Name: Stephen Wharton
Specialist field: Cyber Security
On behalf of Thomas Sheckles

Post Module Assignment Submission form

MODULE TITLE: Digital Forensics

MODULE CODE: WM046-10 (CSM)

MODULE DATES: 15 to 19 February 2021

STUDENT ID NUMBER (2096386):

Name: Stephen Wharton
Specialist field: Cyber Security
On behalf of Thomas Sheckles

Expert Witness Report

Court reference number: 93467

Final report of *2096386* for the Birmingham County Court

Dated	***22/03/2020***
Specialist field:	*Cyber Security.*
On behalf of the Claimant/ Defendant (or both if single joint expert):	*Thomas Sheckles.*
On the instructions of:	*The name of the solicitors who have instructed you.*
Subject matter:	***Assault Charge Investigation***

Your Name: ***2096386***
Address:
Telephone Number:
Fax number/Email:
Reference:

Contents

Report

1 Introduction

1.1 The writer

I am Stephen Wharton. My specialist field is in Cyber Security, with a strong emphasis on digital forensics. I hold a MSc in Cyber Security and Management from WMG – University of Warwick. My prior professional experience involves performing digital forensics investigations on a multitude of devices, ranging from laptop hard drives, and dashcams.

Full details of my qualifications and experience entitling me to give expert opinion evidence are in appendix 1.

1.2 Summary background of the case

The case concerns newly found information allegedly linking a case of assault to a man named Thomas Sheckles, targeted towards his ex-wife. The assault took place at the ex-wife’s house, located at Station Rd, Harborne, Birmingham B17 9LP on December 5th, 2019, Thursday approximately at 9:51 P.M.

Prior to this incident, Sheckles was subjected to multiple court orders, those being listed below:

Court Order 1 – Section 5 (Granted on 1st August 2019)

(a) Prohibited from entering 1.5-mile radius of ex-wife's house.

(b) Can only travel between 09:00 and 17:00 hours.

(c) Must drive with a dashcam that records the GPS coordinates of each journey without being interrupted.

Court Order 2

Must drive with a speed limiter, with the maximum speed permitted being 40mph.

In his interview pertaining to the case, Sheckles stated the following:

1. He has not traversed near his ex-wife's house.
2. Has left the dashcam unaltered.
3. Has not breached Court Order 1
4. Has not breached Court Order 2

I have been instructed to examine a seized dashcam, identified as IMK/2 to gather digital evidence from Sheckles journeys to determine whether Sheckles statements given in the interview are valid. If not, provide the evidence which contradicts a statement made in his initial interview.

1.3 Summary of my conclusions

After investigating the dashcam IMK-2, I have concluded that Thomas Sheckles has ---

Broken the following court orders:

- Court Order 1 (a)
- Court Order 1 (b)
- Court Order 2

Despite breaking these court orders, we could not fully conclude with confidence that Sheckles was the exact perpetrator of the assault on his ex-wife.

-

1.4 Those involved.

Mr. Thomas Sheckles – The main subject in this investigation.

Mr. Sheckles Ex-Wife – Thomas' ex-wife, assault victim of this case. Is a cleaner by profession working in multiple locations across Birmingham. Typical work week is from Friday to Tuesday, having Wednesday and Thursday as days off.

Crown Prosecution Service (CPS) – Provided the restraining order charge to Sheckles. Communicates with police during different stages of the investigation.

Senior Officer – The officer who entrusted us with the task of examining IMK/2, provided the issues which will be discussed later in the document.

1.5 Technical terms and explanations

I have indicated any technical terms in **bold type**. I have defined these terms when first used and included them in a glossary in appendix 8. I have also included in appendix 5 extracts of published works I refer to in my report, and in appendix 6 there are diagrams and photographs to assist in the understanding of the case.

2 The issues to be addressed and a statement of instructions.

After the dashcam device was seized from Sheckles car, authorities had difficulties in properly examining the device for investigative purposes. The team who imaged the file has no experience in performing a digital forensics investigation. My professional experience was sought out to carry out this investigation.

2.1 The purpose of the report.

The main purpose of this report is confirming the validity of Sheckles claims that he was not responsible for the assault on his ex-wife, given in his prior interview with law enforcement. To investigate these claims, we will address the issues that will be addresses later with the report with gathered information.

Investigation Issue 1: Did Sheckles contravene Court Order 1 – Section 5 (a), if so where did he go?
Investigation Issue 2: Did Sheckles contravene Court Order 1 – Section 5 (b)
Investigation Issue 3: Did Sheckles contravene Court Order 1 – Section 5 (c)
Investigation Issue 4: Did Sheckles contravene Court Order 2
Investigation Issue 5: Did Sheckles alter with the dashcam in anyway which could be disguising his movements?
Investigation Issue 6: Did the dashcam record all journeys made, if not, why was it tampered with?
Investigation Issue 7: Was the speed limit maintained at 40mphs?
Investigation Issues 8: Do we have evidence showing Mr. Sheckles is responsible for the assault on his ex-wife on December 5th?

3 My investigation of the facts

This section will clearly outline the steps and precautions taken to gather the date that will be used in investigation. Firstly, before examining IMK/2 for its files and content, it is of utmost importance to create an environment in which it can be safely and securely be operated on. To achieve this, a Windows 10 **virtual machine (VM)** was created, with its networking functionalities disabled. This in effect will create an airtight environment without the influence other software or potential. In addition, a VM can easily be disposed off once the investigation has been concluded.

The following pieces of software were used to perform the investigation.

- **Exiftool**
- **Autopsy**
- **Sublime Text**
- **GPXSee**
- **MyNextBase Player**
- **Command Line**

The mentioned software, except for Command Line were downloaded locally on the main host machine, scanned for malware and viruses.

Due to the lack of internet connectivity on the VM, the above software with the exception of the command line which comes preinstalled on Windows was downloaded locally on the main host machine. After being downloaded, the files were scanned for viruses and malware, then dragged and dropped into the virtual machine securely.

We start this investigation by using **Autopsy**. This program allows us to mount IMK/2 and gain a further insight into the files stored on it.

Breakdown of file contents of the IMK/2 disk image

- 7 Images
- 382 Videos
- 1 json Files
- 3 octet-stream Files
- 6 x-sqilite3 files
- 3 xml files
- 1 x-log file

There are 21 total deleted files. **The breakdown of those files being:**

- 14 deleted videos
- 0 deleted Photos
- 4 deleted sqlite3 files
- 1 .temp file
- 1 .bin file
- 1 .xml file

When analysing the unsaved videos files, we can observe that the first dashcam recording was on 03/12/2019 and the last taking place on 06/12/2019, as seen on Figure 1 and 2, respectively. These dates all take place after Court Order 1 (c), that being from the 01/08/2019.

Now that we have access to all the files, they will be extracted to be used for the investigation. The main files of interest are the video files, so these will be extracted and placed into their own folder for future purposes. In addition, the downloaded program will be placed in this same folder.

By using the command prompt and changing the directory to that of the videos, we can utilize Exiftool commands to view the **metadata** of our files. We are most interested in the following pieces of information.

- Latitude
- Longitude
- Date and Time

The latitude and longitude metadata will denote the exact location Sheckles has been on his car journeys, while the date and time will tell us when they happened.
To extract this information from the videos, a command was run which outputted these results to a **GPX** file.

```
Exiftool -ee -p gpx.fmt "$gpslatitude, $gpslongitude, $gpsdatetime" C:\Users\Investigation \Documents\DashcamVids > output.gpx
```

To have a better, graphical representation of this data, GPXSee is used. As well as showing us Sheckles' journey taking, it provides us a speed graph, showing us his speed in miles per hour across his journeys.

3.1 Assumed facts.

While the metadata provided by Exiftool provides us with the most important information for this investigation, much can be gained from viewing the Autopsy program. In particular, the deleted files remaining on the image. A feature of Autopsy is to recover files that were not properly deleted, as in most cases, the files maintain on the given storage medium despite being seemingly deleted.

With the deleted files, there are multiple ways to speculate as to why they were deleted. Firstly, it could be assumed that the files were deleted intentionally by Sheckles himself, as means to delete evidence that could be used against him. Secondly, with reference to the Garmin Dashcam 55 Owner's Manual, the oldest undeleted files on the system are deleted whenever space is needed for new footage[i].
However, when examining the modified time of the deleted files as seen in Figure 3, this statement does not line up. When ordering the modified time of both deleted and preserved files, there seems to be an intentional deletion of the files.

3.2 Enquiries/investigation into facts by the expert

Earlier, we used the gather metadata to output a graph of Sheckles' route taken, as seen in Figure 4. Glancing at the produced speed graph it is evident that although Sheckles has not been abiding by Court Order 2 and exceeded 40 mph numerous times. With this, we can see that the functioning speed limiter on Sheckles' car has either been overwritten or has not been placed to begin with.

Referring to Figure 5, the wiped time-based metadata from files raised concern. This is not something which can be deleted from a dashcam device. Despite this being removed, we can still extract the geospatial metadata using Exiftool. When playing the videos in My**NextBase Player** we can still see the embedded coordinates of the files as seen on Figure 7.

3.3 Interview and examination

There were no interviews conducted for this investigation past the initial one.

4 My opinion

When reviewing the investigation, we have found substantial evidence that shows that Thomas Sheckles was not being truthful in the initial interview.
When discussing Investigation Issue 1, the graph shows that he indeed did pass by a 1.5-mile radius of his ex-wife's house. The dash-camera images as seen on Figure 8 and 9 show proof that Sheckles has broken Court Order 1 (b) on at least two separate occasions.

The deletion of the .mov files and their time related metadata strongly suggests Sheckles trying to hide his traces. Considering when the files were created there is no feasible way for the files to have been deleted without it being done manually. Even so, the deletion of metadata would not occur unless he went out of his way to do so. This answer both Investigation Issue 5 and 6, Sheckles being guilty for both.

The speed graph shown clearly outlines that Investigation Issue 7 was not meet. While analysing the videos, the speed limit was maintained most of the time, this still counts as a breach of Court Order 2.
Most importantly, is that of Investigation Issue 8. While Sheckles has broken the other Court Orders, we could not find proof that linked him to the assault on his ex-wife that occurred on 05/12/2019.

Appendix

Technical Terms

Virtual machine (VM): An emulation of an operating machine

Command Line: A Windows based interface which allows execution of commands, must be utilized to use Exiftool

Exiftool: A command line-based program which grants different commands to extract information from images and videos. In this scenario, we wish to extract the geospatial information from our exported videos

Autopsy: A digital forensics software that enables us to view disk images in further depth. Allows exporting of files.

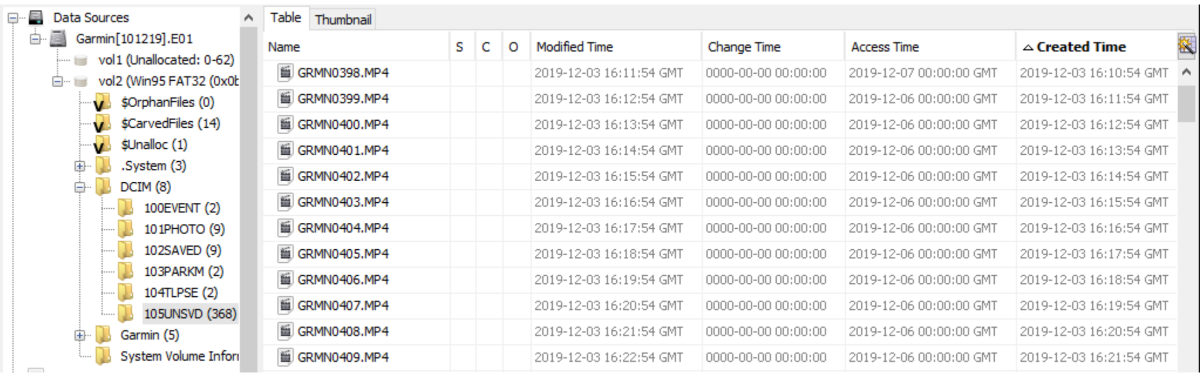
Sublime Text: A text editor which can view various file formats, used to read, and edit .gpx files
GPXSee: Software that creates graphical representations of geospatial data. This is the software which we use to view the speed graph and travel path of Sheckles.

GPX: This stands for GPS Exchange Format. This file format (.gpx) is what is used to store geospatial data, in this scenario, Mr. Sheckles driving routes. Our outputted file should denote the longitude, latitude, and time for the journey of each video

MyNextBase Player: A dashcam viewing video software that can play deleted dashcam footage.

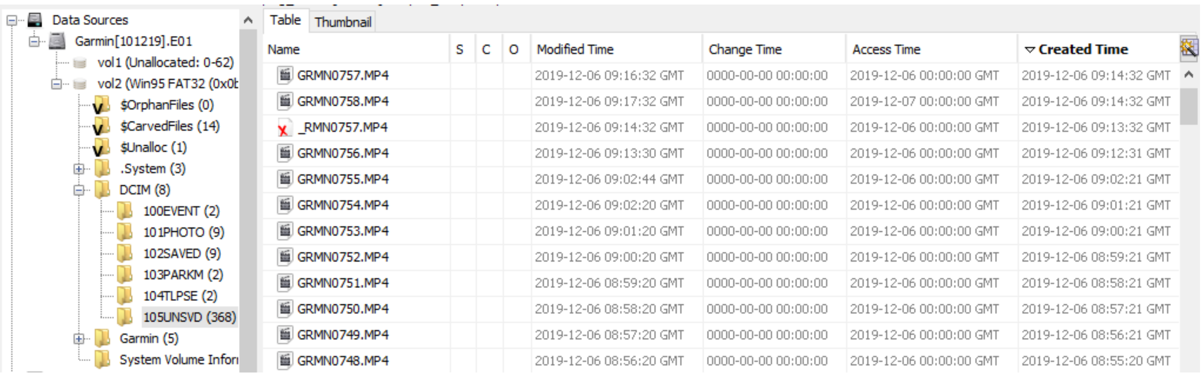
Metadata: Data that gives descriptive information about data

Photos



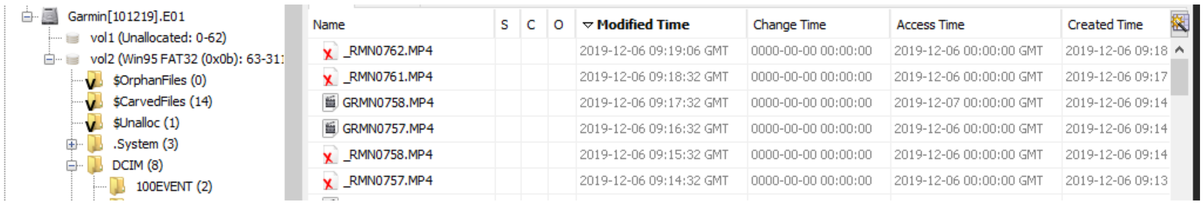
Name	S	C	O	Modified Time	Change Time	Access Time	△ Created Time
GRMN0398.MP4				2019-12-03 16:11:54 GMT	0000-00-00 00:00:00	2019-12-07 00:00:00 GMT	2019-12-03 16:10:54 GMT
GRMN0399.MP4				2019-12-03 16:12:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:11:54 GMT
GRMN0400.MP4				2019-12-03 16:13:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:12:54 GMT
GRMN0401.MP4				2019-12-03 16:14:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:13:54 GMT
GRMN0402.MP4				2019-12-03 16:15:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:14:54 GMT
GRMN0403.MP4				2019-12-03 16:16:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:15:54 GMT
GRMN0404.MP4				2019-12-03 16:17:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:16:54 GMT
GRMN0405.MP4				2019-12-03 16:18:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:17:54 GMT
GRMN0406.MP4				2019-12-03 16:19:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:18:54 GMT
GRMN0407.MP4				2019-12-03 16:20:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:19:54 GMT
GRMN0408.MP4				2019-12-03 16:21:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:20:54 GMT
GRMN0409.MP4				2019-12-03 16:22:54 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-03 16:21:54 GMT

Figure 1 – First Video Files Sorted



Name	S	C	O	Modified Time	Change Time	Access Time	▽ Created Time
GRMN0757.MP4				2019-12-06 09:16:32 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:14:32 GMT
GRMN0758.MP4				2019-12-06 09:17:32 GMT	0000-00-00 00:00:00	2019-12-07 00:00:00 GMT	2019-12-06 09:14:32 GMT
_RMN0757.MP4				2019-12-06 09:14:32 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:13:32 GMT
GRMN0756.MP4				2019-12-06 09:13:30 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:12:31 GMT
GRMN0755.MP4				2019-12-06 09:02:44 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:02:21 GMT
GRMN0754.MP4				2019-12-06 09:02:20 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:01:21 GMT
GRMN0753.MP4				2019-12-06 09:01:20 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:00:21 GMT
GRMN0752.MP4				2019-12-06 09:00:20 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 08:59:21 GMT
GRMN0751.MP4				2019-12-06 08:59:20 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 08:58:21 GMT
GRMN0750.MP4				2019-12-06 08:58:20 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 08:57:21 GMT
GRMN0749.MP4				2019-12-06 08:57:20 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 08:56:21 GMT
GRMN0748.MP4				2019-12-06 08:56:20 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 08:55:20 GMT

Figure 2 – Latest Video Files Sorted



Name	S	C	O	▽ Modified Time	Change Time	Access Time	Created Time
_RMN0762.MP4				2019-12-06 09:19:06 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:18
_RMN0761.MP4				2019-12-06 09:18:32 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:17
GRMN0758.MP4				2019-12-06 09:17:32 GMT	0000-00-00 00:00:00	2019-12-07 00:00:00 GMT	2019-12-06 09:14
GRMN0757.MP4				2019-12-06 09:16:32 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:14
_RMN0758.MP4				2019-12-06 09:15:32 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:14
_RMN0757.MP4				2019-12-06 09:14:32 GMT	0000-00-00 00:00:00	2019-12-06 00:00:00 GMT	2019-12-06 09:13

Figure 3 – Modified Time Sorted

Name: Stephen Wharton
Specialist field: Cyber Security
On behalf of Thomas Sheckles

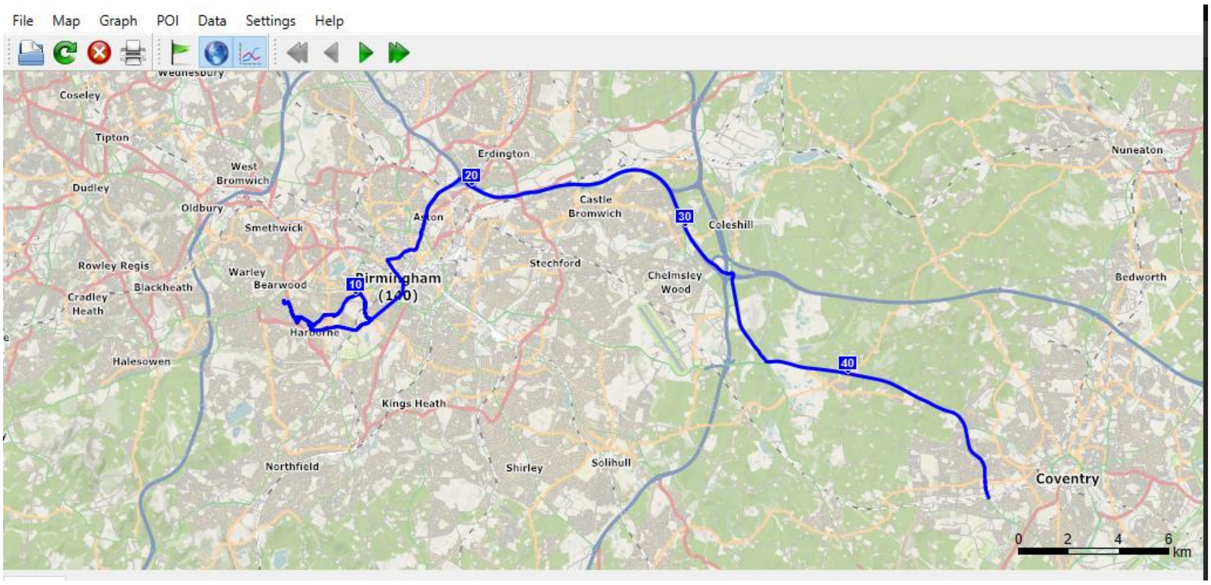
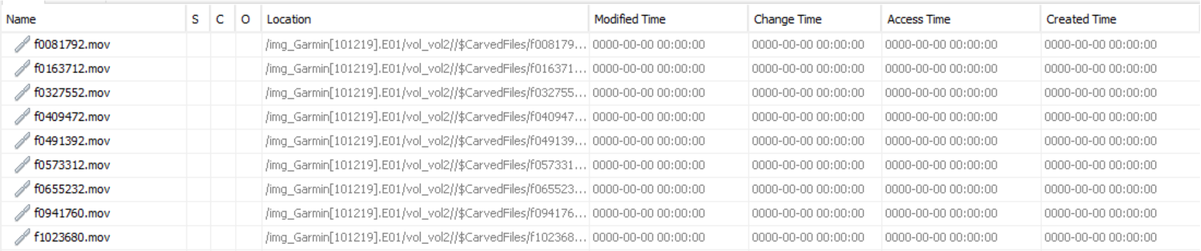


Figure 4 – Sheckles' Journey Graph



Name	S	C	O	Location	Modified Time	Change Time	Access Time	Created Time
f0081792.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f008179…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0163712.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f016371…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0327552.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f032755…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0409472.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f040947…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0491392.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f049139…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0573312.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f057331…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0655232.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f065523…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0941760.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f094176…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f1023680.mov				/img_Garmin[101219].E01/vol_vol2//$CarvedFiles/f102368…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Figure 5 – Deleted Time Metadata

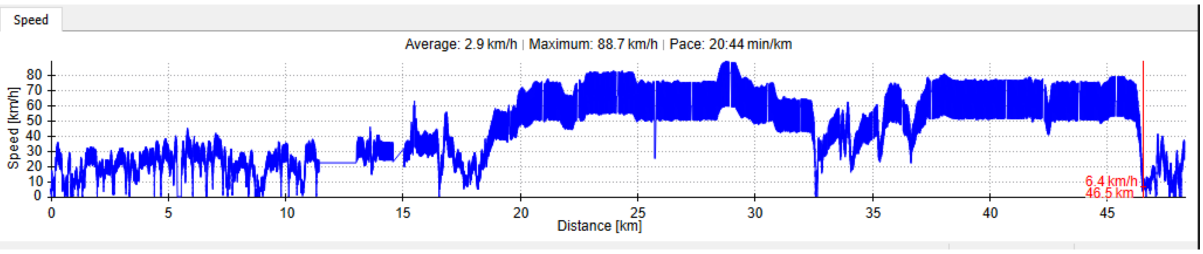
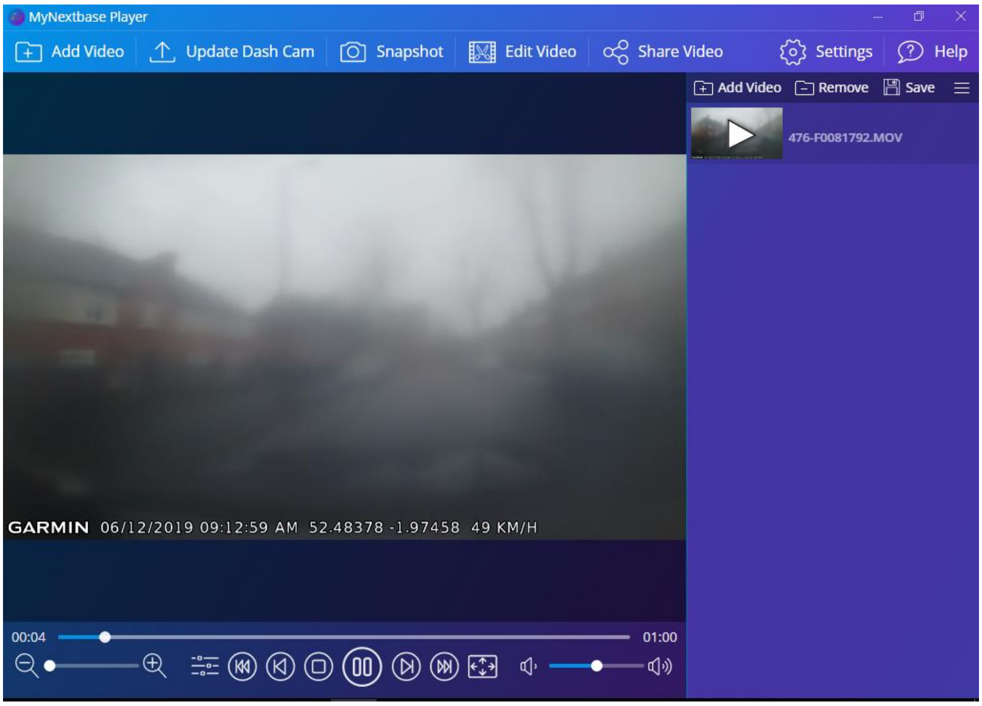


Figure 6 – Speed Graph



GARMIN 06/12/2019 09:12:59 AM 52.48378 -1.97458 49 KM/H

Figure 7 – Embedded Co-ordinates

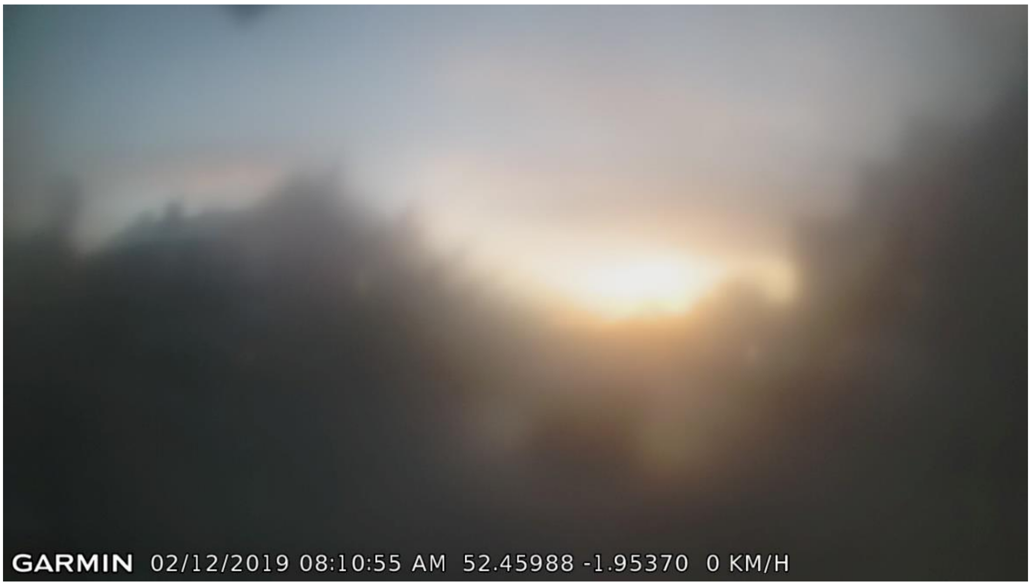


Figure 8 – Court Order 1 (b) Violation

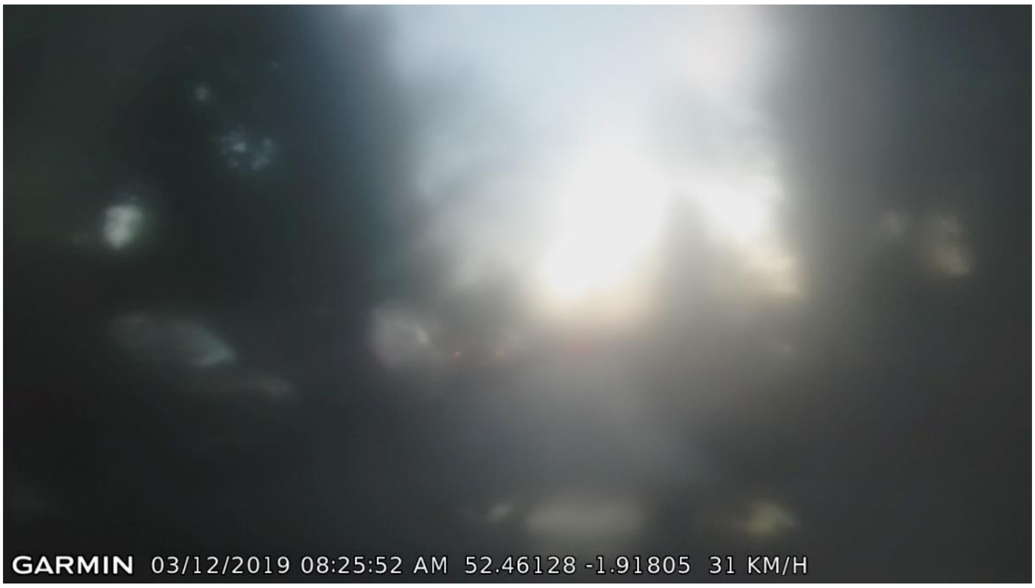


Figure 9 – Court Order 1 (b) Violation

Name: Stephen Wharton
Specialist field: Cyber Security
On behalf of Thomas Sheckles

Statement of conflicts

I confirm that I have no conflict of interest of any kind, other than any which I have already set out in this report. I do not consider that any interest which I have disclosed affects my suitability to give expert evidence on any issue on which I have given evidence and I will advise the party by whom I am instructed if, between the date of this report and the trial, there is any change in circumstances which affects this statement.

Statement of compliance

I understand my duty as an expert witness to the court to provide independent assistance by way of objective unbiased opinion in relation to matters within my expertise. I have complied with that duty and will continue to comply with it. I will inform all parties and where appropriate the court in the event that my opinion changes on any material issues. I further understand that my duty to the court overrides any obligation to the party from whom I received instructions. Parts 33.2 (1), (2) and (3) and 33.4(j) Criminal Procedure Rules

Declaration of Truth

This statement consisting of......... pages, 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 willfully stated in it anything which I know to be false or do not believe to be true.

Statement of conflicts

I confirm that I have no conflict of interest of any kind, other than any which I have already set out in this report. I do not consider that any interest which I have disclosed affects my suitability to give expert evidence on any issue on which I have given evidence and I will advise the party by whom I am instructed if, between the date of this report and the trial, there is any change in circumstances which affects this statement.

Signature………Stephen…Wharton……………………………………………

Date…22/03/2021…………

All reports must be signed and dated, and the Statement/Declaration of Truth must be verified by a signature/date. Therefore, you are advised to include your Statement/Declaration of Truth as your final item in the report, and to follow it with your signature and the date.

Name: Stephen Wharton
Specialist field: Cyber Security
On behalf of Thomas Sheckles

[i] https://www8.garmin.com/manuals/webhelp/dashcam45-55/EN-US/DashCam_45-55_OM_EN-US.pdf