WITNESS STATEMENT

CJ Act 1967, s.9; MC Act 1980, ss.5A(3)(a) and 5B; Criminal Procedure Rules 2005, Rule 27.1

Statement of Sahifa Syed ..... URN: | | | | |

Age if under 18 Over 18 ..... (if over 18 insert 'over 18') Occupation: Student Forensic Investigator.....

This statement (consisting of: ....**3**..... pages each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated anything in it which I know to be false, or do not believe to be true.

Signature: Sahifa SYED..... Date: 15/12/2023.....

Tick if witness evidence is visually recorded ☐ *(supply witness details on rear)*

I am Sahifa Syed, a first-year Cyber Security and Digital Forensics student at the University of the West of England. As a student in this course, I am gaining a comprehensive understanding of the principles and practices of both cyber security and digital forensics. The curriculum covers a vast scope of subjects such as programming in c++, introduction to databases and computer crime and digital evidence. Currently, I am actively involved in conducting investigations and gaining hands-on experience to further enhance my skills in the field of digital forensics. This allows me to develop and expand on critical thinking, problem-solving, and analytical skills necessary for successful digital forensic examinations. By actively participating in real-world scenarios and practical exercises, I am able to apply the theoretical knowledge gained in the classroom to real-life situations. It also provides me with the opportunity to work with different types of digital devices and explore various forensic tools and techniques, ultimately preparing me for a successful career in the field of cyber security and digital forensics.

At **17:20 HRS on 23/10/2023**, I commenced my examination in relation to **Case XP R V HUNTER**. Evidence of my findings can be found in my produced exhibits **SS1: Forensic Report** & **SS2: Evidence record.**

I started my investigation by verifying the contents of the evidence file, **"Hunter XP for Dongled v6.E01"**. I was able to verify the contents of the evidence files with zero errors. Verifying the contents allows me to be sure that the data contained within the image has remained unchanged and its original state has not been altered.

I used two forensic tools, EnCase and Autopsy. I performed most of the investigation using EnCase and verified all the information and found evidence using Autopsy. This is called dual verification and this allows all the information on both tools to be compared to establish accuracy and clear any doubts or discrepancies.

Using EnCase I managed to recover lost folders which are also known as deleted files. Using Autopsy I verified the process, ensuring the folders were correctly recovered and were in working order.

Using EnCase I mounted archive files. Archive files consists of zip files, thumbs etc. I used EnCase's functionality option and expanded the compound files. The expanding of compound files enables access for all file types. This means that everything within EnCase is now decompressed.

Using EnCase I managed to determine the correctness of the MD5, SHA and entropy value. I used EnCase's functionality option and enabled the file signature analysis and hash analysis option. File signatures can help programs read a file when its extension has been changed or misidentified. Hash analysis can reliably tell us when two files are identical. It is important to mention that throughout the investigation process, the SHA value was not initially shown in both tools when the case was uploaded, and this absence persisted.

Signature: ..... Signature witnessed by: .....

Continuation of Statement of .....

I then determined what user activity has been taken place on the computer, this is called profiling. This involves collecting information which has been stored in the Operating Systems (**OS**) main database, also known as the registry. Within the registry I recovered information related to the system artefacts, time zone, user accounts and various other registry records.

System Artefacts consists of specifics about the computer in use such as the product name, ID, which version in use and a timeline of the install and shut down dates. This gave me a timeline to work with, however it is worth mentioning that there is still a possibility of file activity after the given shutdown date and time as they can be easily manipulated either intentionally or due to errors.

In order for me to gain a better understanding of the timeframe of my investigation I had to modify the time zone on my computer. I modified the time zone information to Central Standard Time (CST) which is accurately aligned with the current case. This enabled me to ensure and understand the correct timestamps of my investigation.

A user account is an identity created for a user in a computer or a computing system. The user accounts on the device gave me insight about three different users: administrators, Bob Hunter, and a guest account. This gave me information about whether these accounts were built into the system or not , if they have permission to access all types of resources (files, networks, etc..) and the timestamps of their last logins.

I also analysed the registry and its protected area. I analysed the registry which consists of a number of 'hive' files. These hive files: software, system, sam and security were taken out from EnCase and analysed on the application called Registry Viewer. They held vital information relevant to the case. For the registry protected area, I analysed NTUSER.dat files by downloading an application called 'RegRipper' from the sway. NTUSER.dat files help create rough timeline during forensic investigations and detect file timestamp tampering. They are also valuable for uncovering evidence of file execution or access, as well as reassembling user activity. From my analysis I was able to find relevant information such as the LastWrite Time, LastVisitedMRU , MRU list and the Last directory.

Additionally within the registry records I was able to find out what types of external drives were attached to the device. I found USB drives which are considered as external drives to be attached to the computer. All of this data was found to be present under the registry, offering a comprehensive view of the devices system configurations.

During the investigation I determined whether the device was protected by a password or not. This was done by downloading an application called 'saminside' which aided me in concluding that the device was not password protected. This meant that the device was accessible by anyone.

I was then able to determine that the computer had been used by a user to access the Internet. I was able to recover evidence to suggest that internet had been used to browse various urls that consisted of stalking related websites. I also recovered some notable emails some of which were deleted as well and this seemed to be of great relevance to the case.

From the results I found from the internet history and emails I expanded my investigation further by performing a comprehensive keyword search. This process involved me using terminology related to stalking, words such as 'stalking, stalker, stalk, money' were searched. This search resulted in various files appearing that could be of potential evidence related to the case.

I also determined if there was user interest in encryption by performing an entropy analysis and viewing relevant .log files. Encryption is the method by which information is converted into secret code that hides the information's true meaning. Entropy analysis involves evaluating the degree of randomness present in data in which EnCase assigns an entropy value to each folder and file. Higher entropy values indicate a higher chance of encryption. I focused on files with entropy values from 6 to 7. I examined the hex representation of the files with the highest entropy values and found one false positive, an MZ executable file that turned out to be an archive file. This method guarantees a thorough investigation into the possibility of encryption within the dataset.

Signature: ..... Signature witnessed by: .....

Continuation of Statement of .....

I carried out an in-depth examination of various instant messaging clients (IM), including Yahoo IM. Under the Yahoo IM records, I discovered a series compelling evidence in the form of IM texts from certain individual and this holds significant relevance to the case.

I also investigated the use of CD/DVD burning apps within the device by searching and viewing particular files such as program files, .log files, and prefetch files. I was able to simplify my search by 'green plating'. This process allows me to select the relevant data in order to find the said files. While searching through the files, I was able to decode a file called Hunter.log that contained a conversation about money, which could be important evidence for the case.

I was also able to determine what print artefacts were being used on the device by viewing/examining the spool files. Spool files saves the data of a file that is meant to be printed. I identified a notable file sent to the printer. I was also able to find out the specifications about the printer in use. The contents of the file and the printer information seemed to be of relevance and potential evidence to the case.

Additionally , I was able to locate and retrieve a large number of temporary files that a user had sent from the computer to be printed. I was able to decode these files and recover evidence relating to stalking and blackmailing activity.

I was able to identify and examine more potential evidence related the case by data carving the files. Data carving allows you to recover files that are not indexed by the file system such as hidden files which are placed in unallocated spaces or deleted files. I found files that were important to the case. It included mail sent from the device to the parent of the individual as it referred to the term 'daughter' more than once a well as images being sent of a woman who does not seem to know that someone is taking pictures of her.

I was able to recover and ensure the integrity of the Recycle Bin files and to verify the 'absence of any bypass'. By verifying the absence of any bypass allowed me to ensure that the files and the data within them in the recycle bin were free of any attacks, flaws or changes and they were all intact. Amongst the files in the Recycle Bin, I recovered a noteworthy file called "Sabrina Derwercs".This name has been repeated multiple times throughout noteworthy emails and pictures found, therefore it seemed of relevance to the case.

I also examined different file types. I utilized EnCase's functionality option and filtered my search allowed me to find files based on their file extensions. An extension is a suffix added to the name of a file to indicate the file's layout, in terms of how the data within the file is organized. I viewed and found multiple files that seemed of significance to the case and may be seemed as potential evidence.

I then determined whether or not any wiping utilities were used on the device. I mainly examined various types of files with the .log or .exe extensions. Once these file types were located I found indications of wiping utilities being in use within the computer. If a wiping utility was in use, it is to intentionally erase a certain amount of data and prevent recovery of it. This seemed of high relevance to the case and an important discovery to be stated.

I attest that the information provided in this witness statement is true and accurate to the best of my knowledge. All of the above is my own work and the evidence found has not been tampered with.

Signature: ..... Signature witnessed by: .....

Witness contact details

Home address: .....

..... Postcode: .....

Home telephone number ..... Work telephone number .....

Mobile/pager number ..... Email address: .....

Preferred means of contact: .....

Male / Female (delete as applicable) Date and place of birth: .....

Former name: ..... Ethnicity Code (16+1): ..... Religion/belief: .....

Dates of witness non-availability .....

.....

Witness care

a) Is the witness willing and likely to attend court? Yes / No. If 'No', include reason(s) on **MG6.**

b) What can be done to ensure attendance?

c) Does the witness require a Special Measures Assessment as a vulnerable or intimidated witness? Yes / No. If 'Yes' submit **MG2** with file.

d) Does the witness have any specific care needs? Yes / No. If 'Yes' what are they? (Disability, healthcare, childcare, transport, , language difficulties, visually impaired, restricted mobility or other concerns?)

Witness Consent (for witness completion)

a)	The criminal justice process and Victim Personal Statement scheme (victims only) has been explained to me	Yes ☐	No ☐			
b)	I have been given the Victim Personal Statement leaflet	Yes ☐	No ☐			
c)	I have been given the leaflet 'Giving a witness statement to police — what happens next?'	Yes ☐	No ☐			
d)	I consent to police having access to my medical record(s) in relation to this matter: (obtained in accordance with local practice)	Yes ☐	No ☐	N/A ☐		
e)	I consent to my medical record in relation to this matter being disclosed to the defence:	Yes ☐	No ☐	N/A ☐		
f)	I consent to the statement being disclosed for the purposes of civil proceedings e.g. child care proceedings, CICA	Yes ☐	No ☐			
g)	The information recorded above will be disclosed to the Witness Service so they can offer help and support, unless you ask them not to. Tick this box to decline their services:		☐			

Signature of witness: ..... Print name: .....

Signature of parent/guardian/appropriate adult: ..... Print name: ....

Address and telephone number if different from above: .....

Statement taken by (print name): ..... Station: .....

Time and place statement taken: .....