HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:16/03/2020

2020/131 - Digital Device Analysis

In response to your recent request for information regarding;

Although excess cost removed the forces obligations under the Freedom of Information Act, as a gesture of goodwill, I have supplied information, relative to your request, retrieved or available before it was realised that the fees limit would be exceeded. I trust this is helpful, but it does not affect our legal right to rely on the fees regulations for the remainder of your request.

1. How many of the following types of devices you have seized in the 2015, 2016, 2017 and 2018 calendar years:
*** Mobile phones**
*** Desktop computers**
*** Laptop computers**
*** Tablets**
*** External hard drives or storage devices**
*** Other digital devices**
(or if you do not break down devices into these categories please specify your own)

Our information is set up and searchable for our policing purposes. To obtain the information in the format you have requested would involve manually reviewing each record on our force system to ensure relevance. The cost of providing you with the information is above the amount to which we are legally required to respond i.e. the cost of retrieving the information exceeds the 'appropriate level' as stated in the Freedom of Information (FOI) Fees and Appropriate Limit regulations 2004.

Therefore, in accordance with the FOI Act 2000 the information you have requested is exempt under Section 12 (1), and this letter acts as a Refusal Notice under section 17 (5) of the legislation.

2. How many of the following types of devices have been subject to data extraction or some other kind of digital forensic investigation in the 2015, 2016, 2017 and 2018 calendar years:
*** Mobile phones**
*** Desktop computers**
*** Laptop computers**
*** Tablets**
*** External hard drives or storage devices**
*** Other digital devices**
(or if you do not break down devices into these categories please specify your own)

Please see attached previous FOI response **2019/045** '*Forensic examination of digital devices*'.

3. The purpose of the data extraction or digital forensic investigation – ie. if it was related to a particular type of crime. Please specify this as a number: ie. how many investigations were for one type of crime and how many for another type.

2016
FRAUD 9
Adult attempt to meet a girl under 16 years of age following grooming 3
Make indecent photograph /psuedo-photograph of a child 3
Murder 2
Posses a prohibited image of a child 10
Rape a woman 16 years of age or over 1
Sexual assault on a female 3
Posses indecent photograph / pseudo-photograph of a child 2
Dishonestly fail to disclose information to make a gain for self / another or cause / expose other to a loss 1
Fraud by false representation1
Unauthorised use of a computer to facilitate the comission of an offence 1
IIOC 166
N.A 4
RAPE 12
SEXUAL ASSAULT 24
THEFT 2
VOYEURISM 3

2017
FRAUD 1
Adult attempt to meet a girl under 16 years of age following grooming 44
Arson 1
Attempt to distribute an indecent photograph / psuedo-photograph of a child 5
Burglary Dwelling - theft / attempt theft with violence 1
Distribute an indecent photograph / psuedo-photograph of a child 18
Make indecent photograph /psuedo-photograph of a child 70
Manslaughter 1
Murder 12
Posses a prohibited image of a child 27
Rape a woman 16 years of age or over 16
Robbery 1
Sexual assault on a female 18
Attempt to supply a controlled drug of class A 7
Posses extreme pornographic image portraying act of intercourse/oral sex with an animal 1
Posses indecent photograph/pseudo-photograph of a child 61
Attempt to posses a controlled drug 2
Cause a computer to perform function to secure / enable unauthorised access to a program/ data 2
Dishonestly fail to disclose information to make a gain for self / another or cause / expose other to a loss 1
Fraud by abuse of position 1
Fraud by false representation12
Send letter / communication / article conveying indecent / offensive message 6
Unauthorised computer access with intent to commit other offences 1
Unauthorised use of a computer to facilitate the comission of an offence 1
IIOC 4
RAPE 1
SEXUAL ASSAULT 1

2018
Adult attempt to meet a girl under 16 years of age following grooming 52
Aggravated Burglary - Dwelling 11
Arson 4
Attempt to distribute an indecent photograph / psuedo-photograph of a child 7
Burglary Dwelling - theft / attempt theft with violence 28

Cause death by dangerous driving 3
Cause death by dangerous driving without due care/consideration while unfit through drugs 1
Cause serious injury by dangerous driving 8
Distribute an indecent photograph / psuedo-photograph of a child 22
Make indecent photograph /psuedo-photograph of a child 104
Murder 9
Posses a prohibited image of a child 21
Rape a woman 16 years of age or over 90
Robbery 28
Sexual assault on a female 58
Attempt to supply a controlled drug of class A 131
Cause death by dangerous / inconsiderate driving 3
Posses an extreme photographic image portraying an act which threatened life 1
Posses extreme photographic image portraying act which likely to result in serious injury to a person's private parts 1
Posses extreme pornographic image portraying act of intercourse/oral sex with an animal 3
Posses indecent photograph / pseudo-photograph of a child 34
Attempt to posses a controlled drug 21
Burglary other than dwelling 24
Cause a computer to perform function to secure / enable unauthorised access to a program / data 5
Conspire to make / supply article for use in fraud 1
Criminal damage to property 8
Dishonestly fail to disclose information to make a gain for self / another or cause / expose other to a loss 1
Fraud by abuse of position 5
Fraud by false representation 14
Participate in fraudulent business carried on by a sole trader 1
Posses / Control article for use in fraud 1
Send letter / communication / article conveying indecent / offensive message 40
Unauthorised computer access with intent to commit other offences 4

<u>2019</u>
Adult attempt to meet a girl under 16 years of age following grooming 36
Aggravated Burglary - Dwelling 7
Arson 13
Attempt to distribute an indecent photograph / psuedo-photograph of a child 4
Burglary Dwelling - theft / attempt theft with violence 38
Cause death by dangerous driving 3
Cause death by dangerous driving without due care/consideration while unfit through drugs 2
Cause serious injury by dangerous driving 18
Distribute an indecent photograph / psuedo-photograph of a child 14
Make indecent photograph /psuedo-photograph of a child 97
Manslaughter 6
Murder 7
Posses a prohibited image of a child 28
Rape a woman 16 years of age or over 72
Robbery 22
Sexual assault on a female 72
Attempt to supply a controlled drug of class A 214
Posses extreme pornographic image portraying act of intercourse / oral sex with an animal 3
Posses indecent photograph / pseudo-photograph of a child 33
Attempt to posses a controlled drug 35
Burglary other than dwelling 23
Cause a computer to perform function to secure / enable unauthorised access to a program / data 1
Criminal damage to property 11
Fraud by abuse of position 6

Fraud by false representation23
Posses / Control article for use in fraud 3
Send letter / communication / article conveying indecent / offensive message 46
Unauthorised computer access with intent to commit other offences 2
Unauthorised use of a computer to facilitate the comission of an offence 2

To safeguard any ongoing and/or future counter terrorism investigations we are applying a partial NCND in accordance with sections 23(5) Security Bodies, 24(2) National Security, and 31(3) Law Enforcement.

Rationale for the partial NCND:
Section 23(5) – Information supplied by, or relating to, bodies dealing with security matters - Under s23(5) the duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would involve the disclosure of any information (whether or not already recorded) which was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3). This is an absolute exemption and a public interest test is not required.

Section 24(2) – National security - Section 24(2) is a qualified exemption and as such there is a requirement to evidence any harm in confirming or denying that any other information is held as well as considering the public interest. As such, we appreciate the importance of the public being informed on the pro-active response of the police from a counter terrorist perspective, and it is no secret that digital extraction of electronic media devices is pursuant of that task. In addition, confirming whether any other information regarding such digital forensic activity is or has been conducted would increase public confidence and allow for better informed public debate. However, disclosure under the FoI Act 2000 is a disclosure to the world at large. Therefore, disclosure of the information, if held, runs the risk of providing criminals with information or indeed confirmation, that counter terrorism investigations are, or are not, currently being undertaken by specific forces, which acts as intelligence to those with mal-intent and is therefore likely to have an undesirable effect on the national security of UK overall. This would in turn, have an impact on the ability of local forces and the UK to protect itself from terrorist related criminality and increases the risk to the safety of its citizens. Confirming or denying whether any other information is held would have the effect of making security measures states less effective since it may highlight vulnerabilities within individual forces. To the extent that section 24(2) applies, NPFDU has determined that in all the circumstances, the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in confirming whether or not any other information is held.

Section 31(3) - Law Enforcement – As mentioned already, we recognise the importance of the public being informed on the pro-active counter terrorist posture of the police, and that it is no secret that digital extraction of electronic media devices is pursuant of that task. However, modern-day policing is intelligence led and by its very nature, digital forensic testing has a tendency to reveal more exploitable opportunities above and beyond evidence gathering for a single investigation. Therefore, from a counter terrorist perspective, to confirm or deny that your force is currently engaged, or not engaged in forensic testing for a CT purpose, is to disclose information which could act as a warning or indeed confirm to interested criminal parties whether or not criminal activity of such nature exists within that force area. Disclosure of information that undermines the operational integrity of law enforcement capabilities is highly likely to have an adverse impact on public safety and a negative effect on law enforcement generally. This risk to public safety cannot be said to be in the public interest.

As stated above, the public interest test is a consideration of whether the community benefit of possession of the information outweighs the potential harm. It is not an evaluation of what interests the public. We consider that the public interest test favours withholding the requested information.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

4. Please confirm how much has been spent on specialist hardware and software to facilitate digital forensic investigation activities in each calendar year. Please break this expenditure down by supplier / product.

Financial Year	Spend on Hardware and Software
2015	£50,318.74
2016	£35,927.79
2017	£35,980.63
2018	£33,265.62
2019	£62,693.23

Please note: The above figures relate to Financial year and include Software and Hardware Purchases as well as IT Licences and maitenance renewals.

Harm had been identified to information regarding a break down of expenditure by supplier / product, therefore an exemption is applied by virtue of section 31(1)(a)(b) Law Enforcement.

Rationale for s31 in Question 4

The tactics used by a police force are excluded from being disclosed as they assist the police in the prevention and detection of crime, apprehend or prosecute offenders, and to administer justice. Disclosure into the public domain would prejudice policing. For example, it has been well-publicised that Apple will not work with Law Enforcement Agencies to help unlock phones. However, if it became public knowledge that there is software that can allow the police to bypass or unencrypt passwords to allow access to phones, this could result in incriminating evidence potentially being wiped from phones, or the phones not being surrendered to the police as freely as they are presently, and as such this could prejudice policing. Use of such software for example, may enable access to the contents of a phone even when the owner of the phone deliberately provides the incorrect pin number.

Further, many of the companies that provide policing with the software and tools used to extract data have ensured that individual police forces have signed Non-Disclosure-Agreements. Disclosure of the information may breach the confidence and trust of suppliers and could result in the licence to use such tools being revoked. In addition, suppliers may be reluctant to develop future tools that would benefit law enforcement due to the risk of their capabilities, commercial interests, and trade secrets being made public knowledge. The development of enhanced tools and capabilities would greatly support reasonable lines of enquiry, fair investigations, privacy issues, and improve data management throughout the Criminal Justice System.

The withdrawal of the tools and the associated capabilities would cause numerous difficulties for policing. Such action would seriously hinder investigations, the safeguarding of victims and witnesses, the prevention and detection of crime, apprehension and prosecution of offenders, and the administration of justice.

A high proportion of investigations, such as rape and serious sexual assaults, heavily rely on the extraction of data from mobile phones. These offences involve some of the most vulnerable victims and children in society. As such, the withdrawal of tools by the suppliers could seriously and disproportionally affect some of the most serious and sensitive crimes investigated by the police. Investigators would not be in possession of evidence that could be crucial to meet evidential thresholds required by the CPS. Consequently, there is a risk that dangerous offenders would be not convicted and would remain at large in communities where there is real possibility that they would continue to offend unabated.

The public interest in maintaining the procedural sections of the FOIA exemptions outweighs the public interest in disclosure. This is because withholding the disclosure of policing tactics and the tools at the police's disposal will mean that those members of the public that are committing crimes and pose a risk to the public, will not be aware of these things and will not be able to formulate ways to circumvent the tactics and tools used. If disclosed the tactics will become less effective and will mean that the police are not able to detect and prevent crime, apprehend or prosecute offenders or to administer justice for the wider community.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 10/03/2020

HEDDLU GOGLEDD CYMRU
Gogledd Cymru diogelach

NORTH WALES POLICE
A safer North Wales

Response Date:**15/01/2019**

2019/045 - Forensic examination of digital devices

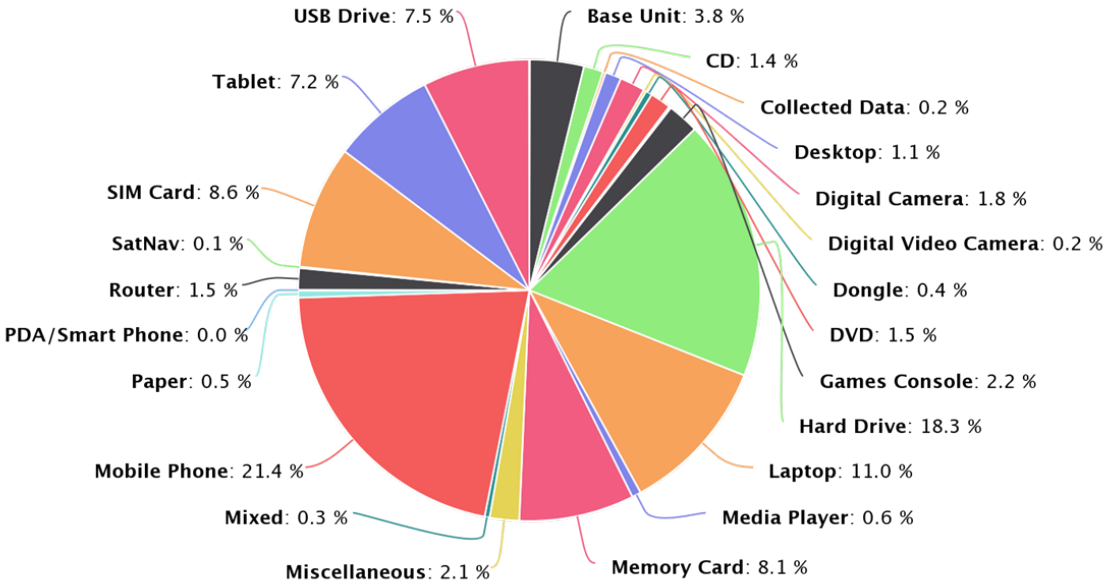
In response to your recent request for information regarding;

1) For each of the last four years (2015, 2016, 2017 and 2018) please could you tell me the total number of digital devices that were forensically examined by your police force?

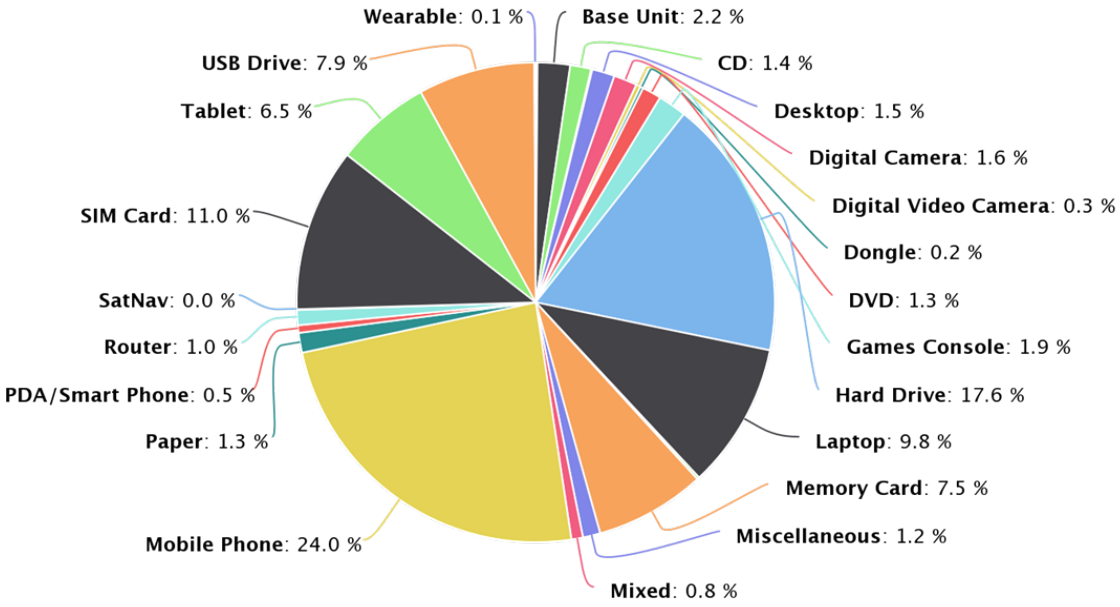
2) Please provide as much of the following information that you hold or are able to gather, for each of the four years:
A breakdown of examined devices by the 'type' of device. Eg 500 mobile phones, 200 iPads, etc.
A breakdown of who the examined devices belonged to – in particular, the number that belonged to (a) suspects, (b) complainants or (c) witnesses.
The average time that the examined devices were held for before being returned to their owners. If the data is available, please break this down for (a) suspects, (b) complainants and (c) witnesses.

The below relates to the number of exhibits submitted to the Digital Forensic Unit for examination, this doesn't guarantee that all exhibits had been examined.

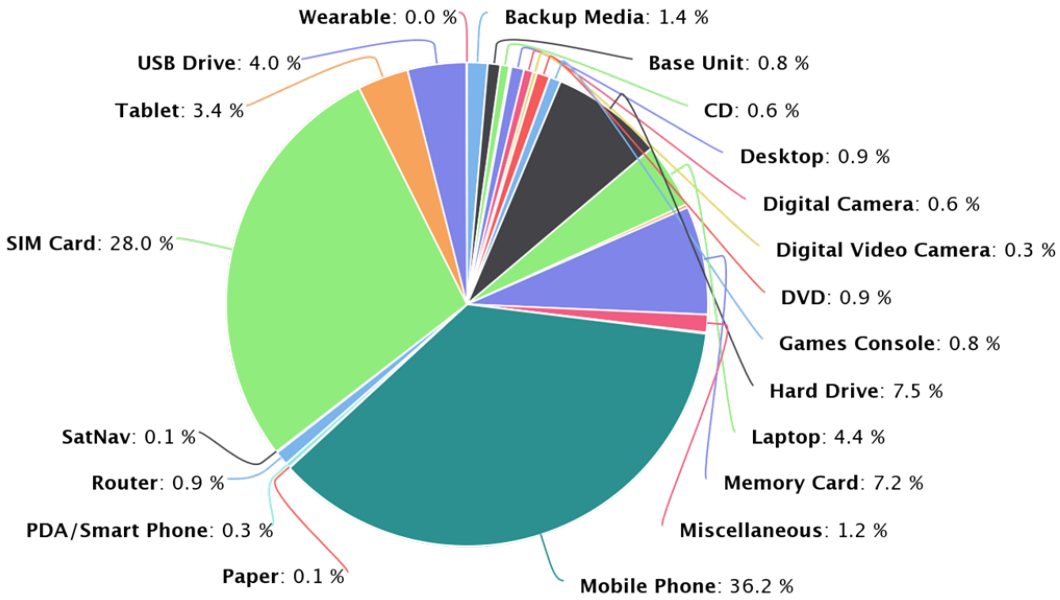
2016: 2047 Items



2017: 2545 Items



2018: 5583 Items



At present we do not record the exhibit against (a) suspects, (b) complainants or (c) witnesses.
2016 and 2017 we only dealt with High Tech Crime Unit exhibits so the combined including mobile phones numbers are not recorded here, 2018 includes the mobile phones combined.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 15/01/2019