

Table of content:

[Cover page 1](#_Toc163333979)

[Table of contents 2](#_Toc163333980)

[Administration information 3](#_Toc163333981)

[The executive summary 4](#_Toc163333982)

[Investigation scope 5](#_Toc163333983)

[Acquisition and handling of the evidences 5](#_Toc163333984)

[Investigation environment 5](#_Toc163333985)

[Tools used in analysis 5](#_Toc163333986)

[Analysis summary 6](#_Toc163333987)

[Analysis 6](#_Toc163333988)

[Conclusion 7](#_Toc163333989)

[Exhibits 8](#_Toc163333990)

[Revision History 9](#_Toc163333991)

Administraation information:

21110241/flower case

HTU digital forensics

Search warrants/authorization for the investigation of the evidence

The participants of the investigation including:

Investigators: Issam Awamleh

Victims: the student which is me ☺

Suspects: Dr.safa heraiz ☺

Interrogated or reviewed people: none

Excuative summury:

The disk has been showed the small parts of it with hidden data which is the docx file after separate it and dig dipper in the file which I found 4 pics the third pic was the evidence.

**Investigation scope:**

The resources are a tool to see the hex of the whole disk and some internet website to know the head and the trial of the files such as docx and png.

## Acquisition and handling of the evidences

The evidence was uploaded as vhd by the eLearning then attach by my laptop to check it out then I find nothing so when I use HxD to see the hex of the whole disk.And the evidence has found which is the flower pic in the deleted docx specially in file slack.

|  |  |  |  |
| --- | --- | --- | --- |
| Tool name | Version | Company name | Description |
| HxD | N/A | N/A | For analyzing the files and breakdown to hex to make it easy to the investigator |

Analysis summary:

The after attaching the VHD and visualized the files in the disk as hex after taking the docx and isolate it from the whole disk after that by searching the head and the trail of the PNGs and extracting it and separated to get the evidence

The evidence:

