

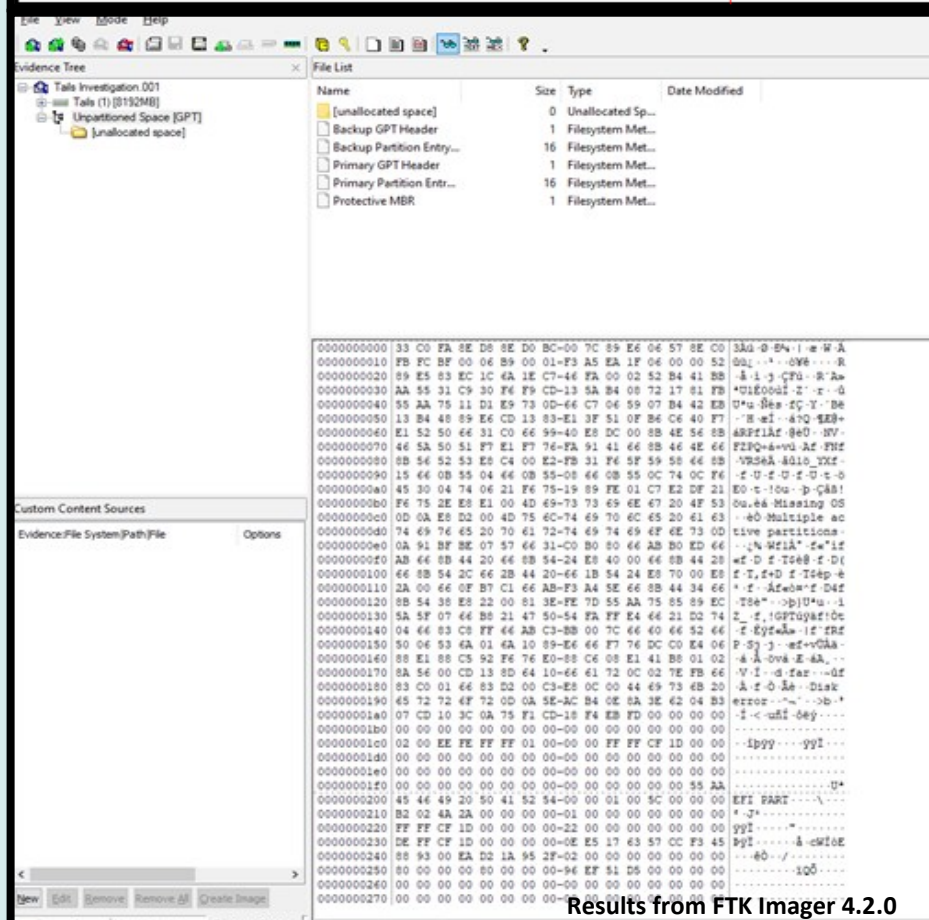
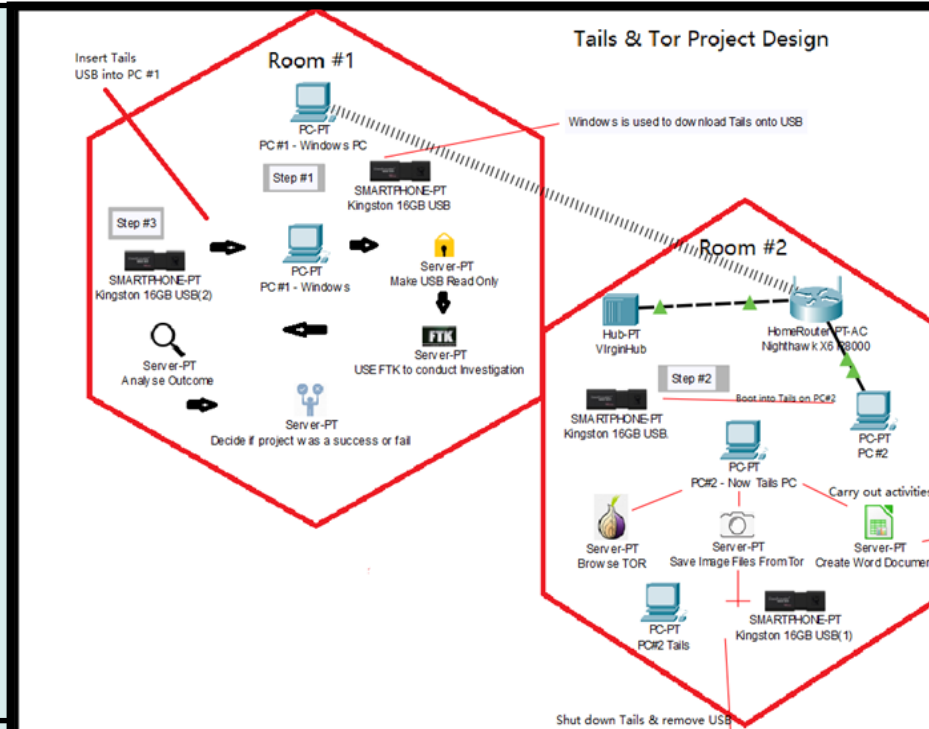
Introduction

In recent years, technology has made great improvements—it is rapidly evolving without the look of any end in sight. People live online, but many are also afraid for their security online, turning towards applications and software that ensure their security.

This is why Tails was created—an operating system that is seemingly 'amnesic' and only boots off a USB or CD Rom; it forgets any data that was saved onto it (whether that be image files, text files, videos, internet data) as soon as it is shut down—it's able to do this by utilising volatile memory—which loses all data upon shutdown.

Objectives

- Investigate the structure of Tails & the fundamentals of how it works.
- Research how criminals use this OS to commit crime.
- Conduct a literature review using other research about this topic.
- Conduct an experiment including data gathering on Tor using appropriate tools and perform a forensics investigation into the data found.
- Present clear discussion of the results of the experiment, along with the impact that Tails has had on the world of digital forensics.
- Conduct the project with the best practice and complete reflective writing on completion of the project.



Design & Implementation

- Ensure the devices to be used are compatible with Tails.
- Create checklist of activities to be carried out on Tails & install Etcher & FTK Imager 4.2.0, then install Tails onto USB using Etcher.
- Boot Tails (change boot settings in BIOS) and perform activities (saving image files, web surfing, word files, etc).
- Boot into Windows, enable write-protection on the USB, perform imaging on USB using FTK, then use the image as the evidence file to carry out forensic analysis on the data retrieved.

Results

After carrying out forensic analysis on the imaged file, it was found that no files that were saved onto the OS whilst active were present; the only files that were recovered were the files that Tails uses to boot and a folder which represented unallocated space. All of the file information for these folders were displayed in Hexadecimal Code—which when converted, was seemingly encrypted.

Conclusion

This project required a lot of research and problem-solving; it was found that Tails is rather unique as it functions on a live drive and removes data after shutdown; because of the nature of the project, a careful approach was taken whilst performing activities and carrying out the investigation. Multiple tools were used to carry the project out, such as: A PC, a router, PC, FTK, Etcher, Tails, and Tor. Fundamentally, the result is that—Tails does exactly what its supposed to, forget.