Citation:
Dixon, MB and Schreuders, ZC and Soobhany, AR and Trevorrow, PA and Miller, S and Collins, L DigiVisor Mobile App: Frontline Officer Awareness Development and Decision Support. (Unpublished)

Link to Leeds Beckett Repository record:
https://eprints.leedsbeckett.ac.uk/id/eprint/5075/

Document Version:
Article (Accepted Version)

The aim of the Leeds Beckett Repository is to provide open access to our research, as required by funder policies and permitted by publishers and copyright law.

The Leeds Beckett repository holds a wide range of publications, each of which has been checked for copyright and the relevant embargo period has been applied by the Research Services team.

We operate on a standard take-down policy. If you are the author or publisher of an output and you would like it removed from the repository, please contact us and we will investigate on a case-by-case basis.

Each thesis in the repository has been cleared where necessary by the author for third party copyright. If you would like a thesis to be removed from the repository or believe there is an issue with copyright, please contact us on openaccess@leedsbeckett.ac.uk and we will investigate on a case-by-case basis.

CARI Project

DigiVisor Mobile App: Frontline Officer Awareness Development and Decision Support

Mark Dixon, Z. Cliffe Schreuders, A. Ryad Soobhany, Pip Trevorrow, Stephen Miller, and Lewis Collins

Leeds Beckett University and West Yorkshire Police

2018

This is a *pre-print*, in the process of undergoing academic publication.

The CARI Project

The CARI Project is a large-scale collaboration between West Yorkshire Police and the Cybercrime and Security Innovation Centre (CSI Centre) at Leeds Beckett University. The CARI Project aims to improve and incorporate an evidence-based approach into the policing of digital forensics and cybercrime investigations. An extensive needs assessment of UK policing and cybercrime and digital evidence was conducted to understand the current situation, and to identify needs across the force. The CARI Project also involved implementing a training and research programme that has impacted the capability of the digital forensics and cyber units within West Yorkshire Police to engage in research. This needs assessment and research training led to the development of a set of research proposals, which were scored and selected. Subsequently, academics and police staff co-produced 9 research and development workstreams: a framework for seizure, preservation and preservation of cloud evidence; automated forensic analysis; image linkage for victim identification and framework for image fingerprint management; automated grooming detection; frontline officer awareness development and decision support mobile app; assessment of methods of cyber training; an evaluation of the role of the Digital Media Investigator within WYP; and characteristics of victims of cybercrime. Each of these projects were designed to address needs within law enforcement and outputs include evidence-based procedures, new capabilities such as software/algorithms, and actionable intelligence.

This work was supported by a Police Knowledge Fund grant, administered by the Home Office, College of Policing, and the Higher Education Funding Council for England (HEFCE).

LEEDS BECKETT UNIVERSITY

WEST YORKSHIRE POLICE

Table of Contents

Executive Summary

There has been a significant rise in cybercrime for the past few years, which made cybercrime the leading type of crime in the United Kingdom (UK Government, 2015). Vast amounts of digital evidence are generated, and correct procedures need to be followed during the seizure stage. The motivation for this project emerged during the course of the needs assessment performed together with the Police force, as part of the CARI project (Schreuders et al, 2017). The study uncovered issues with the accuracy and level of confidence of frontline officers to perform seizure of digital devices from properties. A user-centred design approach was utilised in this project to develop an application which would aid frontline officers in the seizure of digital devices.

A review of the literature surrounding forensic guidelines, current policing policies, and handling of digital evidence was performed, which resulted in a collection of literature sources. The approach taken to carry out the data collection and requirements elicitation phase was based on a user-centred design approach. User-centred design, often referred to as human-centred design, dates back to the 1980's. It is a concept that arose with the intention of involving the end-users in the development process from the initial stages of the design of a product/concept intended for their use (Abras, Maloney-Krichmar and Preece, 2004). End users were identified as the police officers who act as frontline officers in warrant situations and these users have been involved in the design phases. The design of the tool has focused on the possibilities of what the app can achieve in collaboration with the knowledge of the police officers. Focus groups were conducted with police officers to establish software requirements for the Android app, to provide officers with an easily accessible source of reference, guidance and training related to cybercrime and digital evidence. The officers' requirements included ability to assess intelligence, identify potential devices used in crime, capabilities of those devices and how they could be seized and packaged to safeguard the potential evidence they contained. The knowledge-base was developed based on desktop research, and semi-structured interviews with experts in handling digital evidence.

The output resources for the project include a mobile based app that was designed and implemented for the Android mobile phone operating system. The final prototype design kept the application as simple to use as possible, given that officers often have to use the application while undertaking several different tasks and talking to either suspects or victims. To aid in this design decision, the application screen was divided into four distinct "tabs". When selected, each tab provides a view of a screen associated with a specific type of functionality. The four tabs shown on the startup screen are as follows:

- **Devices** – provides information about hardware devices for which information is available.
- **Internet** – provides information about software applications for which information is available.
- **Cases** – allows the officer to record various types of evidence related to a specific case under investigation.
- **Contact** – provides direct phone and Internet access to the DFU and other support agencies.

The app allows the user to collect case evidence such as videos, images, audio, and Wi-Fi signal captures. The latter is not normally retrieved.

The evaluation was performed on a sample of 20 officers to gather some initial data on the impact of using the app. The survey included the following items to be tested:

1. A SUS (System Usability Scale) survey was conducted to assess the usability of the app in the form of a questionnaire.
2. Each officer was provided with a survey which depicted 15 digital devices which they had to decide, using their knowledge only, if they would seize or not seize and how confident (on a scale of 1 to 5) they were with their decision. The officers were then provided with the app and some time to familiarise themselves with it. They then returned to the survey and, whilst using the app, they were provided with images of 15 further digital devices and the same questions. The before and after images were switched for half of the sample to remove the impact of the image alone on the end decision.

The SUS output was interpreted based on the advice published in Bangor et al., which suggest that products which are at least passable have scores above 70 (Bangor et al, 2008). The SUS score was classified as 'acceptable', with room for improvement. The improvement will mainly be around the layout of the app and the polishing of the content.

Statistical tests (paired-samples t-test) were performed to assess the accuracy of device seizure as well as the participants' confidence in decision making. The result showed a statistically significant mean increase for the accuracy of device seizure. There was a 10% improvement in correct seizure of devices, which will lead to a huge timesaving for forensic analysts. The result for the participants' confidence in seizing a device showed a mean increase too. The results are promising considering sample size and impact of image alone.

Introduction

There has been a significant rise in cybercrime for the past few years, which made cybercrime the leading type of crime in the United Kingdom (UK Government, 2015). Digital evidence is a valuable asset in any cyber-enabled or cyber-dependent crime. Law enforcement agencies must recover vast amounts of digital evidence and their associated digital devices when dealing with cybercrime. Therefore, the correct procedures must be followed during the collection, preservation and transportation of digital devices recovered from either the suspect or victim of a crime (National Institute of Justice, 2008). Most often, seizure of digital devices are performed by first responders attending a scene of crime or a property, and these first responders are usually frontline police officers. In cases involving specific crimes, for example CSE (Child Sexual Exploitation) cases, frontline officers are accompanied by officers from the high tech department. The officers have to identify and seize any electronic device that can contain digital evidence and will be relevant to the case.

The motivation for this project emerged during the course of the needs assessment performed together with the Police force, as part of the CARI project (Schreuders et al, 2017). The study uncovered issues with seizure of digital devices by attending frontline officers from properties, for example recovery of incorrect type of digital devices or seizure of a disproportionate amount of digital devices. The main issue raised was the lack of knowledge that frontline officers had about types of digital devices, where some officers are not aware about remote wiping of data from handheld devices. The objective of this research project was to develop the awareness of frontline officers and help their decision making for seizure of digital devices. A user-centred design approach was adopted to design and implement a mobile application installed on standard handheld device issued to frontline officers. The design approach allows the participation of users in the requirements elicitation phase and design phase of the app, by conducting focus groups and interviews. A prototype app was designed and implemented based on the findings of the focus groups. Finally, the usability of the app was evaluated using questionnaires designed based on the System Usability Scale (SUS).

Literature Review

A review of the literature surrounding forensic guidelines and current policing policies and handling of evidence was performed, which resulted in a collection of literature sources. One commercial application was surveyed, the Blue Lights Discovery (Blue Lights Discovery, 2017) application, which is a library of interactive training courses available on smartphones. Users of Blue Lights Discovery need to create a profile in the app and the user is offered a selection of introductory training courses for free and the rest of the more in-depth courses are payable. The main principles of management of police information (MOPI) provide a balance of proportionality and necessity that are at the heart of effective police information management. The principles also highlight the issues that need to be considered in order to comply with the law and manage the risks associated with police information, which include:

- Collection
- Information sharing
- Retention, review and disposal

The seizure of digital devices will include interaction with the devices and personal information of suspects or victims at a scene of crime or property, therefore the legislation encompassing the management of digital evidence and information was reviewed. RIPA (Regulation of Investigatory Powers Act) was brought in to regulate the investigatory powers of law enforcement and government agencies in relation to interception, acquisition and disclosure of data relating to communications

among other types of surveillance (RIPA, 2000). RIPA provides a framework to ensure investigatory techniques are used in accordance to the Human Rights Act and the European Convention on Human Rights (ECHR). Seizure of devices from properties has to adhere to the Authorisation of Action in Respect of Property section of the Police Act (Police Act, 1997) and the Computer Misuse Act (Computer Misuse Act, 1990). The seizure of devices also falls under the Acquisition and Disclosure of Communications Data (Home Office, 2015a) and the Retention of Communication Data (Home Office, 2015b) code of practice, which are part of RIPA.

The police forces in the UK, more specifically West Yorkshire Police (WYP), have to adhere to the ACPO (Association of Chief Police Officers) good practice guide which was written to ensure the guidance of UK law enforcement personnel that may deal with digital evidence (ACPO, 2012). ACPO was founded in 1948 and dissolved in 2015 when it was replaced by the National Police Chiefs' Council (NPCC). Although ACPO has been dissolved, the good practice guide is used in UK and other countries and considered the best practice guide for computer forensics (7Safe, 2015). The DFU (Digital Forensic Unit) and the CCT (CyberCrime Team), within WYP have their own policies for seizure of digital devices and for pursuing online investigations which are based on the ACPO good practice guide. The police staff and officers of these departments have to follow the College of Policing Core Skills in Mobile Phones Forensics course before working with mobile devices.

Methodology

The approach taken to carry out the data collection phase was based on a user-centred design approach. User-centred design, often referred to as human-centred design, dates back to the 1980's. It is a concept that arose with the intention of involving the end-users in the development process from the initial stages of the design of a product/concept intended for their use (Abras, Maloney-Krichmar and Preece, 2004). The way in which they are involved can differ dependent on the specific approach adopted, but the key element remains that the users are involved in some way. For example, some design projects may gather initial 'needs' requirements from the end-users, design a blueprint based on these needs and evaluate this with the users in order to verify before progressing to the implementation phase. Other design projects may involve end-users on a deeper scale and treat them as partners throughout the whole product development cycle. The commonality of all approaches is that the design has emulated from the consideration of the end users and their needs for the process under consideration (Goodman-Deane, Langdon and Clarkson, 2010). Whichever process is followed, by putting the user at the centre of the process the end result will be a product that will be fit for purpose for those intended to use it (Wever, van Kuijk and Boks, 2008); ultimately a proof of concept. In addition, the users will feel more empowered by the process, and have a by-in to use the end product, rather than feeling as if a product has been imposed upon them (Maguire, 2001).

According to Eason (1987) users can be categorised into three types: primary users are those who will use the product, secondary users are those who may occasionally use the product, and tertiary users are those who may be affected by the use of the product. In order for the product to demonstrate full success, all users must be considered, not necessarily all included, in the design process.

This research project included design input from both primary and secondary users; as it is difficult to ascertain which officers may be faced with a warrant including seizure of electronic equipment; it was felt that a wide selection of officers would meet those classed as primary and secondary users.

The main principles of user/human-centred design, according to Maguire (2001) are:

- Active involvement of end users
- Appropriate allocation of defined needs to those best operated by humans and those for the product
- Iterative design phases
- Involvement of a multi-disciplinary design team

Each of these has been addressed within the development life cycle of this research project. End users have been identified as the police officers who act as frontline officers in warrant situations and these users have been involved in the design phases. The design of the tool has focused on the possibilities of what the app can achieve in collaboration with the knowledge of the police officers. The iterations were few in number due to the time constraint but officers were involved as much as was possible. The team who designed the final app included a programmer and an experienced officer from the Digital Forensics Unit.

The inclusion of users in the design process is often through the use of interviews or focus groups (Goodman-Deane, Langdon and Clarkson, 2010). Due to constraints such as time and access to users, the focus group approach was adopted for the initial stages of the project, with an end experiment survey to help evaluate the effectiveness of the app produced. A System Usability Scale (SUS) was designed to measure the usability of the app in terms of three broad areas: effectiveness, efficiency and satisfaction (Brooke, 1996). The SUS consists of a questionnaire of ten questions with five response options on a Likert scale and is used to assess the usability of software, websites and applications.

Results

The findings from the focus groups identified potential gaps in knowledge of frontline officers in identifying:

- Sources of digital evidence on digital devices for seizure
- Correct methodology for safeguarding, packaging and continuity of devices seized from a scene of crime or property
- Awareness of digital evidence that can be remotely wiped on devices
- Perform an effective preliminary triage at the scene for digital devices

A review of exhibits recorded on the Case Management System from DFU identified several issues that were added to the list of requirements for the app:

- Digital evidence not correctly identified
- The packaging and transportation of the digital evidence was also identified as source of issue.
- Memory Card Adapters being seized with no memory card present (no storage)
- Bluetooth dongles being submitted by officer in the case believing them to be a flash drive

The output of the results include a prototype application, which was designed and implemented based on the findings from the focus groups held as part of the user centred design approach. Integral to the user centred design approach is an evaluation phase where feedback can be provided on the product developed in terms of usability and content. This was included in the project lifecycle

via a questionnaire. The evaluation of the usability of the prototype was performed with a group of 20 officers.

The prototype application was developed for the Android mobile phone operating system. This was chosen based on the focus groups that identified that frontline officers are currently provided with Samsung Note 5 devices, which are based on the Android platform. The prototype was developed using standard industry toolsets, such as Android Developer studio. Since the target operating system was Android the product was developed using the Java programming language, along with XML for configuration purposes.

An initial specification of the required product was developed between the research support staff and the primary developer. The specification was produced by analysing outputs generated from focus groups conducted with officers as part of the user-centred design. A number of initial screen designs were also used to identify key functionalities.

The final prototype design kept the application as simple to use as possible, given that officers often have to use the application while undertaking several different tasks and talking to either suspects or victims. To aid in this design decision, the application screen was divided into four distinct “tabs”. When selected, each tab provides a view of a screen associated with a specific type of functionality. The start-up screen shown to the user when the application is first activated is shown in Figure 1. From this screenshot the four selection tabs can be seen at the top of the screen.

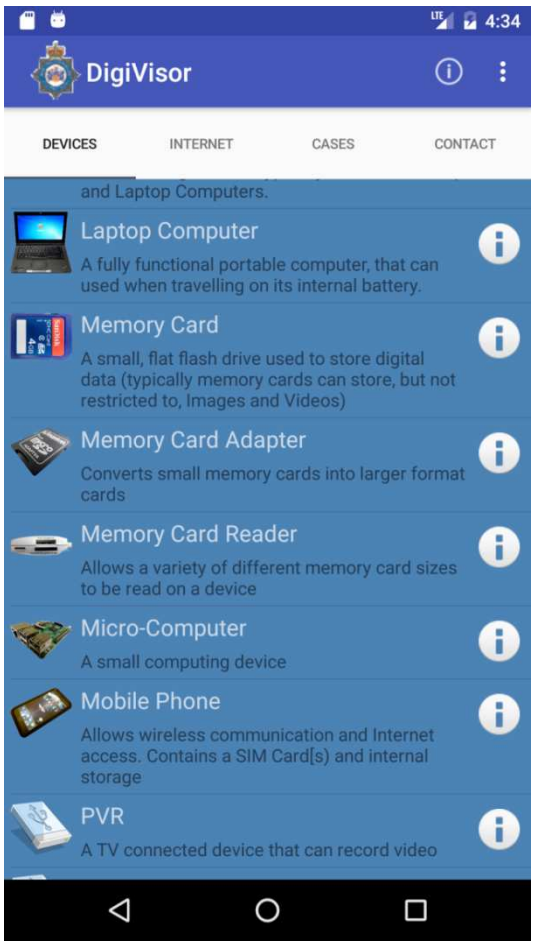

Figure 1 – App start-up screen (showing 4 selection tabs)

The four tabs shown on the start-up screen are as follows:

- **Devices** – provides information about hardware devices for which information is available.
- **Internet** – provides information about software applications for which information is available.
- **Cases** – allows the officer to record various types of evidence related to a specific case under investigation.
- **Contact** – provides direct phone and Internet access to the DFU and other support agencies.

An in-depth description of the app is provided in Appendix A, where all the functionalities of the four tabs are investigated with screenshots. The app displays detailed information categories for each device, which contain:

- TODO list
- generic how to
- Pictures of the device
- Frequently asked questions about the devices
- Video guides with a total of nine bespoke guidance videos
- Security issues
- Additional help

The app allows an investigating officer to create cases to record information and various types of evidence from a scene. The cases are stored locally on the device and can be exported; by saving in a compressed file or emailed to DFU. The user can view existing or add new evidence to a case (the officer's device geolocation is stored with the evidence), such as:

- Enter information about a seized device
- Capture photographic and video evidence of the scene
- Record audio evidence using the phone
- Detect WiFi (wireless) and Bluetooth networks details in the vicinity of the officer's device. The MAC address of each device is used to display the manufacturer of the device to the user

The app also allows the frontline officer to get access contacts for various support groups for victims of crime as well as the Digital Forensics Unit (DFU) in case further information is needed about the seizure of a device. All the resources (pictures, videos) used by the app are stored locally in the file structure and can be altered from outside the app.

The evaluation was performed to gather some initial data on the impact of using the app. A convenient sample size of 20 officers has been selected to evaluate the app. The survey included the following items to be tested:

1. A SUS (System Usability Scale) survey was conducted to assess the usability of the app in the form of a questionnaire.
2. Each officer was provided with a survey which depicted 15 digital devices which they had to decide, using their knowledge only, if they would seize or not seize and how confident (on a scale of 1 to 5) they were with their decision. The officers were then provided with the app and some time to familiarise themselves with it. They then returned to the survey and, whilst using the app, they were provided with images of 15 further digital devices and the same questions. The before and after images were switched for half of the sample to remove the impact of the image alone on the end decision. The accuracy of device seizure as well as the participants' confidence in decision making will be assessed respectively.

The responses of the 20 respondents for the questionnaire were collated and Figure 2 shows the sorted (from Highest to lowest) mode of the scores in each of the 10 questions, with a 5 point Likert scale, in assessing the usability of the app. The 10 questions are also listed in Figure 2.

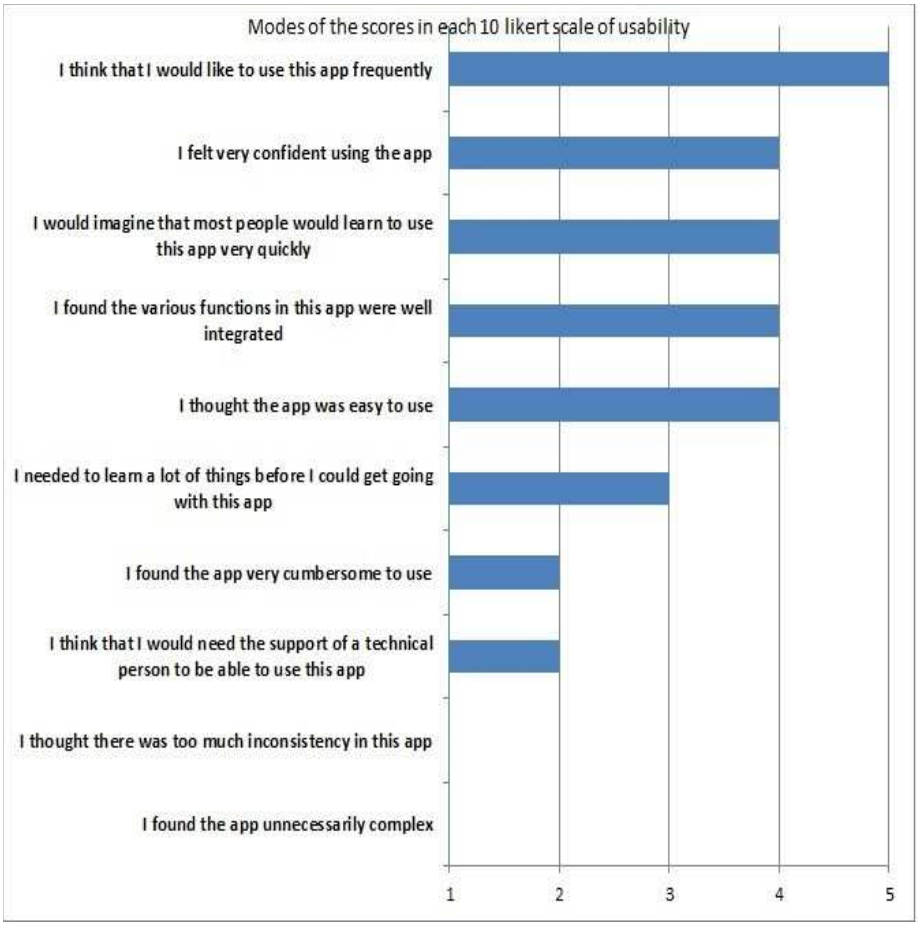

Figure 2 Mode of the score in each of the 10 questions for the usability assessment of the app

The System Usability Scale (SUS), a cost effective and reliable tool to assess the usability of a product ranges from 0 (negative) to 100 (positive) (Bangor et al., 2009). SUS is composed of ten statements (five negative and five positive alternatively), each having a five-point Likert scale from Strongly Disagree to Strongly Agree. The SUS scores for all 20 participants, shown in Figure 3, have been calculated by first summing the score contributions from each item.

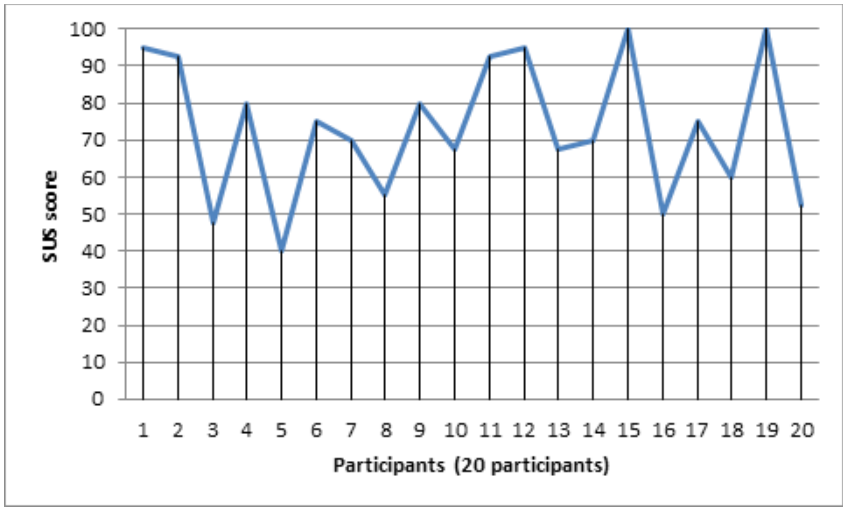

Figure 3: The overall SUS score

Response to the continued use of the app was very positive as demonstrated in Figure 4, which provides some confidence in how the app was received by those who used it in the experiment.

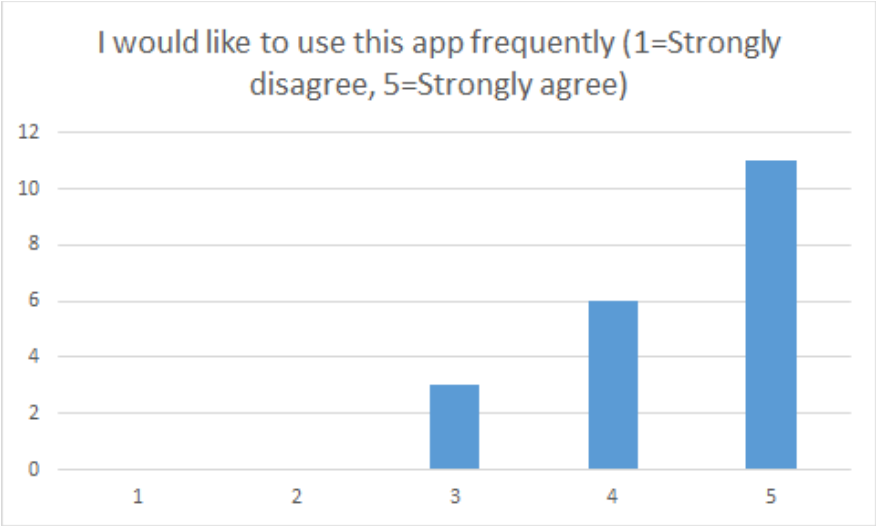

Figure 4: Response to continued use of the app

Such results were replicated in response to the app being easy to use, with the majority (16/20) agreeing or strongly agreeing. Responses to questions such as 'was the app cumbersome to use', 'do you believe most people would learn to use the app quickly' also received very positive and encouraging responses with the majority disagreeing (13/20) with the former statement and agreeing (14/20) with the latter statement.

For assessing the accuracy of device seizure before and after using the app, the results showed that the correct seizure of the digital device increased slightly between the first survey (59.33% correct) and the second where they were able to use the app (67.33% correct). A paired-samples t-test was used to show that there is a mean difference between total score for each participant before using the app and after using or familiarizing themselves with the app to decide whether they would seize or not seize the 15 digital devices, and also how confident (on a scale of 1 to 5) with their decision between using the app and after using it.

By comparing the average confidence scores for each participant before and after seeing the additional 15 images, further t-test reveals that there is a mean increase in the participants' confidence in decision making. The results are promising considering sample size and impact of image alone.

References

7Safe (2015) ACPO Guidelines | Publications | 7Safe, n.d. URL https://www.7safe.com/about-7Safe/downloads/acpo-guidelines (accessed 2 June 2017)

Abras, C., Maloney-Krichmar, D., and Preece, J. (2004) User-Centred Design. In Bainbridge, W. **Encyclopaedia of Human-Computer Interaction**, Thousand Oaks: Sage Publications.

ACPO (2012) ACPO Good Practice Guide for Digital Evidence, **Association of Chief Police Officers**

Bangor, A., Kortum, P.T., & Miller, J. T. (2009). Determining what individual SUS scores mean: Adding an adjective rating scale. **Journal of Usability Studies**, 4, 114-123.

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An Empirical Evaluation of the System Usability Scale. **International Journal of Human–Computer Interaction**, *24*(6), 574–594. https://doi.org/10.1080/10447310802205776

Blue Lights Discovery (2017) [Online], Available from <http://bluelightsdiscovery.com> [Accessed 12 June 2017].

Brooke, J. (1996) SUS: A "quick and dirty" usability scale. **Jordan, P. W., Thomas, B., Weerdmeester, B. A., McClelland (eds.) Usability Evaluation in Industry** pp. 189--194. Taylor & Francis, London, UK

Computer Misuse Act (1990) Computer Misuse Act [Online], Available from <http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf> [Accessed 12 June 2017].

Eason, K. (1987) Information technology and organizational change. London: Taylor and Francis.

Field, A. (2013) Discovering Statistics with IBM SPSS statistics. **4th ed. London: SAGE**

Goodman-Deane, J., Langdon, P., and Clarkson, J. (2010) Key influences on the user centred design process, **Journal of Engineering Design**, 21: 2-3, pp.345-373

Home Office (2015a) Acquisition and Disclosure of Communications Data, **TSO (The Stationery Office), part of Williams Lea on behalf of the Home Office**

Home Office (2015b) Retention of Communication Data,**TSO (The Stationery Office), part of Williams Lea on behalf of the Home Office**

Maguire, M. (2001) Methods to support human-centred design, **International Journal Human-Computer Studies**, 55, pp.587-634

National Institute of Justice (2008) Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Electronic Devices: Types, Description,and Potential Evidence. Electronic Crime Scene Investigation: A Guide for First Responders, **National Institute of Justice**, Second Edition, pp. 1–12.

RIPA (2000) UK Regulation of Investigatory Powers Act [Online], Avaialble from: <http://www.legislation.gov.uk/ukpga/2000/23/introduction> [Accessed 12 June 2017].

Police Act (1997) Police Act 1997 [Online], Available from: <http://www.legislation.gov.uk/ukpga/1997/50/pdfs/ukpga_19970050_en.pdf> [Accessed 12 June 2017].

Schreuders, Z.C., Cockcroft, T., Butterfield, E., Elliott, J., Soobhany, A.R., and Shan-A-Khuda, M. (2017) Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force, **The Cybercrime and Security Innovation (CSI) Centre**, Leeds Beckett University.

UK Government (2015) National Security Strategy and Strategic Defence and Security Review. UK Government [Online]. Available from: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf> [Accessed 12 June 2017].

Wever, R., van Kuijk, J., and Boks, C. (2008) User-centred design for sustainable behaviour, **International Journal of Sustainable Engineering**, 1(1), pp.9–20.

Appendix A

Prototype Application Overview

A prototype application was developed for the Android mobile phone operating system. This was chosen based on earlier research that identified that police officers are currently provided with Samsung Note 5 devices, which are based on the Android platform. The prototype was developed using standard industry toolsets, such as Android Developer studio. Since the target operating system was Android the product was developed using the Java programming language, along with XML for configuration purposes.

An initial specification of the required product was developed between the research support staff and the primary developer. The specification was produced by analysing outputs generated from focus groups conducted with officers as part of the user-centred design. A number of initial screen designs were also used to identify key functionalities.

The final prototype design kept the application as simple to use as possible, given that officers often have to use the application while undertaking several different tasks and talking to either suspects or victims. To aid in this design decision, the application screen was divided into four distinct “tabs”. When selected, each tab provides a view of a screen associated with a specific type of functionality.

The four tabs shown on the startup screen are as follows:

- **Device** – provides information about hardware devices for which information is available.
- **Internet** – provides information about software applications for which information is available.
- **Cases** – allows the officer to record various types of evidence related to a specific case under investigation.
- **Contact** – provides direct phone and Internet access to the DFU and other support agencies.

The startup screen shown to the user when the application is first activated is shown in Figure 1. From this screenshot the four selection tabs can be seen at the top of the screen.

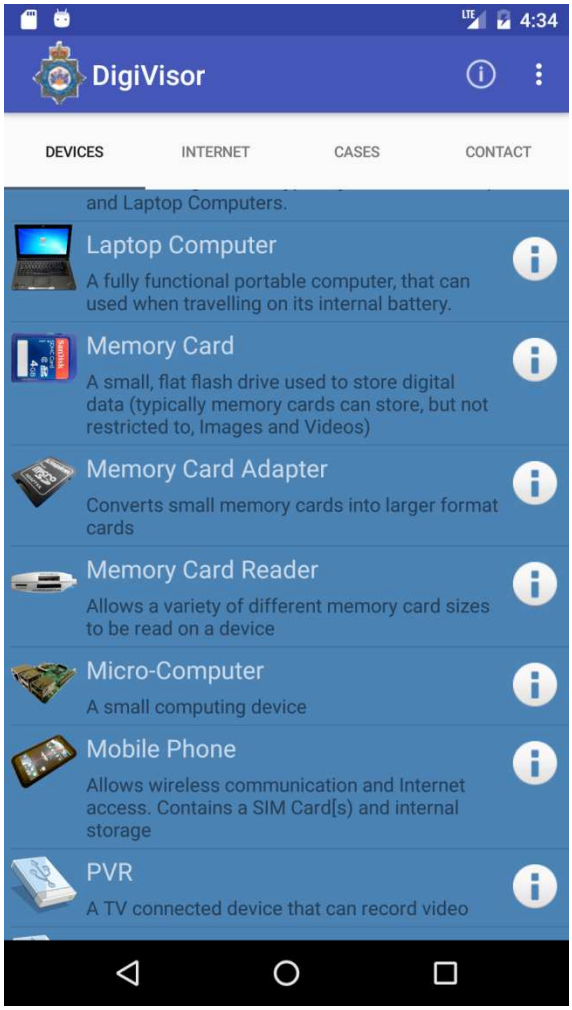

Figure 1 – startup screen (showing 4 selection tabs)

The "Devices" Screen

This screen lists the devices for which information is available within the application. This is the default "tab" that is opened when the application is started, as shown in Figure 1. Each row of the list contains a name, short description and an image of the device. Selecting the image causes a list of other images of the same device to be displayed at different angles. Selecting the "i" Information button provides a longer description of the device within a pop-up window. Selecting the central part of the row itself displays a new screen allowing the categories of available device information to be selected by the user, as shown in Figure 2.

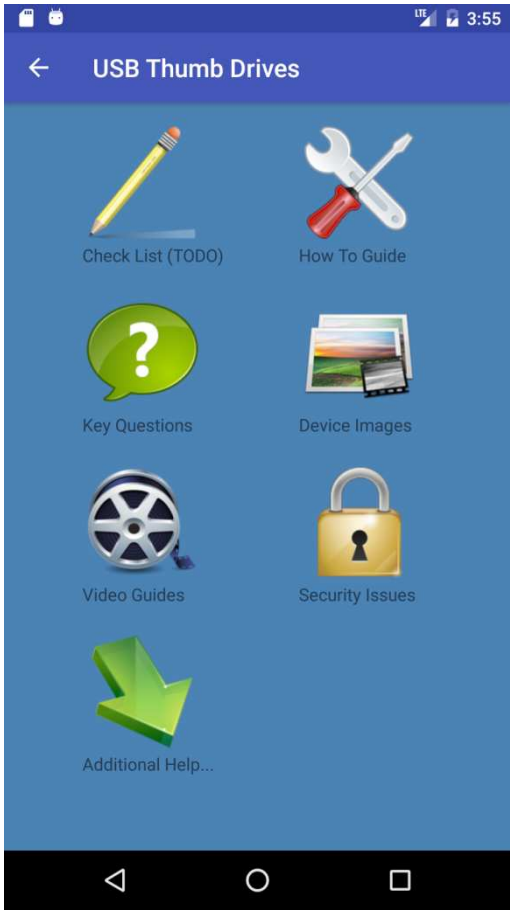

Figure 2 – device information categories

Selecting a category results in the display of another sub-screen that allows an officer to drill down to a specific type of advice that is available for the currently selected device. An example of the type of information displayed is shown in Figure 3. These show the device images, video guides, and a generic examination "how to guide".

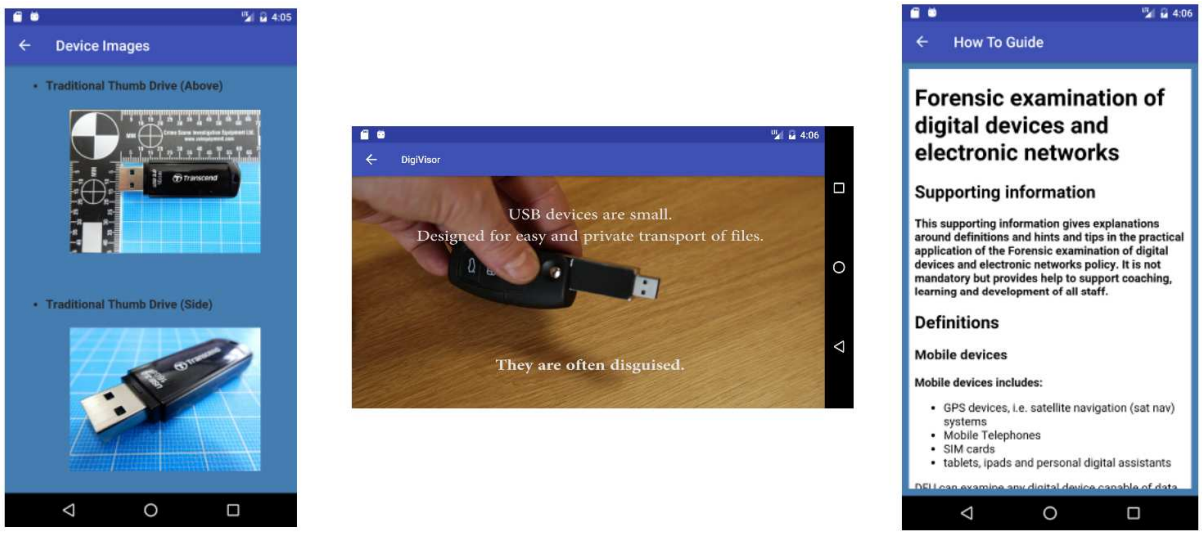

Figure 3 – example category content

The "Internet" Screen

This screen lists the various types of software application for which information is available within the application. This screen behaves in a way consistent with the "Devices" screen, given that it exists for exactly the same purpose. i.e. to provide information about an artifact that may be discovered during an investigation.

The "Cases" Screen

The purpose of this screen is to provide a mechanism for an investigating officer to record information and various types of evidence from a scene. When first activated this screen provides a chronologically ordered list of all cases recorded on this device. Selecting a case causes a new screen to be shown, detailing the information about the case along with an area for adding specific types of evidence, as shown in figure 4.

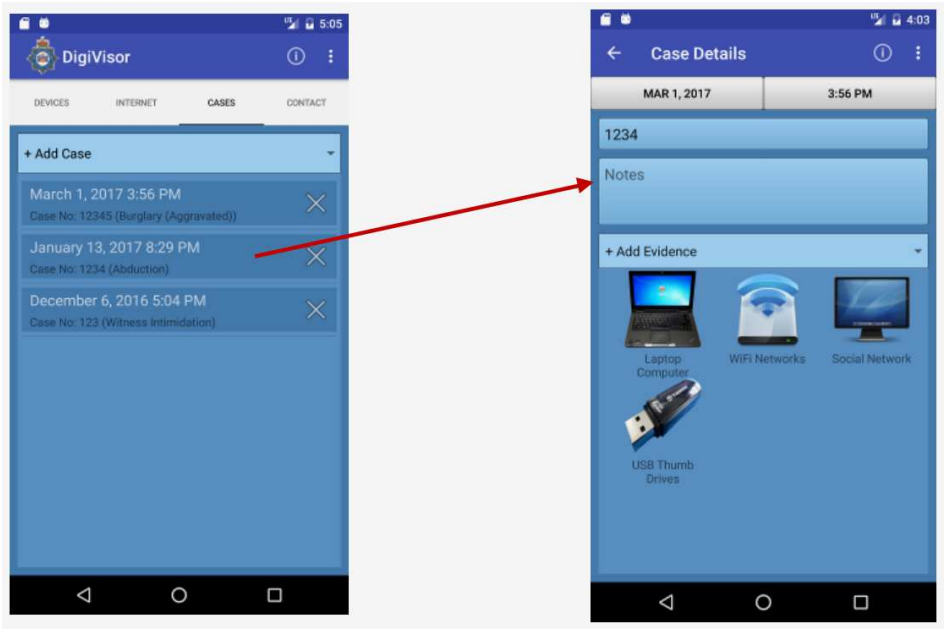

Figure 4 – Cases screen and case detail screen.

The type of evidence that can be recorded and associated with a specific case is as follows -

- **Found Device** – this allows an officer to record information about a found hardware device. Information such as the device type, location found and additional notes can be input by the user.

- **Software Application** – this allows an officer to record information about a software application that may be active while the investigation is underway. Information such as available usernames and passwords may be stored.

- **Photographic Evidence** – this allows the officer to take a photograph using the phone. The photograph is tagged as evidence and shown within the associated case detail screen as a thumbnail.

- **Audio Evidence** – this allows the officer to take an audio recording using the phone. The audio recording is shown with the other evidence and may be played back when required.

- **Video Evidence** – this allows the officer to take a video recording using the phone. The video is tagged as evidence and shown within the associated case detail screen as a thumbnail.

- **WiFi networks** – this automatically detects any WiFi networks within the vicinity of the investigation and displays information about the networks, including signal strength and encryption mechanisms supported. The MAC address of each device is used to identify the manufacturer of the device which is displayed to the user.

- **Bluetooth networks** - this automatically detects any Bluetooth networks within the vicinity of the investigation and displays information about the networks, including signal strength.

When evidence is stored the location at which the evidence was captured is automatically stored in the form of longitude, latitude and level of accuracy (in metres).

The "Contact" Screen
This screen provides quick and direct access to various support groups as well as the Digital Forensics Unit (DFU). A list is provided along with a short summary of the support or services provided. This section of the application was provided not only to provide direct victim support, but also to provide additional support to the officer conducting an investigation. A user may either select the provided web address to view the associated web-site, or select the phone icon to make a direct call to the service. A screenshot of a section of the contact list is shown in Figure 5.

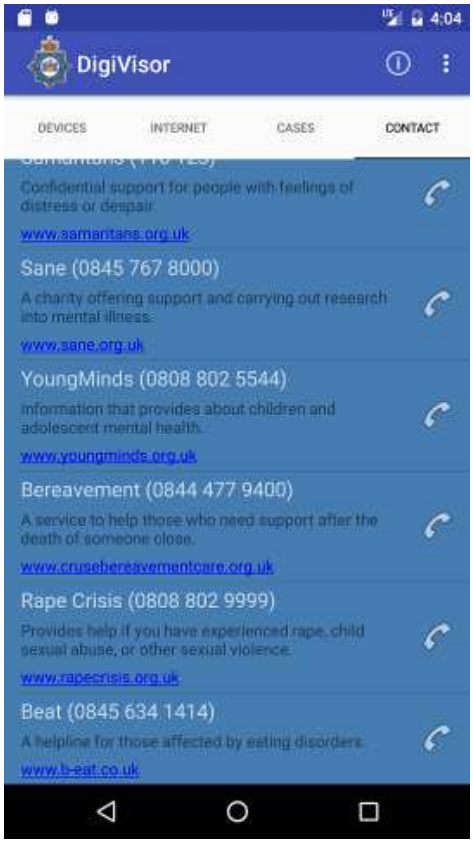

Figure 5 – Contact support list

Exporting of Case data
Since the information regarding specific investigations is stored on the device itself, a facility is provided that allows case information to be exported. This allows all information related to a specific case, including collected evidence, to be collated into a compressed file and optionally emailed to the digital forensics unit. As part of this data, a summary of the case information is produced in a csv

formatted file that can be viewed in standard applications such as MS Excel. A screenshot of the export case details screen is shown in Figure 6.

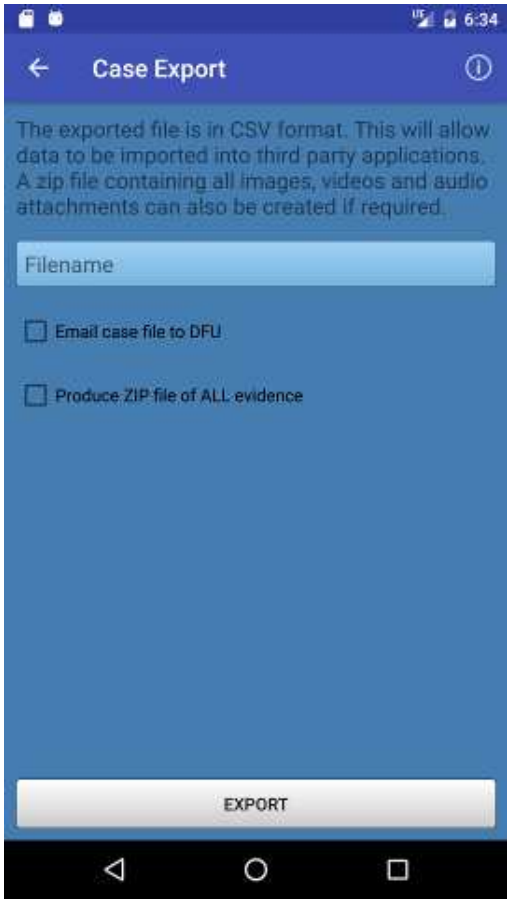

Figure 6 –Case details export screen

Configuration of Application Content

The application was designed and developed in such a way as to allow the content to be easily updated. The information presented to the end user about hardware devices and software applications is actually stored outside of the application code itself, within a regular directory on the target device. When the application is started by the end-user it makes a scan of the information directory, automatically extracts any content, and then presents this to the user within the appropriate section of the application.

In order for this approach to work a standard set of files and naming conventions was agreed upon within the research team. All hardware devices and software applications to be presented to the user must follow this simple standard format.

The name of each directory provided maps to a single device or software application shown within the application. Within each directory a single “details.txt” file contains a short and long description of the device or software application, as presented to the user. There are then a number of Hyper-Text Markup Language (HTML) files containing information displayed to the user via the information screen, along with images of the device from various angles. As an example, the directory structure used to populate the “USB Thumb Drive” device is shown in Figure 7.

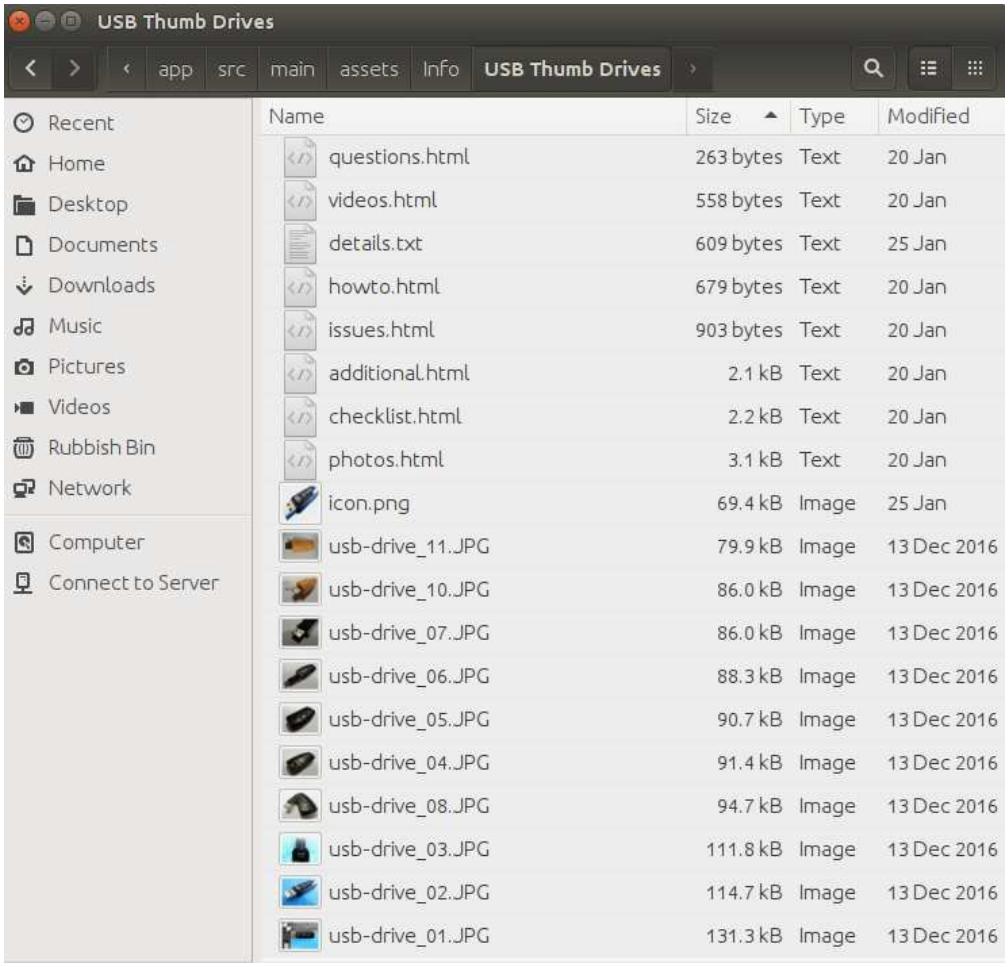

Figure 7 – USB Thumb Drive content configuration directory

Technical Detail

The prototype was developed as a standard Android application using the Java programming language. The source code consisted of 43 Java classes along with 35 xml configuration files. With the source code files totalling approximately 8,000 lines of code. The compiled distribution package for the application is ~1GB in size. The large size is mainly due to incorporated videos.

Future Features

The developed application, although complete in almost all respects, is still in the prototype phase. There are certain improvements that would need to be made in order to produce an application ready to be used by front-line officers. The key improvements identified are described below.

- Automatic updating of content – the area of computing forensics is fast moving, as is the development of new hardware and software technology. Hence the application would ideally need a facility where its content is automatically updated periodically without the need to re-install the core distribution package.

- Separation of video data from distribution package – the video files are very large compared to other content. Therefore the application should be improved so that video files are only downloaded when first accessed, and stored independently of the main application. This will mean the initial application will be very quick and easy to install.

- Encrypted exported data – the exported data should ideally be encrypted before use in the field. This is due to the fact that email is generally insecure and therefore transfer of sensitive data should always be encrypted prior to transmission.

- Better cross version compatibility – the existing prototype was developed for the current devices used by the police force. It is inevitable that in the future the devices used will change and be updated. Hence the application code should be better developed and tested to perform correctly across all platforms as they become available.