Witness Name: NATHAN SHAW

Statement No: WITN0386001

Dated: 2nd February 2026

THE NOTTINGHAM INQUIRY

FIRST WITNESS STATEMENT OF NATHAN SHAW

I, NATHAN SHAW, will say as follows:-

INTRODUCTION

1. I am employed by West Yorkshire Police as a Cyber Security Analyst in Digital Policing.

2. This witness statement is made to assist the Nottingham Inquiry with matters set out in the Rule 9 Request dated 8th January 2026.

BACKGROUND

3. I was employed as a Digital Investigator from 2017 to 2025.

4. At the time of examination, I was a trained and certified Digital Investigator with over 6 years experience in digital forensics.

5. At the time of examination, I had received the following training:

Training Course	Completed Date
GrayKey Tips & Tricks	26/04/2023

Control-F App Investigator 1	15/02/2023
GrayKey Operator	16/01/2023
Introduction to Cryptocurrency	11/11/2022
Oxygen Forensics	04/11/2021
CSI Tech Cryptocurrencies for Investigators	06/10/2021
Certified Mac Forensics Specialist	01/09/2021
Certified Linux Forensic Practitioner (CLFP)	30/07/2021
Axiom AX250	10/01/2021
Cellebrite Premium	09/09/2020
Python Scripting 1	20/11/2019
Control-F eMMC	05/07/2019
Control-F Defeating Android Locks and Encryption	21/06/2019
Axiom AX200	17/05/2019
X-Ways 2	09/05/2019
Control-F Smartphone App Forensics	01/02/2019
Control-F Advanced Smartphone & Tablet Acquisition	25/01/2019
Cellebrite CCO & CCPA	13/12/2018
XRY Intermediate	15/11/2018
X-Ways 1	22/03/2018

CSI Tech RAM Analysis	08/03/2018
DFIR370 - Host Intrusion Methodology and Investigation	15/12/2017
DF420 - MAC Examinations with EnCase	08/12/2017
DF220 - Navigating EnCase version 8	13/10/2017
DF410 - NTFS Examinations with EnCase	06/10/2017
Foundation in Mobile Phone Forensics	22/09/2017
DF320 - Advanced Analysis of Windows Artifacts with EnCase	25/08/2017
DFIR350 - Internet based Investigation with EnCase	18/08/2017
IR250 - Incident Investigation	21/07/2017
DF210 - Building an Investigation with EnCase	23/06/2017
IACIS Basic Computer Forensic Examiner (BCFE)	12/05/2017
DF120 - Foundations in Digital Forensics with EnCase	28/04/2017

6. Mobile phone examinations was a large part of my role which I conducted daily. My competency was tested and verified through the ISO17025 accreditation associated with the Digital Investigations lab I worked in.

EXAMINATION OF EXHIBIT JR/11

7. I have been asked to provide dates on which images, videos and documents referred to in a report made by DC Small of Nottinghamshire Police (NGPF0003744) were downloaded and potentially viewed by Valdo Calocane using the mobile device known as exhibit JR/11. In accordance with the request made by the Inquiry, I have focussed on those items which relate to violence, drugs, child exploitation and state surveillance.

8. On the morning of 13th June 2023, the attacks by Valdo Calocane were deemed a Marauding Terrorist Attack (MTA). This immediately initiated 'Op Plato' which is the UK's national protocol response to a Marauding Terrorist Attack (MTA). This immediately fell to CTPNE (Counter Terrorism Police North East), due to being in the region that we cover. CTPNE works under a local host force. The host force for CTPNE is West Yorkshire Police. Subsequently, after the attack was deemed not to be terrorist activity all assistance was handed back over to the local force (Nottinghamshire).

9. On 14 June 2023 I retrieved exhibit JR/11 from the Digital Investigations secure store. I conducted a forensic examination which resulted in a forensic download of the device.

10. This examination consists of retrieving the exhibit from secure store and ensuring continuity is completed, isolating the exhibit from the network, connecting the exhibit to a forensic workstation, using forensic tools and strategies to connect to the exhibit, downloading the data from the device and finally repackaging and resealing the exhibit. Photographs are taken throughout the examination, and the forensic download was stored on the Digital Investigations Unit secure server.

11. For the purposes of making this statement, the forensic download has been re-examined to identify items within the parameters of the Inquiry's request. A copy of a table showing the analysis of relevant items has been exhibited as NGPF0010324 – File information of relevant media.

12. As the exhibit JR/11 is an Android device, it uses an Android filesystem. This means files are generally not given a "Created Date and Time" and instead the "Modified Date and Time" is used as this reference.

13. Where the file name contains the phrase "embedded", this indicates the file was embedded within another file and was separately extracted by forensic software. Therefore, the user does not have immediate access to this file and the file does not have a direct creation or modified time and date.

14. I have exhibited a copy of the image of what appears to be Cannabis plants in a large room under a number of lights as NGPF0010325 – Image

relating to drugs (1). This file is cached (I refer to paragraph 16 below). The timestamp of this file is 13/03/2022 09:46:19(UTC+0). This was the time and date it was cached. A reverse image search was performed for this file, and results show that it is available on the internet.

15. I have exhibited a copy of the image of what appears to be a large quantity of drugs in various bags on a tile floor as NGPF0010326 – Image relating to drugs (2). This file is cached (I refer to paragraph 16 below). The timestamp of this file is 27/02/2023 15:06:06(UTC+0). This was the time and date it was cached. A reverse image search was performed for this file, and results show that it is available on the internet.

16. Caching is an automatic process performed by a device to improve the user experience. An example of this is when a user accesses a website, content from that website is automatically downloaded to the device in a location that the user cannot access. This happens because if the user decides to access that website again, the device doesn't have to redownload all the content again, it is already on the device and speeds up the website loading process. Users are not informed of this process happening. What this indicates forensically, is that when cached images are found on a device, the user did not download them knowingly, but their contents will have appeared on the device through user interaction at some point.

17. Two images were identified as potential indecent images. These have been assessed and graded by a trained grader and are determined not to be images of children.

Statement of Truth

I believe the content of this statement to be true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief of its truth.

Signed: GRO-B

Dated: 2nd February 2026

Index to First Witness Statement of NATHAN SHAW

No.	URN	Document Description
1	NGPF0003744	Letter from DC 4299 Hayley Small to SIO Operation Hendrix re: Reference: Op Hendrix, Review of download, JR/11 Extraction 1
2	NGPF0010324	Copy of NS1.xlsx
3	NGPF0010325	NS2.jpg
4	NGPF0010326	NS3 (002).jpg