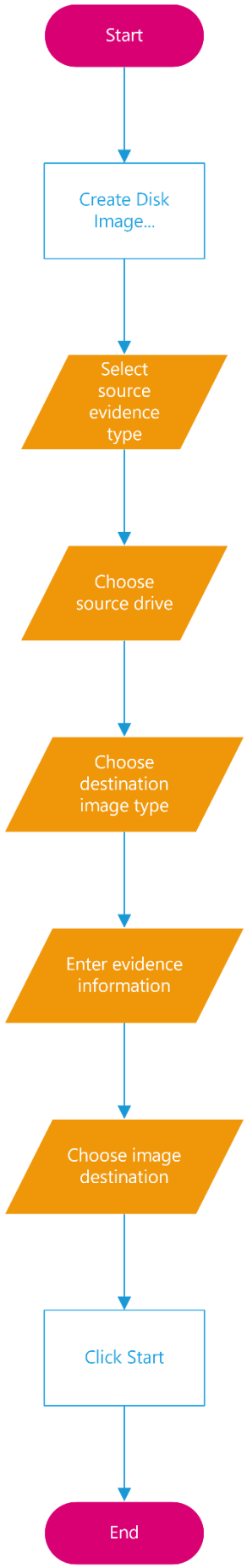
Muhammad Izham Bin Norhamadi
B032020039
S2G1

Class Activity

1. Capture from the video on how the imaging process is executed using FTK Imager.

- In the File button select the “Create Disk Image…” option. On the option to select the source evidence type we usually would want to choose Physical Drive option to recover more information. Logical Drive reserved for drives that might be too big as there will be hidden information. Image File is a forensic copy of the drive for forensic investigation. In the next screen select the source drive, and then add an image destination by selecting the destination image type. Raw(dd) option is the exact copy of the drive (bit to bit), E01 has all the raw data and extra features such as checksum and easier encryption. In the next screen enter the evidence item information, then choose the image destination. Lastly, click Start.

2. Based on your understanding, draw a flowchart to represent the imaging process. (Hint: You can use Visio as the tool to draw the flowchart or any tools available)


Start
Create Disk Image...
Select source evidence type
Choose source drive
Choose destination image type
Enter evidence information
Choose image destination
Click Start
End