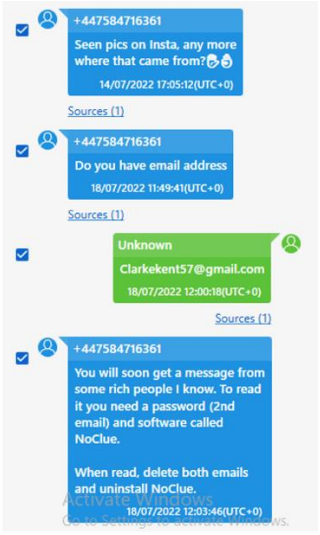
Dr John Kingston

Investigator Information:
The following report was conducted by Tomiwa Oladejo. The role given to me is to provide verified facts using the evidence provided.

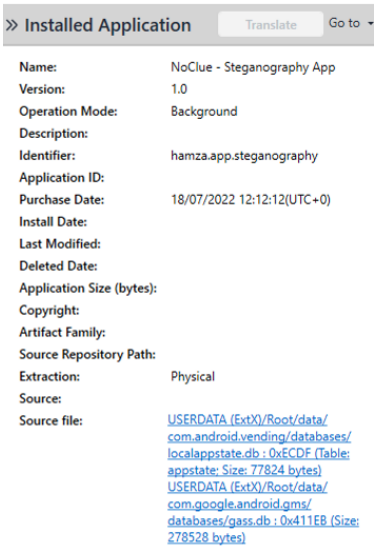
Case Description:
A student is being investigated under the premise of trespassing and is under suspicion of planning a theft of one or more valuable items from the stately home.

Computer and Forensic Tool Statistics:
The suspect's phone was seized and two forensic images of it were made using Cellebrite software. The images are a Physical image and an Advanced Logical image. Cellebrite physical analyser was used for the examination of the Physical image.

Investigation:
Statement: Planning a theft is denied
To begin the search for evidence, I looked through various records on the phone to locate records indicating a theft was planned. As a result of looking through the text messages, I was able to find a conversation between the individual and an unsaved number.



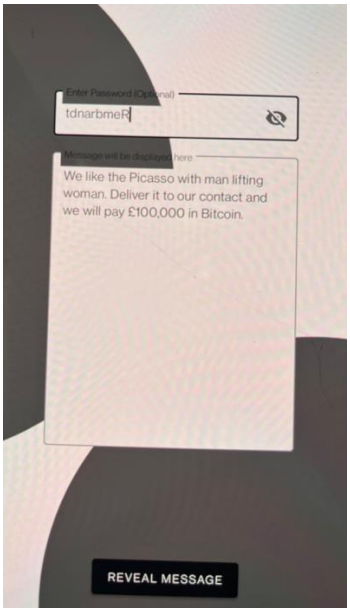
The unknown number references his Instagram, showing an interest in the contents. The individuals email address is then requested and he sends the email "Clarkekent57@gmail.com". This shows that the user of the phone's email is Clarke Kent. As a response, the number informed him he will receive a message soon.



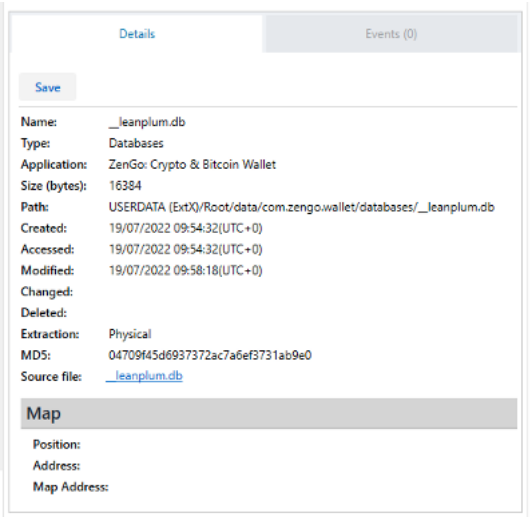
» Installed Application Translate Go to

Name:	NoClue - Steganography App
Version:	1.0
Operation Mode:	Background
Description:	
Identifier:	hamza.app.steganography
Application ID:	
Purchase Date:	18/07/2022 12:12:12(UTC+0)
Install Date:	
Last Modified:	
Deleted Date:	
Application Size (bytes):	
Copyright:	
Artifact Family:	
Source Repository Path:	
Extraction:	Physical
Source:	
Source file:	USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db : 0xECDF (Table: appstate: Size: 77824 bytes) USERDATA (ExtX)/Root/data/com.google.android.gms/databases/gass.db : 0x411EB (Size: 278528 bytes)

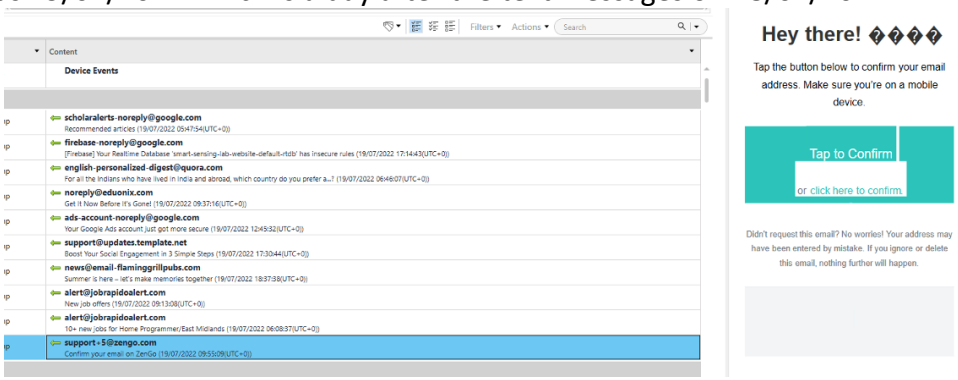
To delve deeper into the events that took place, I searched the phone for the key word “NoClue”. It was found that shortly after the conversation took place, the individual had installed the NoClue application. After finding the password given to the individual, the message that was sent was revealed.



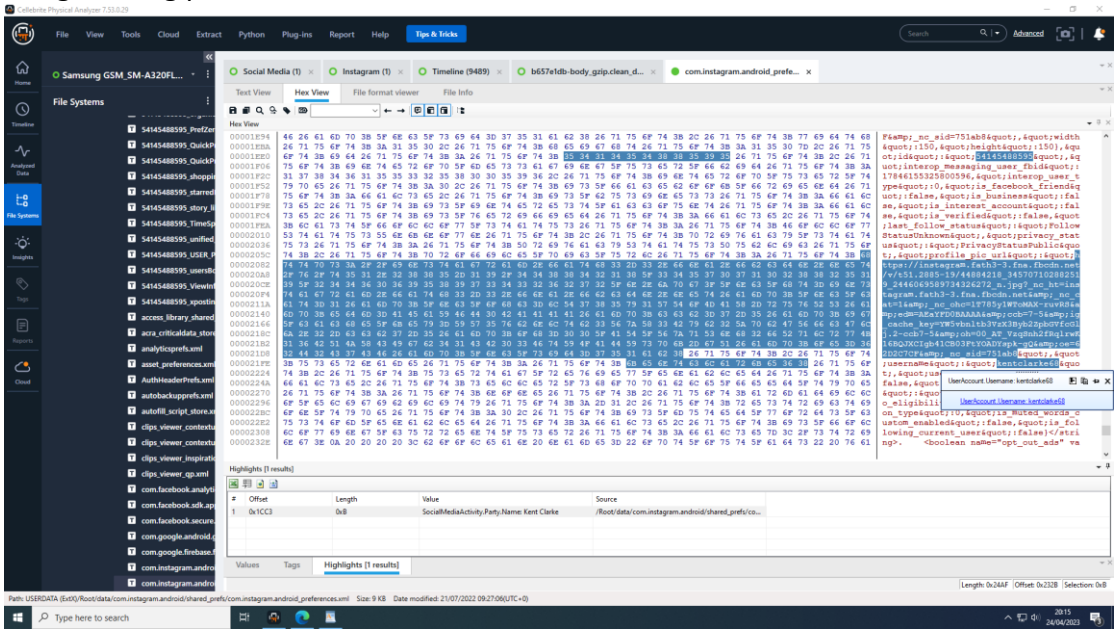
He was offered 100,000 bitcoin if he was able to successfully break into the property and steal the Picasso with the man lifting the woman. The individual then messaged the unknown number once again asking if they are the one who sent him the offer and stating he will contemplate making the deal.



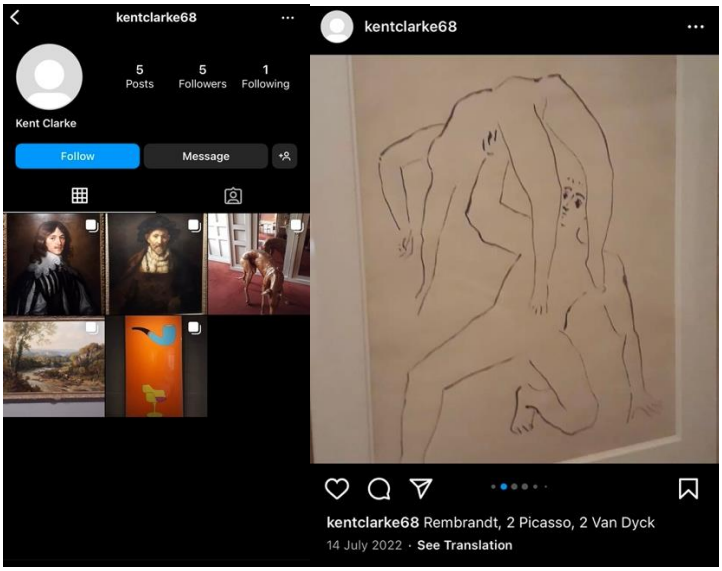
Following the offered being received, he accessed a crypto wallet named zengo. The date of access was 19/07/2022 which is a day after the text messages on 18/07/2022.



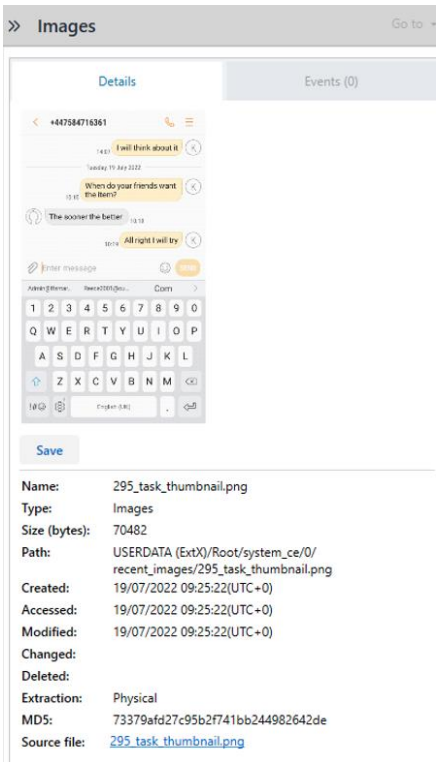
After taking a look into his emails, it was found that he created an account with the wallet. The creation of an account suggests he had an intent to take up the offer.
I decided to look into his Instagram account as the unknown number showed an interest in the images being posted.



To find the locate the name of the Instagram account, I searched the hex code in hex view. I was able to locate the username, kentclarke68, and find the account on Instagram. The account had a number of images inclusive of drawings, paintings and sculptures.



The image of the man lifting the woman matches the description given through the no clue application.



After further exploration, a screenshot was found in the images. Observing the screenshot, more messages being sent back and forth seemingly between the individual and the unknown number. The phone number in the screenshot matches the number shown earlier in the messages with the individual. During the conversation, he states he will attempt to carry out the act of theft for the painting. This occurs the same day he creates the account for the crypto wallet.

The next day (20/07/2022), the web history revealed he was searching for balaclava's on ebay and ways to hire a van. Additionally, there is search history of methods to disable cctv cameras and renting a mirai bot. Mirai bots are a form of malware used to infect smart devices and like smart cameras and home routers. The history points towards him planning his method of infiltration into the stately home and with how he intended to getaway.

Statement: That the individual is a student at Nottingham Trent University

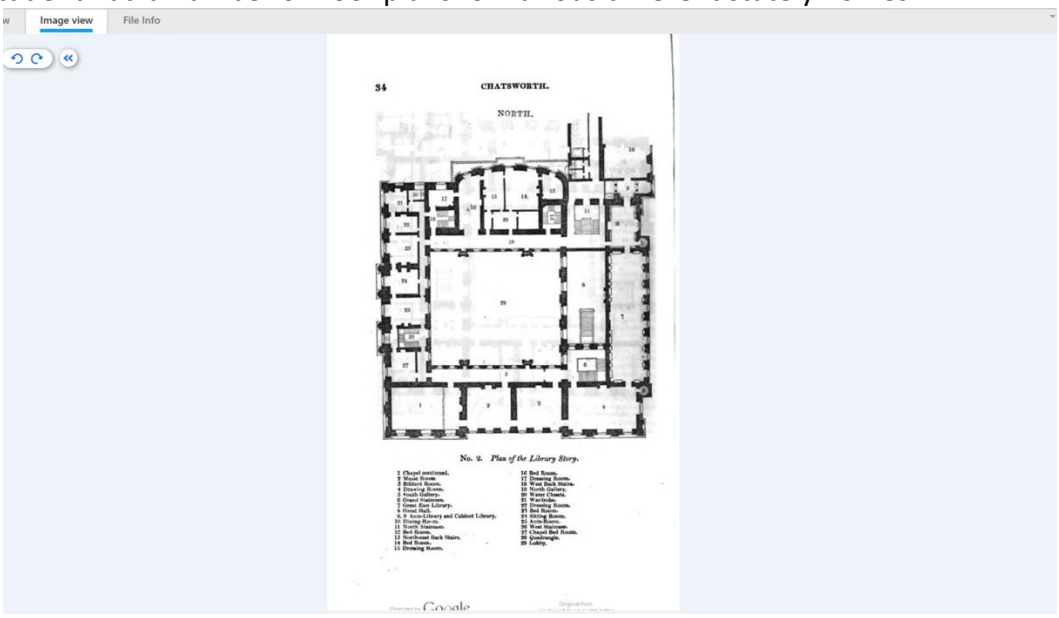
To figure out whether or not he is a student at NTU, I searched through emails which may potentially provide a lead on this matter. There was no email indicating the individual is a student at the university. I then decided to transverse through the call history texts, but there was no proof. However, when checking the web history, it was found that on 18/07/2022 a login was made onto NTU now.

☑	3		Web History	LastVisited	**Nottingham Trent University Online Workspace (NOW)** http://now.ntu.ac.uk/
☑	4		Web History	LastVisited	**Nottingham Trent University Online Workspace (NOW)** https://now.ntu.ac.uk/
☑	5		Web History	LastVisited	**Homepage - NTU Online Workspace** https://cas.ntu.ac.uk/d2lcas_cloud/copyright/copyright.aspx?TARGET=
☑	6		Web History	LastVisited	**Homepage - NTU Online Workspace** https://cas.ntu.ac.uk/d2lcas_cloud/copyright/copyright.aspx?TARGET=
☑	7		Web History	LastVisited	**Sign In** https://fs.ntu.ac.uk/adfs/ls/?wtrealm=https%3A%2F%2Fcas.ntu.ac.uk%2Fd2lcas_cloud%2Fcopyright%2F&wctx=WsFedOwinState% YquBjWoawsg8oU47X5N93iaepe2KTKe8Yyqt3zFGv5-NCMm8ak38AWeInke-tWBBgkcp3rp70tQjxkiicbPG-oqy-byOk8IhjstuOupuMv
☑	8		Web History	LastVisited	**Working...** https://fs.ntu.ac.uk/adfs/ls/?wtrealm=https%3A%2F%2Fcas.ntu.ac.uk%2Fd2lcas_cloud%2Fcopyright%2F&wctx=WsFedOwinState% YquBjWoawsg8oU47X5N93iaepe2KTKe8Yyqt3zFGv5-NCMm8ak38AWeInke-tWBBgkcp3rp70tQjxkiicbPG-oqy-byOk8IhjstuOupuMv id=8116a0a9-e869-4247-a732-0080010000af
☑	9		Web History	LastVisited	**Not authorised - NTU Online Workspace** https://now.ntu.ac.uk/d2l/lp/auth/login/ssoLogin.d2l?guid=itsqPTLdEqyf0nxo4RBnOsvkQQJWcb818nKVcxuA- dGzqbh79__c47GM7P5lEqb57IWlkfHXY0qGdneMjaUdz3cxFSkrrFrO4fRpInz1tBWyro5vOMAe_dFggRNqQwEYityCjOJXS14c0B8Cg1- SB9uXxfDWe4Nc2aJRLKIj8i_5hrZit9LNd_aZSpkvElvZnbTzPMKvaDYOZ1Qh3-OzqFVpIqIRdTTJc3LcyaUCdjiObTZ43- dvII24T9SXwHHp8ZRricTtz0aR2ZWWgkdBfDvq7BLRjrht22O6N32K6qsHHAI9bkurkU_Egqnodkw_4SoifbUi-zu-3s0oxS2Th_D5vmHM WxffIo8Wdhf_GHI4pAW3I0F2kTsTuhUWVnpBU3tMIGgfok5VT9tMmQmACdJ9R5L1THiYhtKpbcCu4neljaHqh5QpeTXvoBSXQVC1P84 LeAjxH0UQ5GuN3TN2qybKpEJsxAxHdk2djhjPs3CTotfELxYNI6yMho.&username=RC189120&orgID=&target=
☑	10		Web History	LastVisited	**Not authorised - NTU Online Workspace** https://now.ntu.ac.uk/d2l/error/403
☑	11		Web History	LastVisited	

The individual should not be capable of logging into the NTU website is they do not own any credentials. An NTU calendar was also discovered on the device, which would serve no purpose to the student if they were not a student.

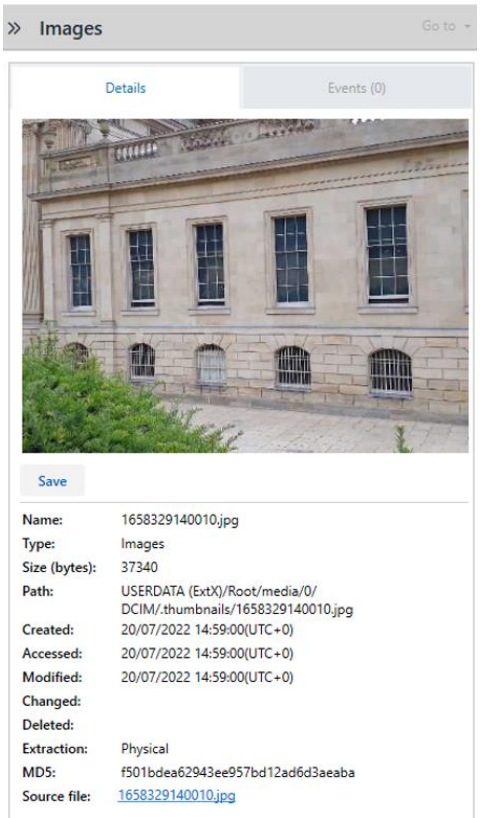
That the student has visited the stately home twice

The student had a number of floor plans for various different stately homes.

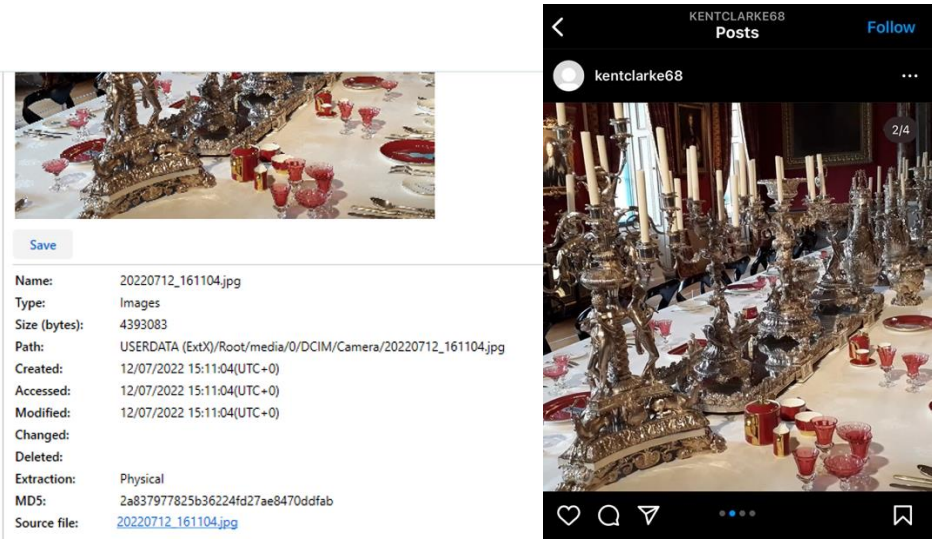


A floorplan for Chatsworth stately house was found in the catalogue of images. The floorplan alone is not enough proof to convict him of this statement, so I decided to search for an image of the stately home.

After searching google for an image of the Chatsworth, I found an image displaying the building's architecture. I realised the windows in on the building looked similar to an image previously seen.



The image above was taken on the 20/07/2022, which is the same day the web history shows specific searches such as the van hire, and mirai bots, were made. There are also images of cctv cameras which were taken on this day and the colour of the cement matches the stately home. The existence of the image also proves he was at the home on this day. To confirm whether he had been at the stately home at an earlier date, I continued investigating the images. I then came across an image which was posted on the kentclarke68 Instagram.

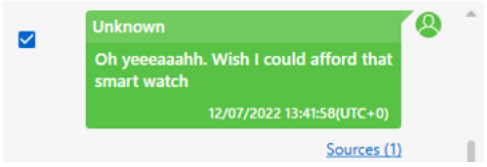


The two images shown above are identical to one another. This sparked an idea to search for the interior design of Chatsworth house as if the interior matches then it would mean the student had visited the stately house, Chatsworth, twice in the space of a few weeks.

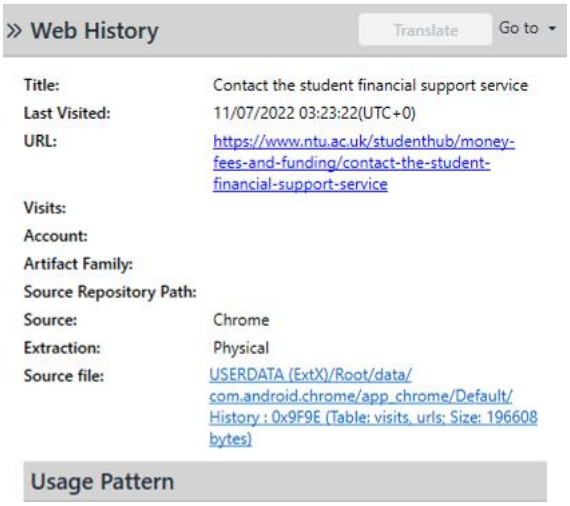
When comparing the interior design within the Chatsworth house image located on the internet and the image on the individual's Instagram, it is clear that the layout, background and other themes are identical. As a result, it could be said that he did visit the stately home twice, with the first visit occurring on the 12/07/2022, and the next on the 20/07/2022.

<u>Statement: That the student is happy with his current life and has no need to carry out theft</u>

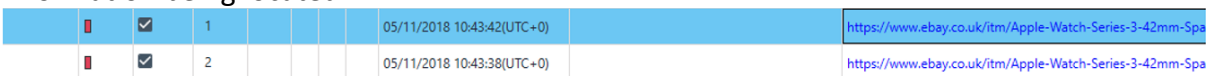
Earlier in the investigation, the individual mentioned he wishes he owned an apple watch within a text message. This <u>message was sent on 12/07/2022.</u>



After further investigation I also discovered the individual had been searching for information regarding student financial support. The web history of the student financial support service suggests he required money as he did not have enough to sustain himself.

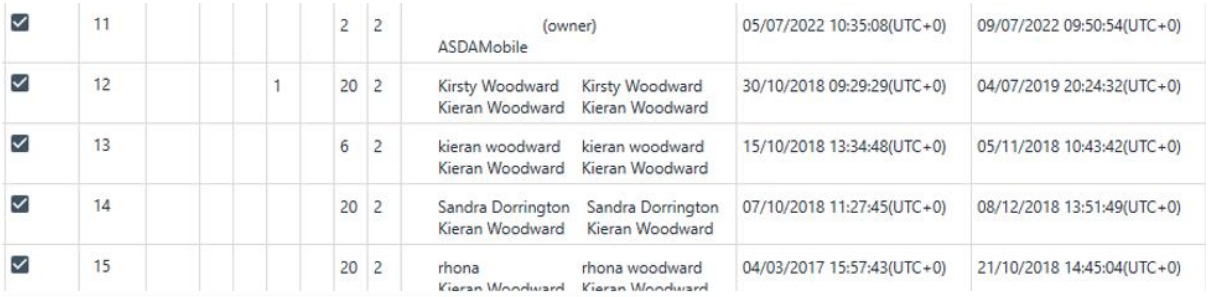


The date the search occurred is 11/07/2022, which is a day before he was contacted by the person who offered a sum of money. In an attempt to find more information on this matter, I used the keyword watch as a basis for the search. The search resulted in additional information being located.



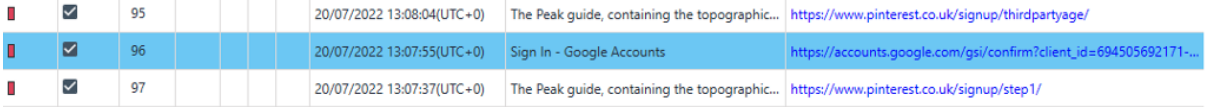
On 05/11/2018, there were searches related to apple watches which connects to the earlier text message regarding smart watches. The individual appears to have been unhappy financially for a while, giving him reason to carry out theft.

Moreover, as the eBay search and the text message seem to be connected, it is supposedly the same person. However, the search occurred during 2018. The user during this time period was Kieran Woodward.



As displayed in the screenshot above, Kieran Woodward is assumed to have possessed the phone before the current user Clarke Kent. I created a theory that Kieran and Clarke are the same individual.

In an attempt to prove this, I looked into the sign in history of both accounts. It was found that on the 20/07/2022, a switch between google accounts took place.



After delving deeper into the account activity and user history, I discovered Clarke Kent logged back into the device on the 21/07/2022. This is a day after the previous switch in accounts.

#	Identifier	Serial number	Name	Created	Last logged in	Restrictions	Gro
1	0	0	Kent Clarke		21/07/2022 09:26:1...		

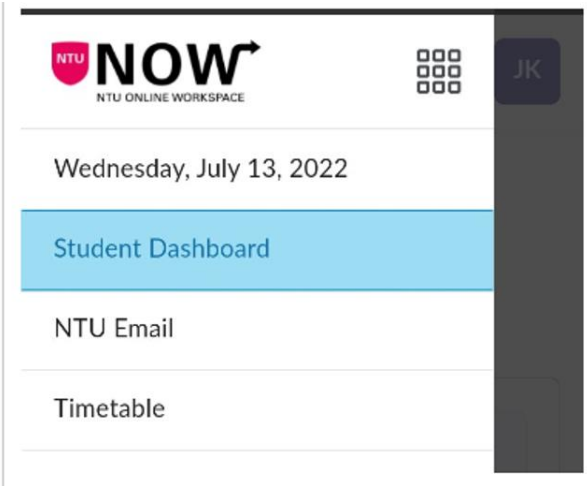
This could potentially confirm that Kieran and Clarke are the same person. Kieran may have created the alias Clarke as a way to change his identity.

<u>Statement: That the student obtained his phone from someone else at his university and so any illegal content must have been uploaded by the previous owner(s).</u>

For the identification of the owner of the phone and the phone's history, I had to first take a look at when it was activated.

Advertising ID #1	1eabf24d-343a-48d6-b596-70a1a8e012bd	adid_settings.xml : 0x99
Android fingerprint	samsung/a3y17ltexc/a3y17lte:7.0/NRD90M/A32...	build.prop : 0x590
Bluetooth MAC Address	48:27:EA:B1:72:72	bt_addr : 0x0
Android ID	1ea156ed0ae13650	settings_secure.xml : 0x4345
Bluetooth device address	48:27:EA:B1:72:72	settings_secure.xml : 0x5375
Bluetooth device name	Galaxy A3 (2017)	settings_secure.xml : 0x3D8B
Carrier Name	No service	telephony.db : 0x3FED
Detected Phone Model	SM-A320FL	build.prop : 0x2B7
Detected Phone Vendor	samsung	build.prop : 0x2D2
Location Services Enabled	True	googlesettings.db-wal : 0x1F7E0E
Mock locations allowed	False	
OS Version	7.0	build.prop : 0x134
SIM Change Operation	1	SimCard.dat : 0x2F
Factory number	RF8J62SK77R	serial_no : 0x0
ICCID	89441000304301063257	com.android.phone_preferences.xml : 0xEE8
IMEI	359751081442373	2400257.cfg : 0x108
IMSI	234159400201276	Checkin.xml : 0x8BF
Mac Address	48:27:EA:B1:72:73	.mac.info : 0x0
Phone Activation Time	31/12/2016 17:00:00(UTC+0)	
Recovery Event	01/01/2017 12:00:02(UTC+0)	last_log.2 : 0xFC
Recovery Event	16/03/2018 13:35:14(UTC+0)	last_recovery : 0x7B13
Recovery Event	18/03/2018 04:12:24(UTC+0)	last_log : 0x9B
SIM Change Time	20/09/2017 00:11:38(UTC+0)	SimCard.dat : 0xE
Time Zone	(UTC+00:00) London (Europe)	persist.sys.timezone : 0x0

The phone was first activated on the 31/12/2016 at 17:00:00. There was a previous user of the device whose email was "kelvinjayden@gmail.com". The user is expected to be a former NTU student as there is an image with their initials on the NTU now page. I found the screenshot within the images file.



As a result of looking through the text message history, I was able to locate the messages received about his sim card from the network. These messages informed him on things such as accessing his data abroad and instructions for browsing the internet using picture messaging. Additionally, there is a message received from google stating the number is being verified on the device as part of the setup. All of the messages are received on 05/07/2022, indicating this date is when the users were switched.

	2		Chats	StartTime Messages	**Chat: ASDAMobile** ASDAMobile=> : To browse the mobile internet and use picture messaging, we will shortly be sending you a text with some settings (05/07/2022 10:35:08(UTC+0))
	3		Chats	StartTime Messages	**Chat: 2732** 2732=> : Hi, we'd like to make sure your phone can access data abroad if you're planning to travel this summer. We've previously sent settings to your phone which should already be installed. Sometimes these settings may have been missed - please visit http://mobile.asda.com/APN for info on how to check you have the correct settings before you travel. We'll also be resending settings to you in the next few weeks. Please follow the instructions in the message when you receive these. (05/07/2022 12:03:45(UTC+0))
	4		Chats	StartTime LastActivity Messages	**Chat: +447537452518** =>To: +447537452518 : (XfInbkIn6Ifr) Google is verifying the phone# of this device as part of setup. Learn more: https://goo.gl/LHCS9W (05/07/2022 15:47:27(UTC+0))
	5		Chats	StartTime Messages	**Chat:** To browse the mobile internet and use picture messaging, we will shortly be sending you a text with some settings (05/07/2022 10:35:08(UTC +0))
	6		Chats	StartTime Messages	**Chat: 2732** 2732=>: Hi, we'd like to make sure your phone can access data abroad if you're planning to travel this summer. We've previously sent settings to your phone which should already be installed. Sometimes these settings may have been missed - please visit http://mobile.asda.com/APN for info on how to check you have the correct settings before you travel. We'll also be resending settings to you in the next few weeks. Please follow the instructions in the message when you receive these. (05/07/2022 12:03:45(UTC+0))

As the date of 05/07/2022 is the expected date users were switched, this means the illegal content was not uploaded by the previous user. A vast majority of illegal content on the phone was uploaded after this date, pointing towards the student as the person who uploaded the content. However, the student did obtain this phone from someone else at the university.

Conclusion:

Throughout the report, information relating to the individual's case has been outlined. It can be said that there is a plethora of evidence against the individual regarding this case. Evidence has shown that a theft has been planned and the individual is a student at Nottingham Trent University. They are also expected to have visited the stately home twice. My role is only to present the facts as I have found them presented to me on the given phone. It is now up to the judge to decide whether or not the provided evidence is enough to convict the suspect.