Drone Forensics Software
Step by Step User Guide

Software Installation - Prerequisites and configuration requirements

*Mandatory

1. Install Virtual Box/VMware (optional)
2. Install a Linux Distribution (E.g. Ubuntu or Parrot) on your computer. *
3. Install The Sleuth Kit, PyQt (GUI) *
4. Go to – **www.github.com/p16214718/ctec3453** and download DFS Software by selecting clone/download repository. *
5. Save 'DFS' software into a directory of your choice. *

Running DFS :

1. Right click on the DFS folder. Various files will be displayed.
2. Right click within the folder and select 'Open in Terminal'.
3. A terminal window will open. Type in 'python menu.py' (space between python and menu). Press enter.5
4. After a few seconds, a window will appear with title 'Drone Forensics Software'. This is the main menu and reflects tabs 'Functions, Help, Exit'.

Using DFS

1. Click on 'Functions' tab.
2. A drop-down menu appears displaying 4 functions
    - List Devices
    - Sanitisation
    - HDD Imaging
    - Deleted File Recovery

Using Function 1: List Devices

1. Insert the disk/device(s) to either sanitise or to use to make a forensic copy.
2. Select 'List Devices'. Press enter.
3. A window will appear displaying disk/device information of your current system including all disks inserted.
4. The program will always reflect your system's disk as 'SDA' which is a non-selectable value. All other drives will be displayed as 'sdb', 'sdc' 'sdd' and so on.
5. From the devices listed, identify and make note of the device (**) you wish to either sanitise or copy.
6. Close the function by clicking on the 'red circle' (close button) on the 'list devices' window.

Using Function 2: Sanitisation (Erasing and Formatting a device).

1. Return to the main menu, by selecting it from the taskbar.
2. Select ‘Functions’.
3. Select ‘Sanitisation’.
4. A window will appear with an input field.
5. Type the device name into the input field e.g. sdb, sdc. (**) . This is the device you wish to sanitise. Click on the ‘OK’ button.
6. The program will now run to sanitise and reformat the disk. The time for completion of this process is dependent on the size of the disk. Once complete it a message will appear on the terminal, confirming this. Do not close the window whilst the operation is running.
7. Once the process is complete, close the window by clicking on the ‘red circle’ of that window.

Using Function 3: HDD Imaging

1. Return to the main menu, by selecting it from the taskbar.
2. Select ‘functions’.
3. Select ‘HDD Imaging’.
4. A window will appear with an input field
5. Type the device name into the input field e.g. sdb, sdc. This is the device you wish to copy.
6. Click on the ‘OK’ button.
7. The program will now run to copy the disk and will store the forensic image within the current directory.
8. This forensic image should now be moved onto the sanitised disk. Copy and verify methods can be used to ensure that the image is moved in a forensically sound manner.
9. The time for completion of this process is dependent on the size of the disk. Once complete it a message will appear on the terminal, confirming this. Do not close the window whilst the operation is running.
10. Once the process is complete, close the window by clicking on the ‘red circle’ of that window.

Using Function 4: Deleted File Recovery

1. Return to the main menu, by selecting it from the taskbar.
2. Select ‘Functions’.
3. Select ‘Deleted File Recovery’.
4. A window will appear with an input field
5. Type the name of the forensic image into the input field e.g. ‘img.dd’. This is the forensic image you wish to recover files from.
6. Click on the ‘OK’ button.
7. The program will now run to recover files from the forensic image and store them in a folder called ‘Recovered Files’ in the current directory. These files should be moved to the sanitised disk.
8. The time for completion of this process is dependent on the size of the forensic image and the number of recoverable files.
9. Once complete it a message will appear on the terminal, confirming this. Do not close the window whilst the operation is running. Once the process is complete, close the window by clicking on the ‘red circle’ of that window.