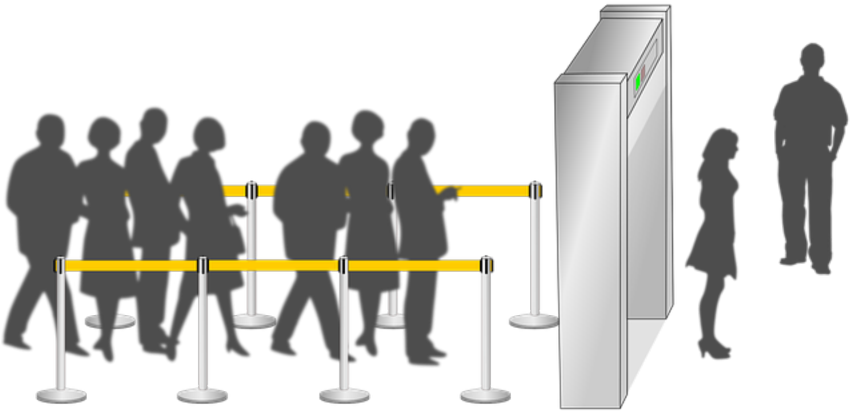
Digital Forensics

Introduction

The following case scenario has been described in detail and must be followed for the forensics analysis you have been asked to perform.

Case Scenario

A company (Superfake Inc) have requested our forensic services to examine a thumb drive found on a company employee during a routine search when leaving the building.



This search is mandatory and is part of the company's employment contract. The nature of the company's research and general safe servicing and repair is confidential and subject to a number of government contract worldwide. Employees are not permitted to bring computer hardware or equipment in or out of the building. The scanner detects metal and computer components and will sound an alarm if an object is detected.

On Thursday 17th February 2022 @ 17:33 an employee of the company (Diana Prince) passed thorough the scanner and the alarm sounded. The security team have a procedure they will follow in such a scenario. The employee is requested to take two steps forward to create space from anyone else in the queue and to answer the following questions:

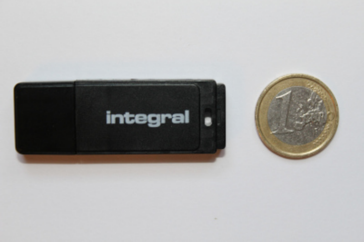
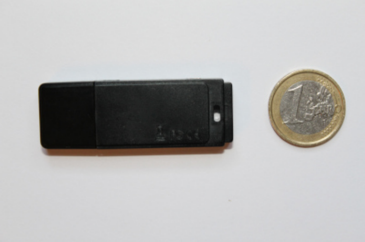
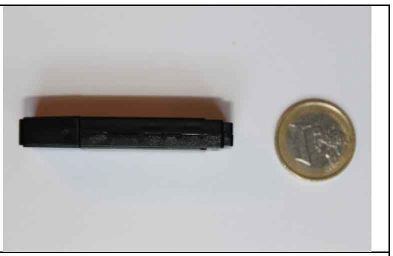
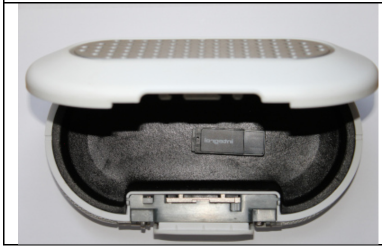
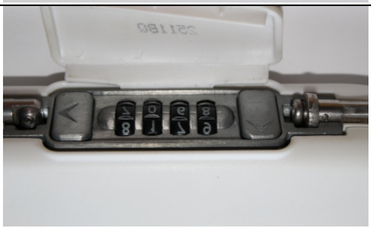
1. Have you any metal items or computer components on your person?
2. Do you wish to remove an item from your person and go through the scanner again?
3. If the answer to question 2 is "no" a search of the person and their property must be conducted.

The search procedure required the employee to be accompanied to a room for a search to be conducted. The search procedure has been approved by the company's legal team and is in full compliance with its statutory any legal responsibilities.

The employee answered no to question 2 and was accompanied to the search room. A USB key was found in Diana's coat pocket. Diana Prince stated she did not own the drive and she has no idea how this got into her pocket. This interaction was recorded and is documented in the company's CCTV footage.

Once the search was completed the security team secured the USB Key and placed it in a secure storage container to be placed in a secure chain of custody. Diana Prince was present for the storage of the device and this is part of the CCTV footage. The container has a secure 4 digit pin combination which was set by the security manager and documented in the company password register which resides in the company safe. The container was placed in the safe by the security manager and was supervised by the CTO and a member of the HR team.

Images from the acquisition of the USB Key:

Following the company's policy and procedure the chain of custody document was created by the manager of the security team. (See Appendix A for larger images)

A forensic image of the USB key was created by the Systems Manager (Miles Dyson). It is noted that a forensics team may prefer to create their own image. The Systems Manager has completed the required certification to complete this task and the company have a lab with all the appropriate hardware.

Requirements:

You are required to complete a forensics analysis of the image provided.
In your submission you must address the following:

- Use digital forensics tools to perform the analysis of the USB key image (eg. Autopsy)
    - Demonstrate how to perform a manual carve for a file using a Hex Editor
- Document the process needed to prepare the pen drive for imaging
- From a digital forensics perspective, demonstrate the theory and application of the following:
    - Recovery
    - Carving (Signatures)
    - Filesystems
    - Partial Recovery
    - Metadata
- Presentation of the useful files/data recovered (this can be submitted via a zip file)
- Report Writing
    - Documentation (of full process)
    - How was the items discovered in Autopsy (what Ingest modules were used)
    - Presentation of results
    - Recommendations of findings / and additional actions needed for the investigation going forward.
    - Have any Irish / EU laws been broken?

Assumptions / Considerations:

1. The image size has been kept small to ensure the analysis can be performed on systems with a minimal spec. Large disk images can require a large amount of RAM to perform the analysis and can take a large amount of time to complete. This does not limit our investigation, it just speeds up the analysis phase.