Digital Forensics

Rob Stewart

Table of Contents

[1. Introduction 2](#_Toc22390398)

[2. Tools used 4](#_Toc22390399)

[3. Methodology 5](#_Toc22390400)

[3.1. Acquire forensic image 5](#_Toc22390401)

[3.2. Examine Image using Autopsy in Windows 7](#_Toc22390402)

[4. Results 12](#_Toc22390403)

[5. Conclusions 12](#_Toc22390404)

# Introduction

This report outlines the steps used to carry out a forensic investigation on a USB key for Mondial Ltd. Mondial suspected that their employee, Frances Byrne, used this key to remove a copy of the company database from the premises.

The alleged theft took place on Sunday the 6th of October. The USB key was obtained from the suspects’ desk on Friday 11th of October 2019.



Figure 1.1 USB found abandoned on desk.

Desk has been scanned for any other pieces of evidence, discovery of further evidence proved fruitless, noted that other items are missing but are currently classed as irrelevant.



Figure 1.2 USB is the only certifiable piece of evidence.

Evidence has been removed from scene and placed in a transport ziplock bag, this will be brought to the lab for further analysis.

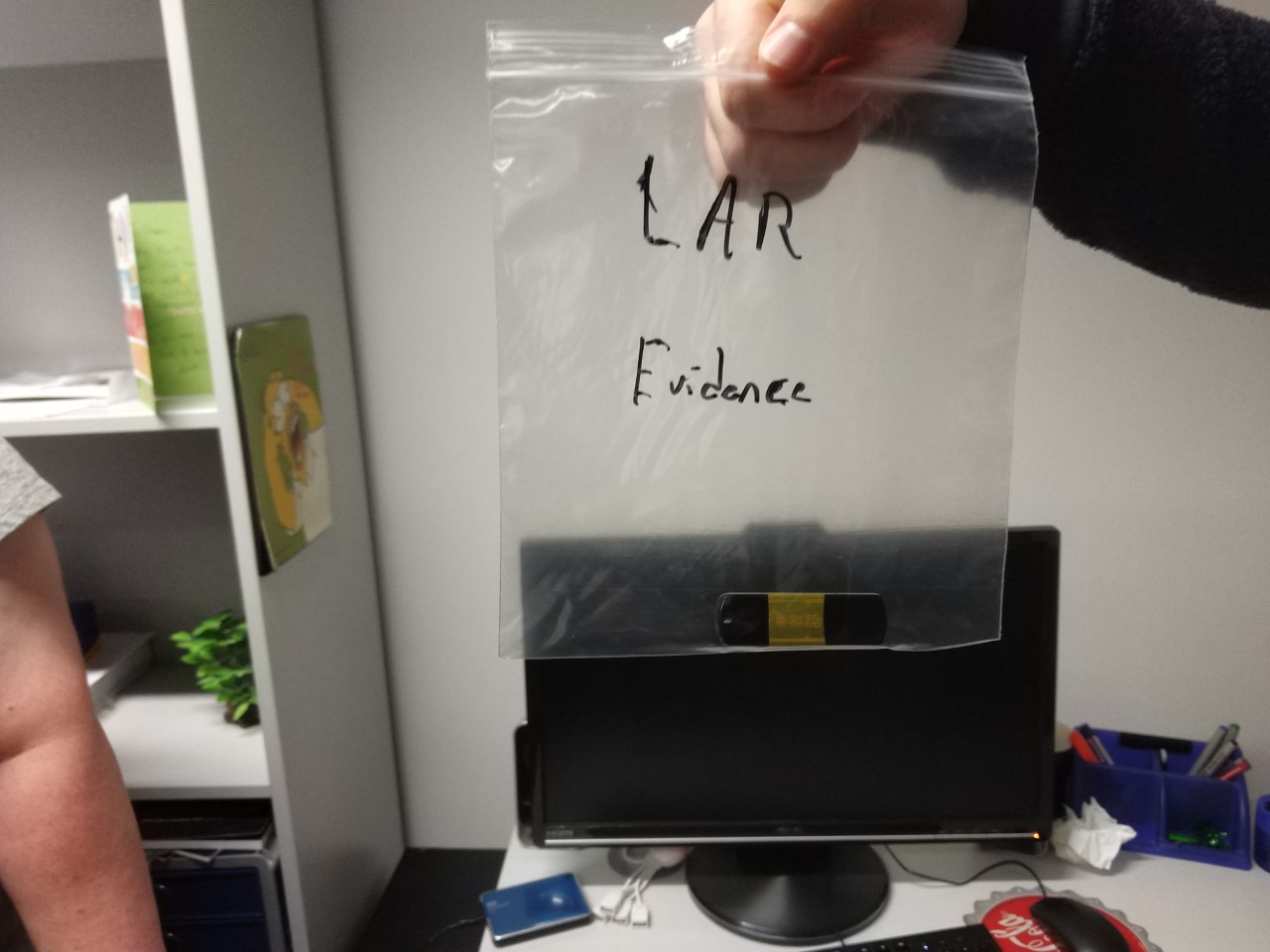


Figure 1.3 USB removed from scene.

# Tools used

* Deft Zero version 8.2 installed on 8GB USB
* Laptop Dell Inspirion 15 3000
* Autopsy version 4.12.0
* Microsoft word
* Microsoft access
* Microsoft photos
* Snipping tool

# Methodology

## Acquire forensic image

Deft was used to acquire a forensic bit-stream copy of the evidential USB key. The Laptop was booted from the USB key. Once Deft booted the suspect USB was inserted and mounted in read-only as shown in figure 3.1.1.

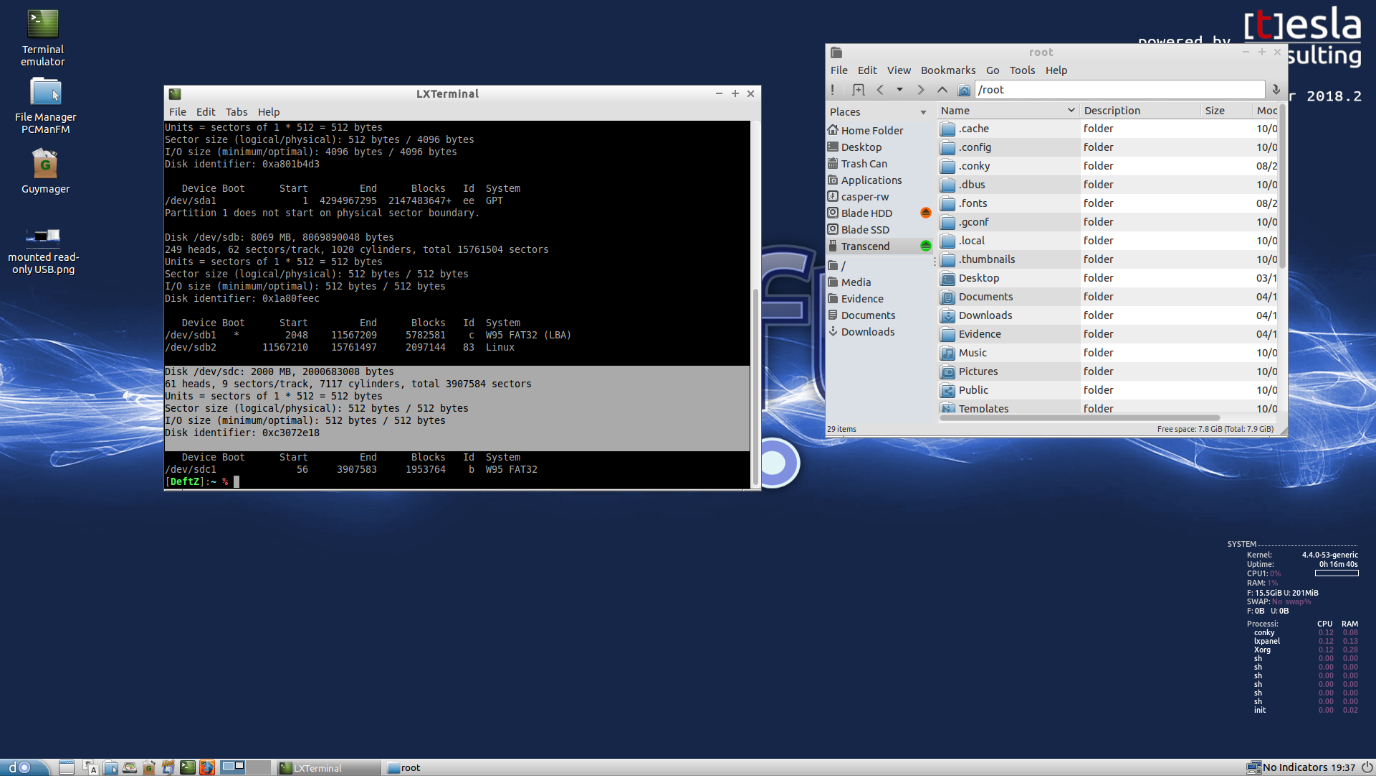


Figure .1 USB mounted in read-only.

The USB was mounted to /dev/sdd found using the fdisk -l command, as shown in figure 3.1.2.

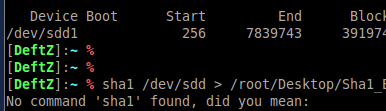


Figure .2 USB mounted to dev/sdd.

An MD5 was obtained of the entire USB drive shown in figure 3.1.3.

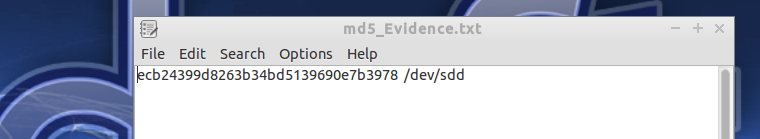


Figure .3 MD5 hash.

Additionally, a SHA1 of the entire USB was obtained as seen in figure 3.1.4.

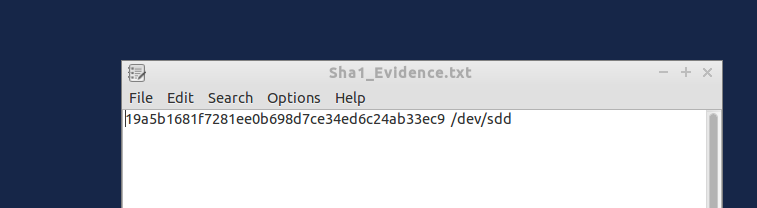


Figure .4 SHA1 hash.

Image acquired using Guymager, with in it the MD5 and SHA1 hashes can be seen and match the previous figures 3.1.3 and 3.1.4 hash values.

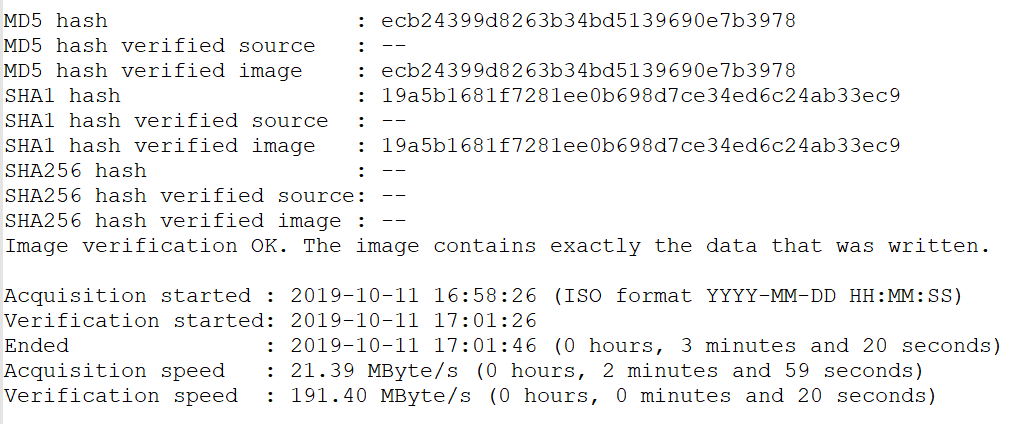


Figure .5 Guymager MD5 & SHA1 hashes.

The E01 file was successfully obtained using Guymager and will be used with the digital forensics software, Autopsy.

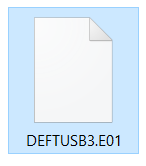


Figure .6 USB.E01 file.

## Examine Image using Autopsy in Windows

In Autopsy a new case was created for a single user, the case was appropriately named, numbered and saved in a suitable base location. Upon creation the disk image option seen in Figure 3.2.1 was selected.

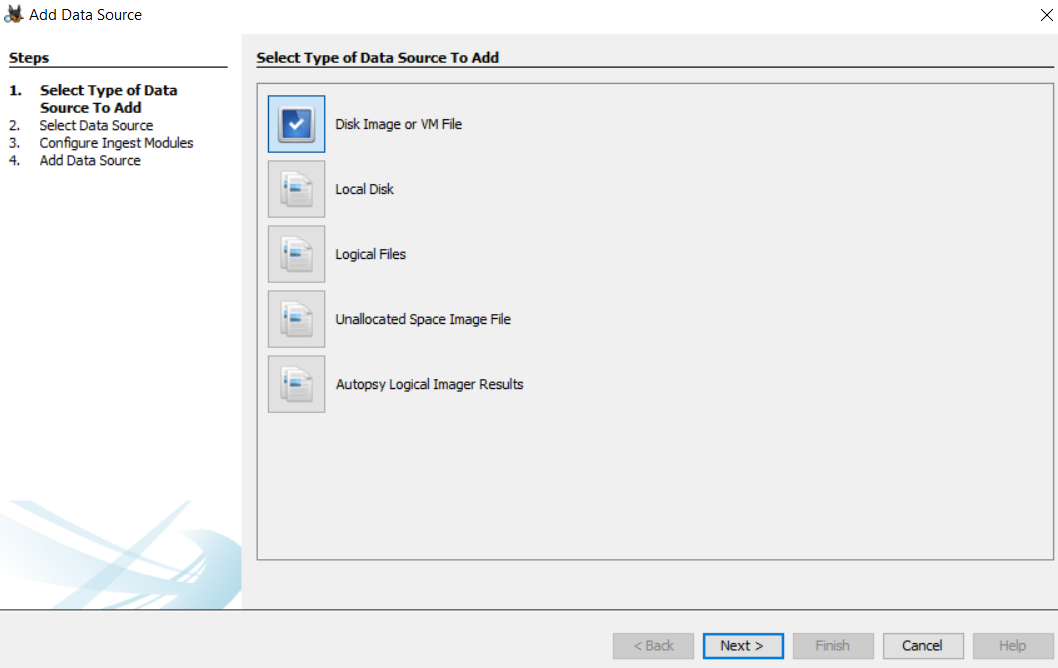


Figure . Disk image is selected.

Next Hash Lookup, Email Parser, PhotoRec Carver and Android Analyser were deselected

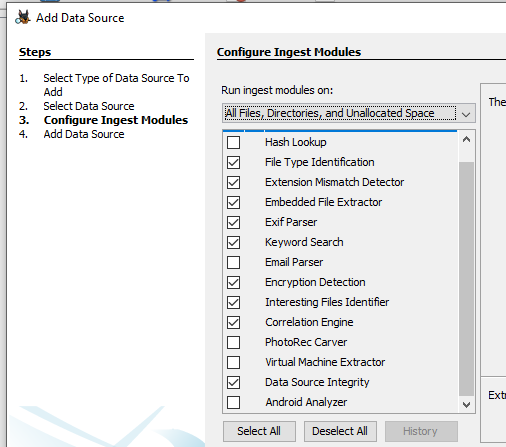


Figure . Selected only the necessary options.

Initially it was shown that the deleted files were empty, but running the file type identification module revealed more evidence.

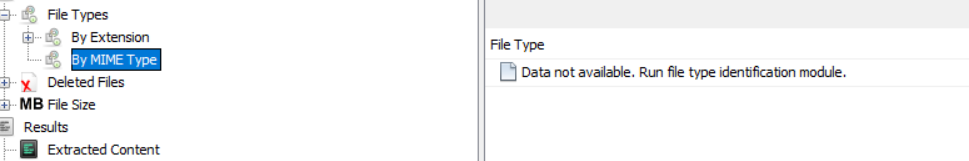


Figure . Shows zero deleted files initially.

Figure 3.2.4 shows that the database was copied to and deleted form the evidence USB.

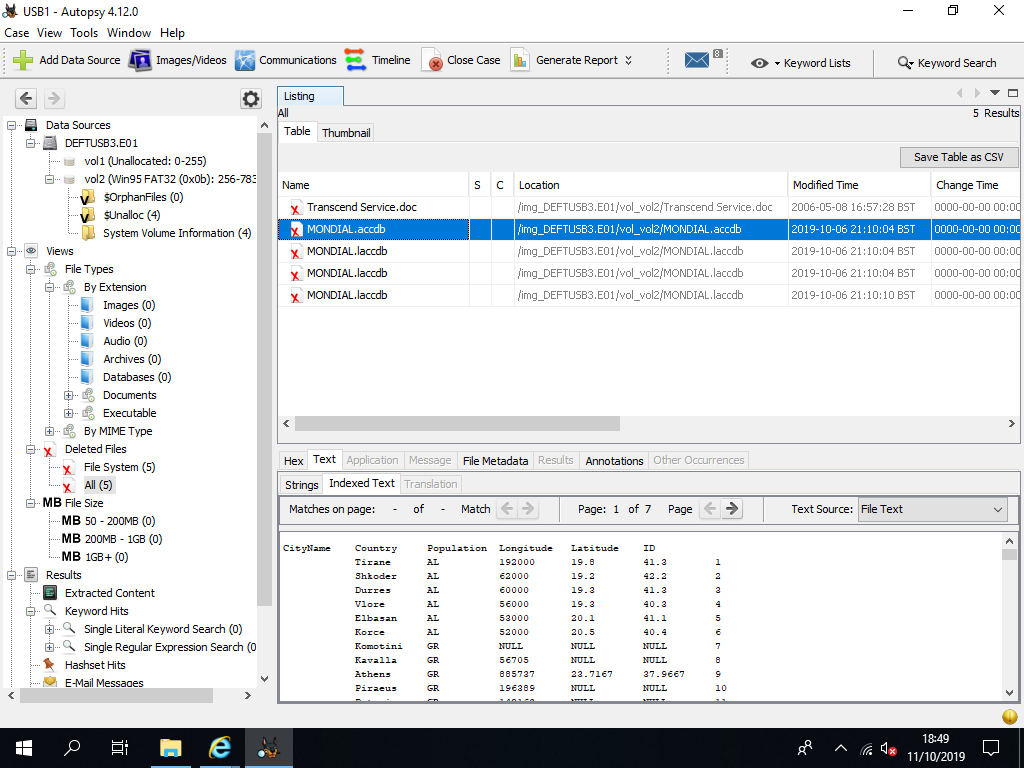


Figure . MODIAL access database located.

Figure 3.2.5 shows the level of usage the USB received between the months of May and October, August shows some usage, where October shows a large scale of use. Thus, this shows further evidence of this USBs use in this case.

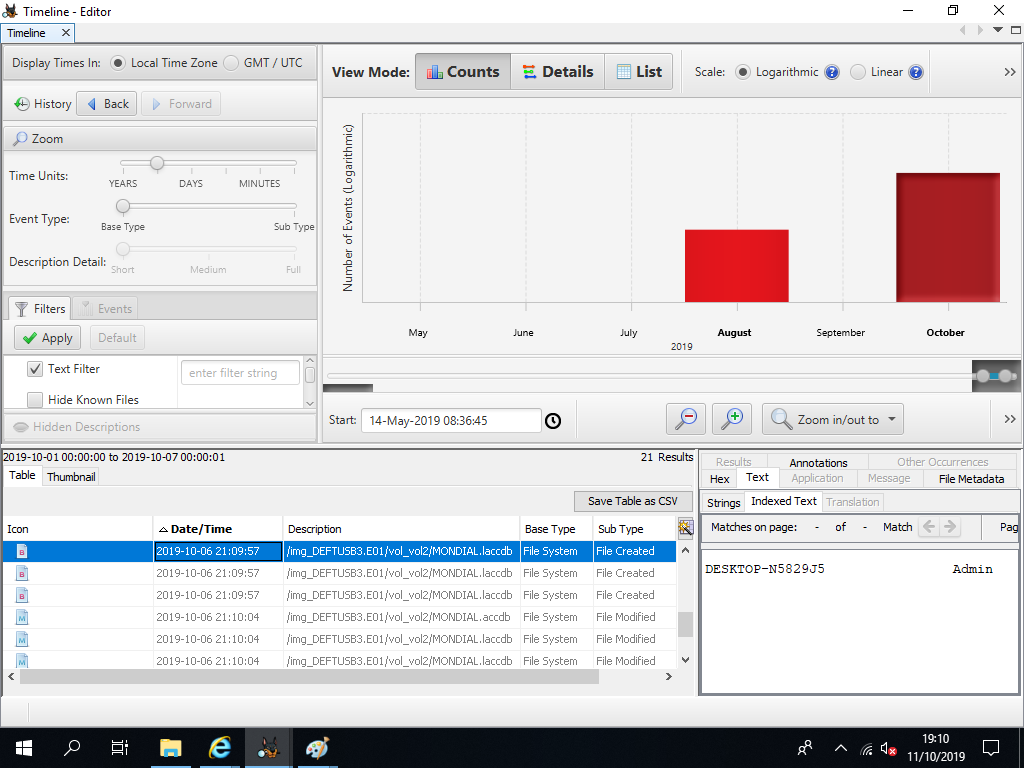


Figure . USB usage from May to October.

On finding the database, it was extracted and opened in Microsoft Access, this can be cross-referenced with MONDIAL Ltds current database at the companies earliest convenience.

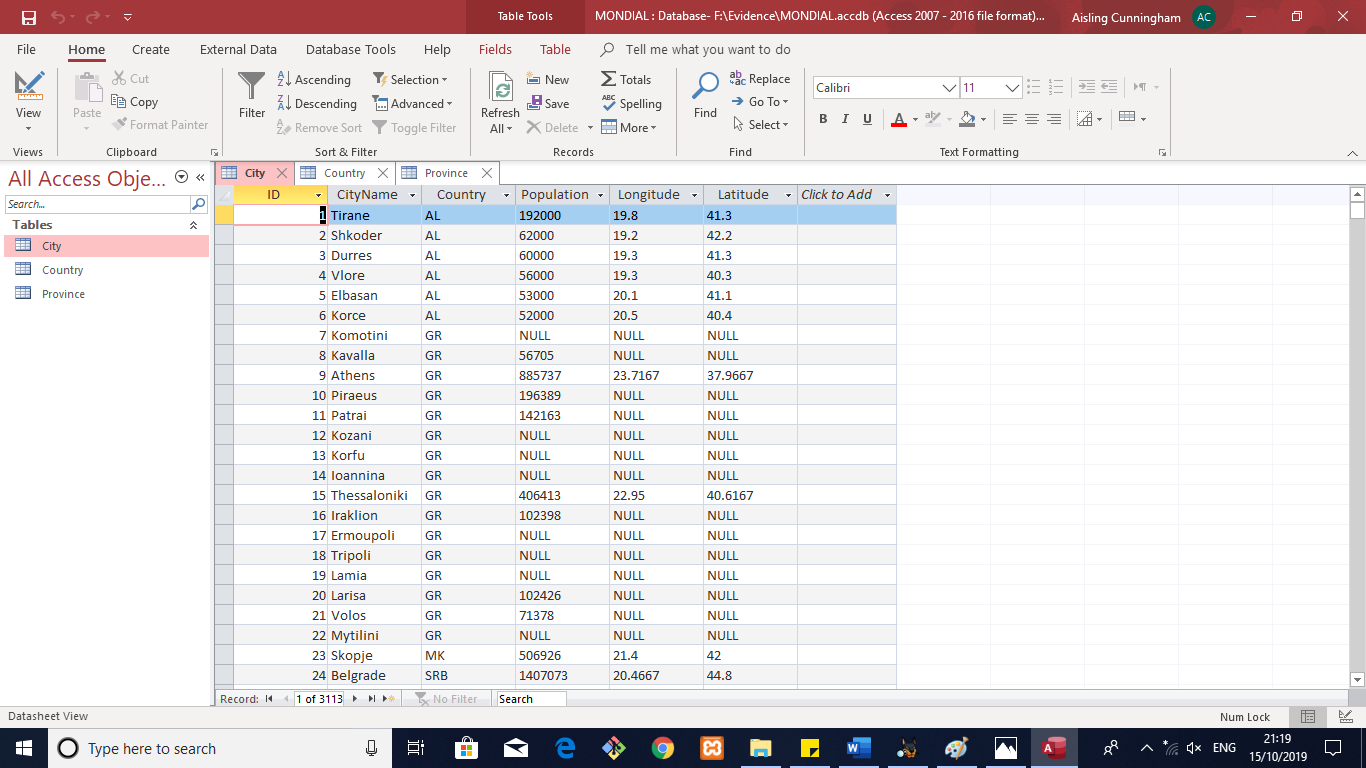


Figure . Deleted database containing all copied details.

# Results

The evidence USB that was obtained on Friday the 11th of October at the desk of MONDIAL Ltd employee Frances Byrne, was certifiably used to take a copy of a database in MONDIAL Ltd, it was deleted from sed USB soon afterwards. Deft and Guymager successfully acquired an image of the entire USB without changing anything on it and Autopsy successfully found the database in question, despite it being deleted from the USB. It was then able to be opened in Access and compared to the live database in the company. Naming a suspect currently is inconclusive. Further investigation will have to be carried out.

# Conclusions

On Sunday the 6th of October the suspect entered the premises at approximately 9pm, they made their way to the office space of one of MONDIAL Ltds employees named Frances Byrne. The suspect then logged into the computer using the employees account, they then placed the USB in the machine took a copy of the database and then deleted the database from the USB.

The suspects interaction with the copied database ran from 9:09:57pm when the copy was made, until 9:10:04pm when the copy was deleted, only 7 seconds elapsed in this interaction.

The USB was abandoned on the employees table and not discovered until Friday the 11th of October when it was noticed that the employee had been missing for the past week since the incident occurred, additionally the employees’ personal belongings are missing.

There is no CCTV footage in the office space for any of MONDIALS employees, and the review of any other footage, particularly not belonging to the company, must be permitted by the proper authorities.

MONDIAL Ltd have not reported an ill occurrence in their system since the incident, they have not reached out to their missing employee to ensure their wellbeing, this should be a priority as the irregular disappearance of the employee suggests they could be in danger. Failure to follow up on this should result in it being made a police matter.

Final main point conclusions are:

* Suspect entered premises at approximately 9pm on Sunday the 6th of October.
* Suspect entered the office space of Frances Byrne and gained access to the employee machine and account.
* The database was copied to the evidence USB and deleted from it soon afterwards.
* Suspect is unknown.
* Motive is unknown.
* CCTV footage is currently unobtainable.
* CCTV footage at the scene is non-existent.