**CSE3CFN**

**Group Assignment - Team B**

**Name: Viraj, Jagsir, Shehbaz**

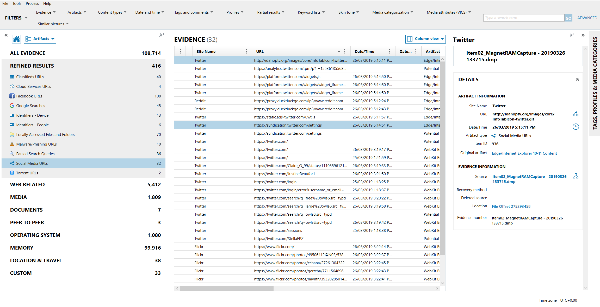
**Student ID: 20625630, 19263446, 21044916**

***Question 1:***

1. Most *o*f the skype client artifacts come from the SQLite database main.db. More specifically the accounts table of the main.db.
2. The files that store the skype user preferences and settings is Accounts table of the main.db. This table stores the minimum information needed to create a user account and their preferences within Skype.
3. The filmstrip view grabs still from a video file at every 10%, resulting in 10 total thumbnail images that allow the examiner to view the contents of the video file quickly.

A screenshot of a computer

Description automatically generated

1. One function to quickly isolate a specific social media site is to filter on the site name column and typing the desired site name:

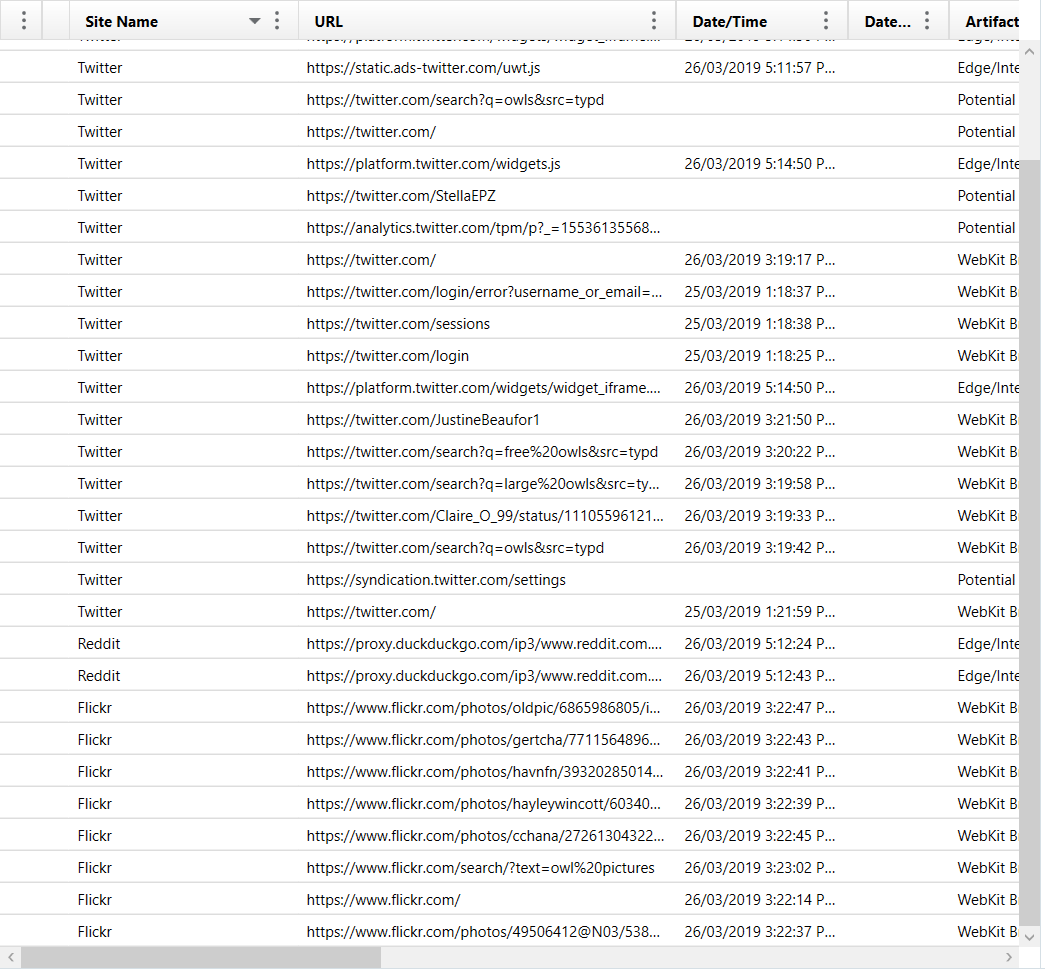
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The next function to sort in the social media URLs category is to do column sorting. By just clicking on a specific column, such as the site name, it will sort the evidence according to the site names, making it easier to find a specific site.



1. A screenshot of a computer

   Description automatically generatedSession recovery files store a browser’s last used pages or tabs, as well as providing a way to restore these last used pages or tabs in the event of a crash or power loss. The Session Recovery will always hold this information in case a crash occurs and doesn’t just populate in the event of a crash.
2. A google analytics cookie are more detailed in nature and provide a means to track visitor activity. These types of cookies are used to accurately figure out the exact actions of a user, such as their means of accessing a specific website, where they initially came from, how long they visited a webpage, what exact pages they had viewed, etc. These cookies aren’t just used by Google bowsers themselves, but are a service also provided to other browsers such as Firefox and Microsoft Edge. There are also three different types of Google Analytics cookies. First Visit Cookies track the information relating to website visits. More specifically it includes a hash value of the domain, visitor ID, created date/time, etc.

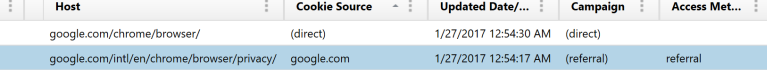
A computer screen with a white background

Description automatically generated

A computer screen with a white background

Description automatically generated with medium confidenceThe next type is Session Cookies. These track the activity that occurred during a visit on a website. These are valid for too long as they expire if the user is idle for more than 30 minutes.

The last type of cookie is a referral cookie, which show how a user travelled to a specific website.



However, normal cookies aren’t as detailed in nature. They still hold user data on the host machine and keeps track of data such as login credentials, user preferences, etc.

1. The operating system artifacts in AXIOM are recovered from the windows (system root) folder structure, the user profile folder structure, and the Windows Registry. On older systems, a restore point folder contains these artifacts, but on a newer system, the System Volume Information folder structure contains the artifacts. Microsoft also define the Windows Registry as “a hierarchical database that stores configuration information. The registry contains profiles for each user of the computer, and information about system hardware, installed programs, and property settings. Windows continually references this information during its operations.”
2. The key located in the ntuser.Dat file which allows any USB that has been plugged in to be linked with a user account is the MountPoints2 registry key. This helps keep track, especially if there is more than one user on the machine. The location link that references MountPoints2 begins with HKU as seen in the screen shot.

A screenshot of a computer

Description automatically generated

1. To scramble the data in the USERASSIST key, windows use an obfuscation scheme named ROT13, in which the letters in the alphabet are rotated 13 places to the right, according to the ROT table.
2. The three different operating system artifacts that can help identify the name of a file, path for the file, and application used to watch a video from an external hard drive by a user is firstly LNK files, as it shows the path of the file including the original drive letter, helping to determine whether it was an external drive or not. LNK files are also persistent and will remain in a system, regardless of whether it has been deleted or not.

A screenshot of a computer

Description automatically generated

The second artifact that can be used of the file system information artifact. This artifact is a system level artifact and is typically parsed from the booth record of any drive that was imaged on a machine. It also includes Volume Offset (Bytes) values that can help determine whether or not the artifact is located within the Master Boot Record (MBR) or Volume Boot Record (VBR). This then also provides the technical information needed to examine one of the imaged drives, showing information such as the drives geometry, files system, and whether it was a fixed or external/removable drive.

A screenshot of a computer

Description automatically generated

The third type of artifact that can be used are Jump Lists. Jump Lists identify the files and resources that have a user has accessed, also including important data such as timestamps and file paths. The most recently used section is where this information is stored. Jump lists also help identify whether a user has accessed a program or application to create, edit, or view specific files such as photos or videos. Jump Lists also show detailed information on the object that the user opened with whatever application they used, and also shows user behaviour via timelines and history. Much like an LNK file, Jump List evidence is stubborn in the fact that it shows evidence for when a user has deleted a file of the local drive or used a removable hard drive for whatever they were doing.

**Question 2:**

**Abstract (BBC, 25 April, 2017):**

This paper describes the digital forensic processes and techniques used to support the police investigation into the death of Richard Dabate's wife, Connie Dabate, who was charged with her murder. The data from Connie's Fitbit fitness tracker, which refuted Richard's account of what happened, was what made the case. I was a key player in gathering evidence as a computer forensic investigator and testifying as an expert in court **(Helen, 2020).**

**Table of contents:**

1.**Introduction:**

Digital forensics were used in the Richard Dabate case to aid the police investigation. The data from Connie Dabate's Fitbit activity tracker was the most important piece of digital evidence in this case since it disproved the suspect's alibi and revealed crucial details about the sequence of events that led to her murder. The digital forensic methods and processes utilised to support the investigation are described in depth in this report **(BBC, 25 April, 2017)(Helen, 2020)**.

2. **Digital forensic procedures (Helen, 2020):**

Collection of evidence:

It was decided to gather the victim's Fitbit as potential proof. Other nearby electronic equipment, including laptops, security cameras, and smartphones, were also protected.

Evidence of preservation:

The integrity of the digital evidence was ensured by following the correct chain of custody protocols. To avoid manipulation, the Fitbit gadget was kept in a safe location. Photographic evidence of the crime scene was also taken to ensure nothing else would be tampered with.

Data Acquisition:

Data acquisition is the process of gathering and storing digital data from various devices, including computers, smartphones, and other electronics. It is essential to use forensically sound procedures to preserve the obtained evidence's integrity and admissibility. This entails carrying out the data extraction in a controlled setting with a low possibility of contamination or modification. Fitbit data was meticulously and securely recovered by using such forensically sound techniques. As a result, the data collected may be trusted to be accurate, making it appropriate for further analysis and research.

Data Analysis:

The GPS positions that were derived from the Fitbit data offer useful geographic context. They provide details about specific places the victim frequented, allowing detectives to follow her activities and possibly spot any peculiar or strange locales. The GPS data, when combined with timestamps, can provide a more precise reconstruction of the victim's travels and activities before to the incident.

The Fitbit device's heart rate data also plays a significant function in comprehending the victim's physiological state. Experts in forensics can learn more about the victim's stress levels, physical activity, and other irregularities by examining the heart rate patterns and variations. These details may offer crucial hints regarding the victim's condition and emotional state just before her death.

It's important for assembling a thorough event chronology because it shows what the victim did and her vital signs prior to her sudden death. This analysis helps forensic specialists make sense of the incident's circumstances and possibly find any pertinent evidence.9b

Data Interpretation:

Connie Dabate's final moves were more than an hour after the suspect said she had been slain, according to the data analysis. The court was shown this material, which showed contradictions in the suspect's testimony.

3. **Expert witness testimony:**

The following questions might be raised by the other side's attorney or team during my testimony as an expert witness **(BBC, 25 April, 2017)**:

1. Could you describe the steps involved in gathering and analysing Fitbit data, along with the tools and techniques employed?

1. What procedures did you take, particularly in the case of the Fitbit device, to protect the authenticity and integrity of the digital evidence?

1. Can Fitbit data be changed or modified in any way? How can one be sure the information is true and trustworthy?

1. Could Fitbit data have any restrictions or technological concerns that could compromise the timeliness of events it establishes?

1. Did you examine other causes for the discrepancies between the Fitbit data and the suspect's alibi, such as technical problems or synchronisation issues?

4. **Conclusion (BBC, 25 April, 2017):**

In assisting the police investigation in the case of Richard Dabate, digital forensics was essential. The Fitbit data contributed significantly to the prosecution's case against the defendant by offering solid evidence that refuted his account of the incident. The methods and techniques used in this investigation met the strictest forensic requirements.

5**. Glossary:**

Terms used in this report are as follows **(BBC, 25 April, 2017)**:

Fitbit:

A wearable fitness tracker that collects health and activity data such as steps, heart rate, and sleep habits.

Digital forensics:

The collection, preservation, and analysis of digital data in order to investigate and find evidence in judicial disputes.

Prosecution:

In a criminal proceeding, the legal side is in charge of presenting evidence and pressing accusations against a defendant.

Alibi:

In a criminal proceeding, a claim or evidence made by a defendant to indicate that they were not there at the site of the accused crime when it occurred.

Tampering:

Unauthorised or unauthorised adjustments or interference with physical or digital evidence, frequently done to conceal or misrepresent the truth.

Expert witness:

A specialised specialist who is asked to testify in court to offer views, analysis, or explanations in a certain subject.

Timeline of events:

A thorough record of when certain activities or situations occurred based on a chronological sequence of happenings.

Forensically sound:

A word used to define digital forensic practises and approaches that preserve the integrity and dependability of evidence.

Chain of custody:

A trail of evidence that chronicles its custody, transfer, and management to ensure its integrity and admissibility in court.

7. **Acknowledgements:**

We acknowledge the law enforcement agencies,forensic experts, Fitbit, prosecution team, victims family, the court and the combined efforts of all the team members (Viraj,Jagsir and Shehbaz) for all the research and help in order to finish and finalise this report.

8. **Appendixes:**

This report includes a thorough summary of the steps taken, the evidence gathered, and the expert witness testimony in addition to summarising the crucial role those digital forensics played in the Richard Dabate investigation. Data from the Fitbit gadget was a key piece of the digital evidence, which was crucial in this case.

# References

***BBC. ( 25 April, 2017). Fitbit contradicts husband's story of wife's murder - police. Available at: <***[***https://www.bbc.com/news/world-us-canada-39710528***](https://www.bbc.com/news/world-us-canada-39710528)***>***

***Helen, M. (2020). Internet-enabled medical device data introduced as evidence of arson and insurance fraud. USA. Available at:<***[***https://ccybers.org/wp-content/uploads/2022/11/State-of-Ohio-v.-Ross-Compton-Internet-enabled-medical-device-data-introduced-as-evidence-of-arson-and-insurance-fraud.pdf***](https://ccybers.org/wp-content/uploads/2022/11/State-of-Ohio-v.-Ross-Compton-Internet-enabled-medical-device-data-introduced-as-evidence-of-arson-and-insurance-fraud.pdf)***>***