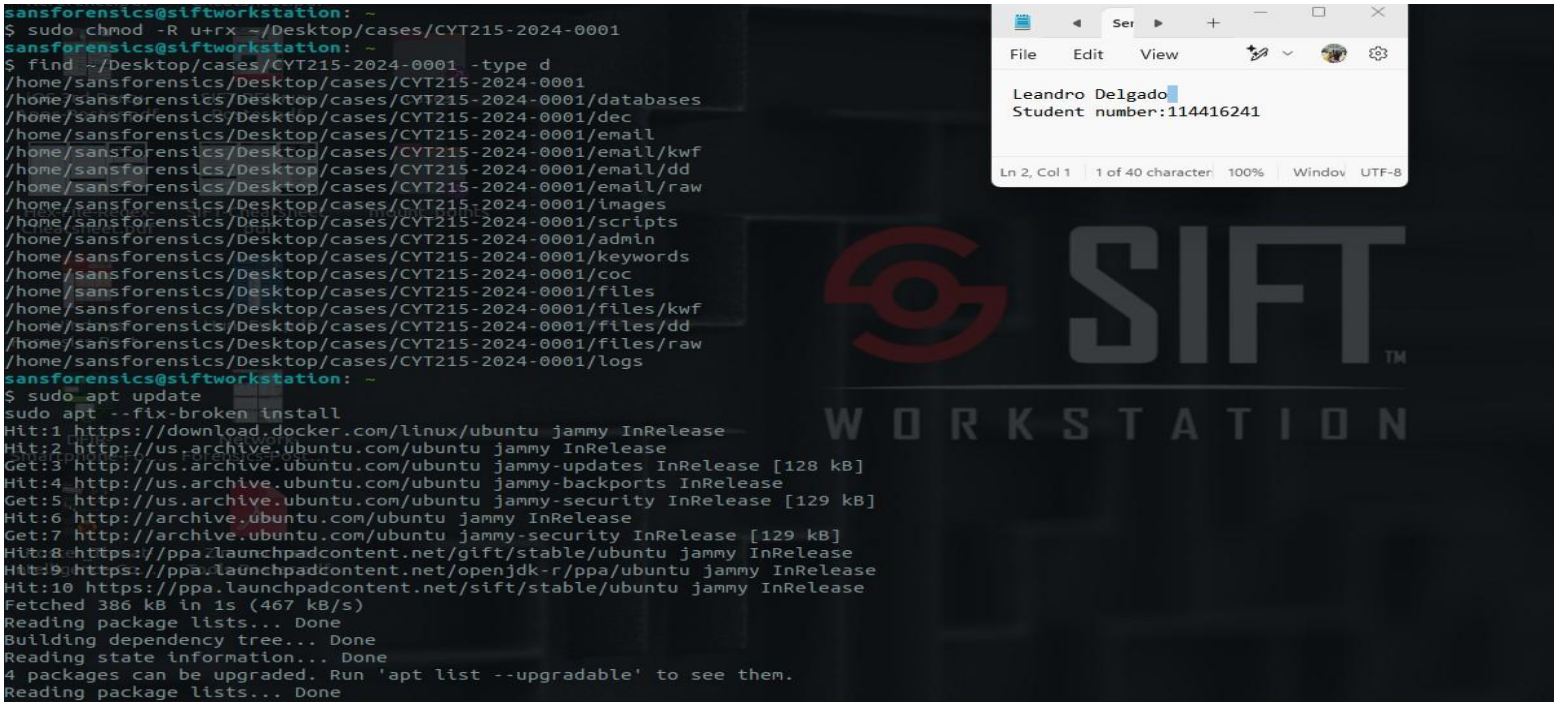
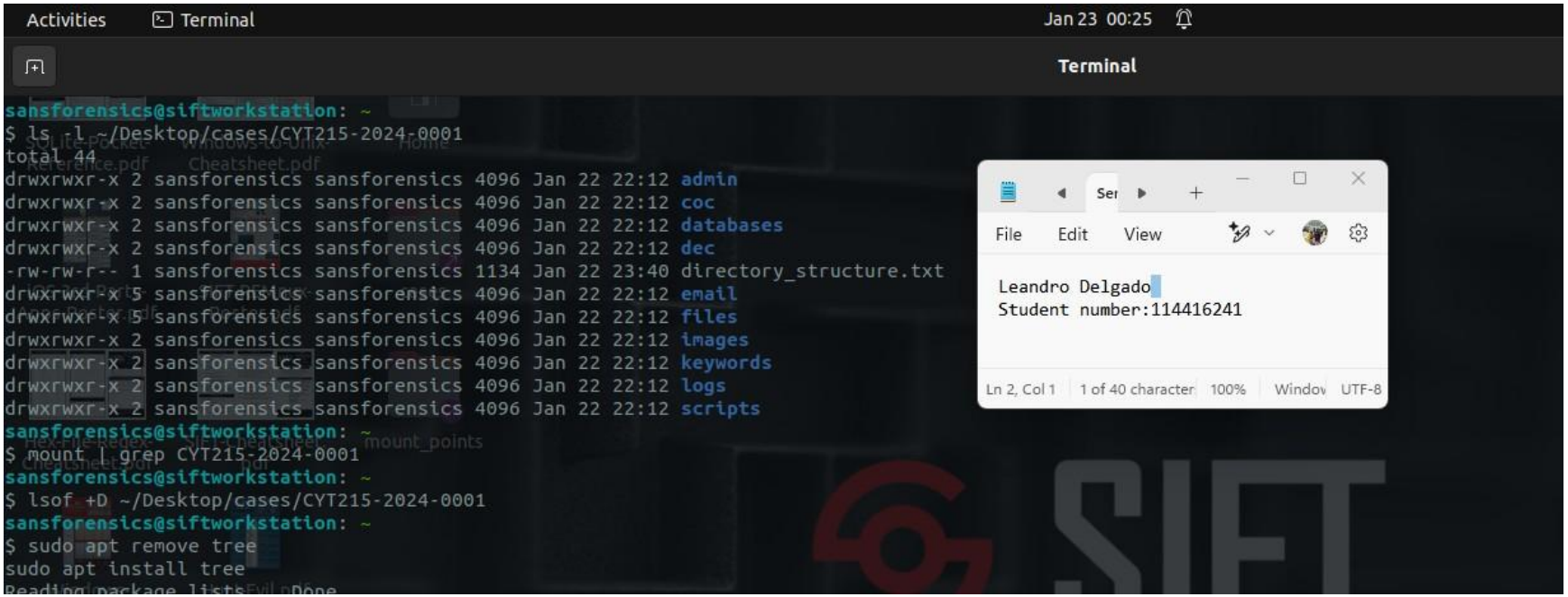
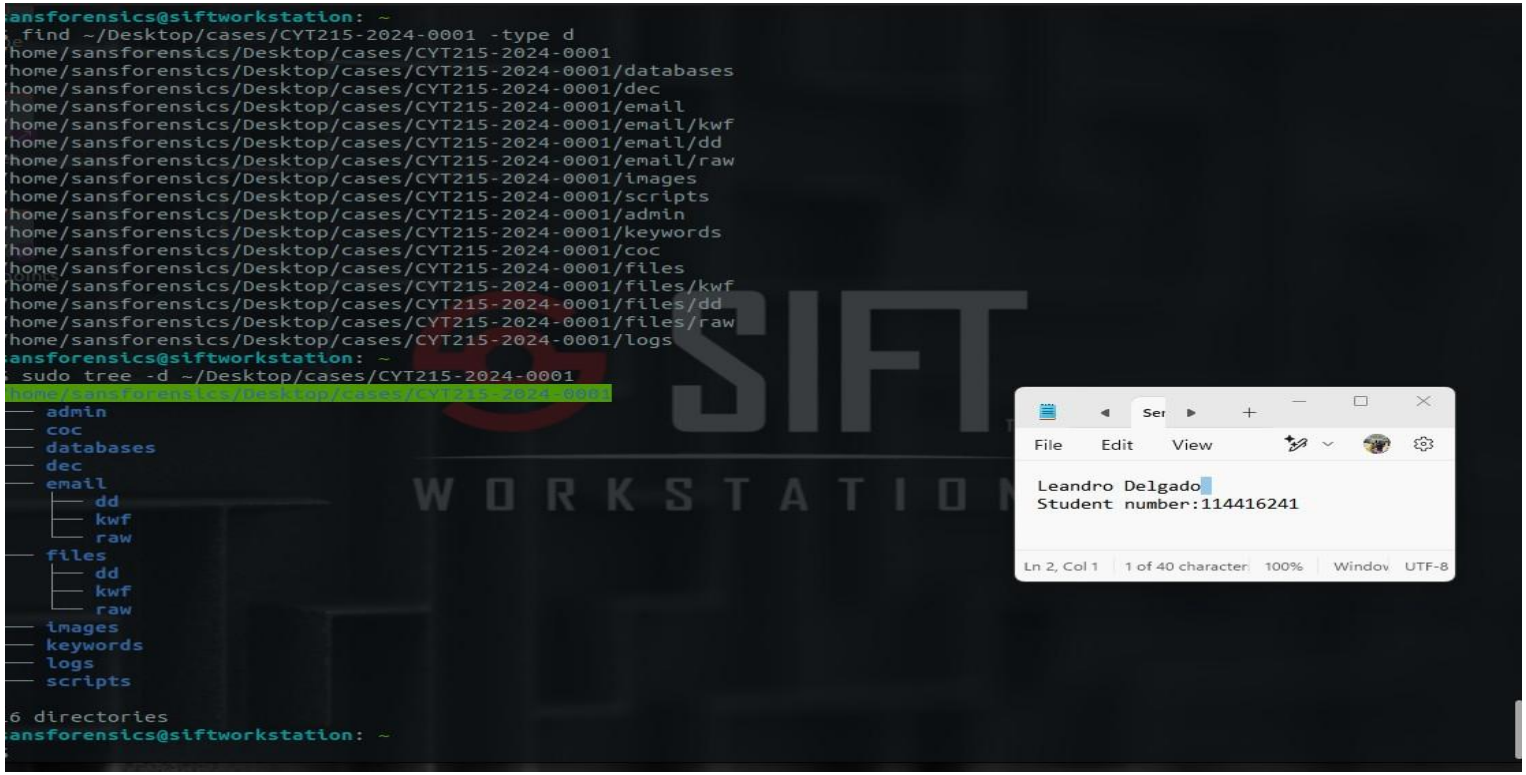


image lab 2-FEX imager
T7 (E:) > 2nd SEMESTER > iT SECURITY FORENSICS > Lab 2 tools > image lab 2-FEX imager
New
Sort
View
Home
Gallery
Desktop
Documents
Downloads
Pictures
Name
Date modified
Type
Size
LAb 2 disk image.L01
2025-01-21 3:36 PM
L01 File
5 KB
LAb 2 disk imageEventLog_0
2025-01-21 3:36 PM
Text Document
1 KB


sansforensics@siftworkstation: ~
$ sudo chmod -R u+rx ~/Desktop/cases/CYT215-2024-0001
sansforensics@siftworkstation: ~
$ find ~/Desktop/cases/CYT215-2024-0001 -type d
/home/sansforensics/Desktop/cases/CYT215-2024-0001
/home/sansforensics/Desktop/cases/CYT215-2024-0001/databases
/home/sansforensics/Desktop/cases/CYT215-2024-0001/dec
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/kwf
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/dd
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/raw
/home/sansforensics/Desktop/cases/CYT215-2024-0001/images
/home/sansforensics/Desktop/cases/CYT215-2024-0001/scripts
/home/sansforensics/Desktop/cases/CYT215-2024-0001/admin
/home/sansforensics/Desktop/cases/CYT215-2024-0001/keywords
/home/sansforensics/Desktop/cases/CYT215-2024-0001/coc
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/kwf
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/dd
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/raw
/home/sansforensics/Desktop/cases/CYT215-2024-0001/logs
sansforensics@siftworkstation: ~
$ sudo apt update
sudo apt --fix-broken install
Hit:1 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:6 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:7 http://archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:8 https://ppa.launchpadcontent.net/gift/stable/ubuntu jammy InRelease
Hit:9 https://ppa.launchpadcontent.net/openjdk-r/ppa/ubuntu jammy InRelease
Hit:10 https://ppa.launchpadcontent.net/sift/stable/ubuntu jammy InRelease
Fetched 386 kB in 1s (467 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
4 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
File Edit View
Leandro Delgado
Student number:114416241
Ln 2, Col 1
1 of 40 character
100%
UTF-8
SIFT
WORKSTATION


Activities
Terminal
Jan 23 00:25
Terminal
sansforensics@siftworkstation: ~
$ ls -l ~/Desktop/cases/CYT215-2024-0001
total 44
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 admin
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 coc
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 databases
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 dec
-rw-rw-r-- 1 sansforensics sansforensics 1134 Jan 22 23:40 directory_structure.txt
drwxrwxr-x 5 sansforensics sansforensics 4096 Jan 22 22:12 email
drwxrwxr-x 5 sansforensics sansforensics 4096 Jan 22 22:12 files
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 images
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 keywords
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 logs
drwxrwxr-x 2 sansforensics sansforensics 4096 Jan 22 22:12 scripts
sansforensics@siftworkstation: ~
$ mount | grep CYT215-2024-0001
sansforensics@siftworkstation: ~
$ lsof +D ~/Desktop/cases/CYT215-2024-0001
sansforensics@siftworkstation: ~
$ sudo apt remove tree
sudo apt install tree
File Edit View
Leandro Delgado
Student number:114416241
Ln 2, Col 1
1 of 40 character
100%
UTF-8
SIFT
WORKSTATION


sansforensics@siftworkstation: ~
$ sudo apt install tree
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tree is already the newest version (2.0.2-1).
The following packages were automatically installed and are no longer required:
gir1.2-snapd-1 libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
sansforensics@siftworkstation: ~
$ find ~/Desktop/cases/CYT215-2024-0001 -type d
/home/sansforensics/Desktop/cases/CYT215-2024-0001
/home/sansforensics/Desktop/cases/CYT215-2024-0001/databases
/home/sansforensics/Desktop/cases/CYT215-2024-0001/dec
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/kwf
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/dd
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/raw
/home/sansforensics/Desktop/cases/CYT215-2024-0001/images
/home/sansforensics/Desktop/cases/CYT215-2024-0001/scripts
/home/sansforensics/Desktop/cases/CYT215-2024-0001/admin
/home/sansforensics/Desktop/cases/CYT215-2024-0001/keywords
/home/sansforensics/Desktop/cases/CYT215-2024-0001/coc
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/kwf
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/dd
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/raw
/home/sansforensics/Desktop/cases/CYT215-2024-0001/logs
sansforensics@siftworkstation: ~
File Edit View
Leandro Delgado
Student number:114416241
Ln 2, Col 1 1 of 40 character 100% Windov UTF-8


sansforensics@siftworkstation: ~
find ~/Desktop/cases/CYT215-2024-0001 -type d
/home/sansforensics/Desktop/cases/CYT215-2024-0001
/home/sansforensics/Desktop/cases/CYT215-2024-0001/databases
/home/sansforensics/Desktop/cases/CYT215-2024-0001/dec
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/kwf
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/dd
/home/sansforensics/Desktop/cases/CYT215-2024-0001/email/raw
/home/sansforensics/Desktop/cases/CYT215-2024-0001/images
/home/sansforensics/Desktop/cases/CYT215-2024-0001/scripts
/home/sansforensics/Desktop/cases/CYT215-2024-0001/admin
/home/sansforensics/Desktop/cases/CYT215-2024-0001/keywords
/home/sansforensics/Desktop/cases/CYT215-2024-0001/coc
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/kwf
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/dd
/home/sansforensics/Desktop/cases/CYT215-2024-0001/files/raw
/home/sansforensics/Desktop/cases/CYT215-2024-0001/logs
sansforensics@siftworkstation: ~
sudo tree -d ~/Desktop/cases/CYT215-2024-0001
/home/sansforensics/Desktop/cases/CYT215-2024-0001
admin
coc
databases
dec
email
dd
kwf
raw
files
dd
kwf
raw
images
keywords
logs
scripts
6 directories
sansforensics@siftworkstation: ~
File Edit View
Leandro Delgado
Student number:114416241
Ln 2, Col 1 1 of 40 character 100% Windov UTF-8

This lab really showed me how important it is to stay organized in forensic investigations. By setting up a clear directory structure, I can manage large amounts of data more easily and avoid getting overwhelmed. Getting hands-on with commands like mkdir, cp, and tree also helped me feel more comfortable using the command line. I also realized how helpful automation can be. Writing scripts to run commands saves time and ensures I can repeat my work the same way every time, reducing mistakes. This will be useful in bigger cases, where staying consistent is key to getting accurate results.