CJTEC

VERIFICATION REPORT

Targeted Data Extraction System (TDES) for Mobile Devices

CJTEC Verification Report **July 2022**

PURPOSE

Perform a verification review of a software tool developed by Florida State University (FSU) for a National Institute of Justice (NIJ) R&D proposal (award 2016-MU-CX-K003) and review its corresponding final report entitled A Targeted Data Extraction System (TDES) for Mobile Devices (Principal Investigator: S. Aggarwal).

The reference patent and technical publication for the Targeted Data Extraction System (TDES) are as follows:

- Aggarwal, S. et al. (2020). Targeted Data Extraction System and method (U.S. Patent No. US20200218546A1). U.S. Patent and Trademark Office. Retrieved from https://patents.google.com/patent/US20200218546A1/en
- Aggarwal, S., Dorai, G., Karabiyik, U., Mukherjee, T., Guerra, N., Hernandez, M., Parsons, J., Rathi, K., Chi, H., Aderibigbe, T., & Wilson, R. (2019). A Targeted Data Extraction System for mobile devices. In G. Peterson & S. Shenoi (Eds.), Advances in digital forensics XV (Vol. 569, pp. 73-100). Digital Forensics 2019. IFIP Advances in Information and Communication Technology. Springer, Cham. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-28752-8_5

CJTEC

INTRODUCTION

Technical Expectations of TDES

The objective of the experimental plan was to verify the claims of Aggarwal et al. (2019) regarding the prototype software for the targeted extraction of data from mobile phones. Specifically, the tool is designed to extract data that were generated and stored on a mobile phone during defined time intervals to the exclusion of information that was not generated and stored during those incident-related intervals. A performance requirement is that the TDES offers at least comparable performance to existing digital forensic software tools available for examining and analyzing mobile devices.

Choosing defined time intervals to extract data from a mobile phone reflects the law enforcement environment and the need to afford privacy to individuals who encounter the criminal justice system, whether they are a victim or witness. The ability for investigators to analyze digital evidence that is present on mobile devices is usually subject to the terms of the applicable warrant, which defines a time interval that is relevant to the incident(s) under investigation. Further, noting that most people have considerable private information on their devices, in order to protect the privacy and gain the cooperation and consent of victims and witnesses, investigators must be able to assure the owners that their information is protected and only information related to the time during which an incident occurred will be examined.

CJTEC

Methodology

The TDES verification testing plan was executed using a phase-gate approach, which enables the periodic assessment of project progress and allows for the effort to be monitored at specific milestones to ensure project success and facilitate a positive return on investment for NIJ.

For file-level software tools used in digital forensic analysis, such as the TDES tool, at a minimum verifying that the tools can read and interpret a file system is important. The ability to read a file system is assessed by the following parameters:

- The tool correctly reads a data stream as demonstrated by the calculation of a cryptographic hash for a file.
- The tool correctly reads the file path for the files of interest.
- The tool correctly interprets and displays the metadata of a file, as demonstrated by examination of the file modified/accessed/created times and dates.

If a software tool demonstrates the ability to meet these requirements, it is verified for that particular file system. The two most common file systems used in mobile devices available in the U.S. consumer market—iOS (Apple) and Android (Samsung)—were chosen for testing. In addition, both phones were connected to a U.S. carrier (Verizon):

Apple

Subscriber number: +1 202 993 0570

Device model: Apple iPhone X

Model number: MQCP2LL/A

Device ID: FK2WE0ZJCL7

International Mobile Equipment Identity (IMEI):

35 305309 891524 4

Operating system: iOS 15.2

Plan: Datascape Prepaid Refill

Apple ID: 4thStreetGlobal.test1@gmail.com

Passcode: 147258

Face ID: Activated

Samsung

Subscriber number: +1 202 993 0775

Device model: Samsung Galaxy A42 5G 128 GB

Device ID: 89148000007496241866

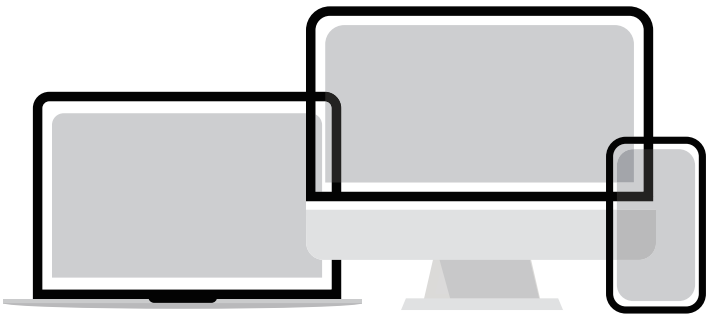
IMEI: 3507605508742

Operating system: Android 11

Plan: 5G Start with unlimited data (no hotspot available)

Phone ID: 4thStreetGlobal.test2@gmail.com

Passcode: Not employed



CJTEC

Generating Data

Loading Apps

On commencement, apps were accessed and loaded from the two usual sources for iPhone and Android operating systems (see **Table 1**):

- Apple iPhone—Apple ID (see above) used to download the subject apps from the Apple App Store to the device
- Samsung—Apps downloaded from Google Play

Table 1–Apps loaded to each of the mobile devices and their status

App Type	App Name	iPhone		Samsung	
		Loaded	Activated	Loaded	Activated
Browser	Chrome	ü	na	üü	na
	Firefox	ü	na	ü	na
	Edge	ü	na	ü	na
	Safari	ü	na	ü	na
Social Networking	Facebook	üü	ü	ü	ü
	LinkedIn	ü	ü	ü	ü
	Twitter	ü	ü	ü	ü
Communications	Apple Mail	üü	na	û	û
	Gmail App	ü	na	üü	na
	WhatsApp	ü	ü	ü	ü
	Messenger	ü	ü	ü	ü
	Skype	ü	û	û	û
	Zoom	ü	û	û	û
	Instagram	ü	ü	ü	ü
	WeChat*	ü	û	û	û
	Viber	ü	ü	ü	ü
	Line	ü	ü	ü	ü
	Telegram	ü	ü	ü	ü
	Signal	ü	ü	ü	ü
	YouTube	ü	ü	üü	ü
	TikTok	ü	ü	ü	ü
	Snap**	ü	û	û	û

ü = loaded but not activated or not loaded
üü = preinstalled
na = not applicable because activation is not required
* WeChat was not activated because of limitations on the "existing user referral"–dependent identity validation procedure.
** Snap (Snapchat) was loaded to the devices but not activated because of time constraints.

- Two email accounts were created, corresponding to the Apple/Android IDs:
  - 4thStreetGlobal.test1@gmail.com with a password ujPjRSrk3H35ksQ
  - 4thStreetGlobal.test2@gmail.com with a password Ph7Th9bppgzxYzj

The email accounts were used, among other purposes, to send and receive emails between the phones and to other third-party email accounts.

Loading Data onto the Devices

Over the period from the afternoon of December 3, 2021, to the morning of December 8, 2021, the following data were seeded to all of the apps:

- **Messages sent between the devices on the above communications apps, primarily between the two test devices, but also from third-party devices, including:**
  - Simple text messages were sent and received.
  - Messages with images, including photos, stickers, gifs, and links, were sent and received.
  - All messages were viewed on the receiving device.
  - All links were clicked.
  - Replies to messages were sent.
  - Some messages were deleted.
- **Voice calls:**
  - Voice calls were conducted using the carrier subscription service.
  - Voice calls were conducted using each of the apps.
  - Some video calls were made using each of the apps.
- **Photos and videos:**
  - Photos and videos were made using both devices.
  - Some were created in the various apps.
  - Some photos and videos were sent using the apps.
- **Emails sent between the devices and from third-party accounts:**
  - Simple email messages were sent and received.
  - Emails with images including photos and links were sent and received.
  - All emails were viewed on the receiving device.
  - All links were clicked.
  - Replies to messages were sent.
- **Browsers:**
  - All browsers were opened and used for internet searches throughout the data-seeding period.
  - Some browsers were opened by clicking on links from messages and emails.
  - Some specific searches were conducted in the various browsers.
- Social networking:

- The three social networking apps were populated with the personal accounts of Paul Reedy.
- Partway through, the Twitter account @ReedyL was deleted and replaced with @4THStreetGlobal.
- Some interactions and messaging in Facebook and LinkedIn were conducted.
- Some interactions (viewing) with TikTok were conducted.

- Geospatial:
  - Travel to various locations around Washington, DC, and northern Virginia occurred while location services were switched on for each device.
- Some of the above activities were performed in the various locations.

On December 8, 2021, the phones were powered down in preparation to be sent to the lab for testing.

Process for Installing the TDES Software

The user manual provided by the software designers was followed yet required additional steps:

- The iPhone device required flight mode to be disabled; iTunes was required to be installed on a computer for which an iTunes user account was required and therefore was created. Disabling flight mode is counter to good forensic practice when examining a live phone because the phone can be wiped remotely.
- The Samsung device required substantial additional programs to be downloaded from the internet before the application would recognize the device.
  - Refer to **Attachment A – Android Report – TDES Manual**, which describes the steps required for the TDES software to operate and the additional steps needed for the software to function.

CJTEC

Operation Process of the TDES Tool

The FSU research team provided the user manuals for installing and operating the TDES tool. The installation and operation of TDES differed between the iPhone and the Samsung devices. For the software to function on either device, the operator must select the settings as they appear in **Appendix B – Camera Settings**.

The software provides no option to acquire the device, that is, the forensic acquisition (or physical image) of the data on the phone. The ability to acquire a device forensically is regarded as a "normal" or usual function of a mobile forensic tool. The inability to acquire the device means that a subsequent forensic analysis will require a new process that starts from the beginning using a validated mobile forensic tool. A subsequent forensic analysis is likely to reveal artifacts from the prior installation, operation, and removal (in whole or part) of the TDES tool and any other interactions and manipulations that the TDES user or other persons might have engaged in. As a result of the way the TDES tool is installed and operated, there is also an increased possibility of remote device wiping. These actions and their impacts are inconsistent with sound forensic practice.

It appears as though the TDES tool did not distinguish between messages in the various apps. The TDES tool refers to messages as "SMS messages" (pp. 14, 16, 17, 26, and 36 of Appendix A – Android Report – TDES Manual) but gives no indication of capturing messages in other apps. It was not possible to determine if the visualized messages were text messages or were app-to-app messages. Note, iMessages, the default message protocol for sending and receiving messages between iPhones, are not SMS protocol; similarly, messages sent via app to app[1] are not SMS protocol.

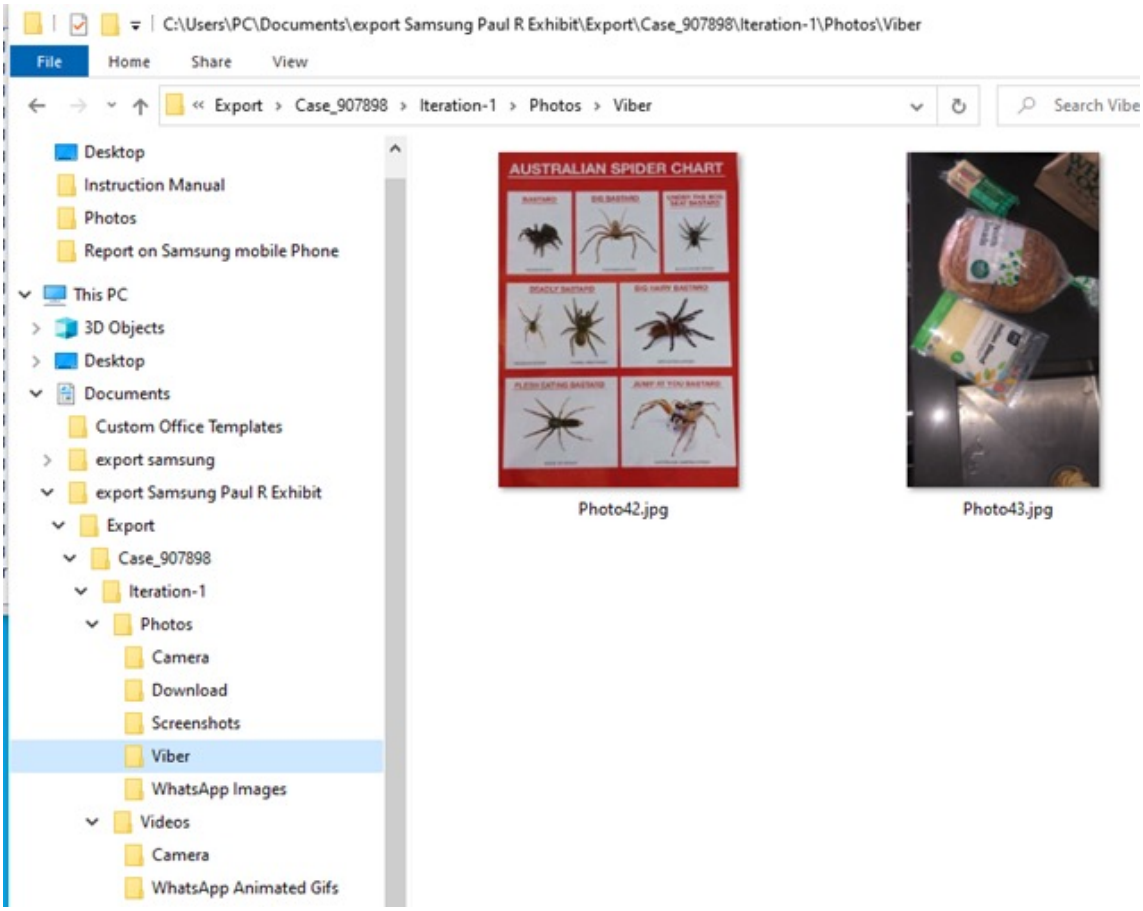
Similar to messages, the TDES tool refers to phone calls (see **Appendix A – Android Report – TDES Manual**), but there is no reference to calls through app-to-app[1] or video calls. The question then is: Did TDES extract calls other than phone calls?

The paper by Aggarwal et al. (2019) indicated that app-to-app messages could not be extracted. However, further doubt was cast on the sources of the messages because images purported to be sourced from Viber and WhatsApp were visible in the directory tree when TDES was operated in desktop mode (see **Figure 1**).

1. "App to app" refers to communications using third-party apps usually installed by the owner, such as WhatsApp and Viber.

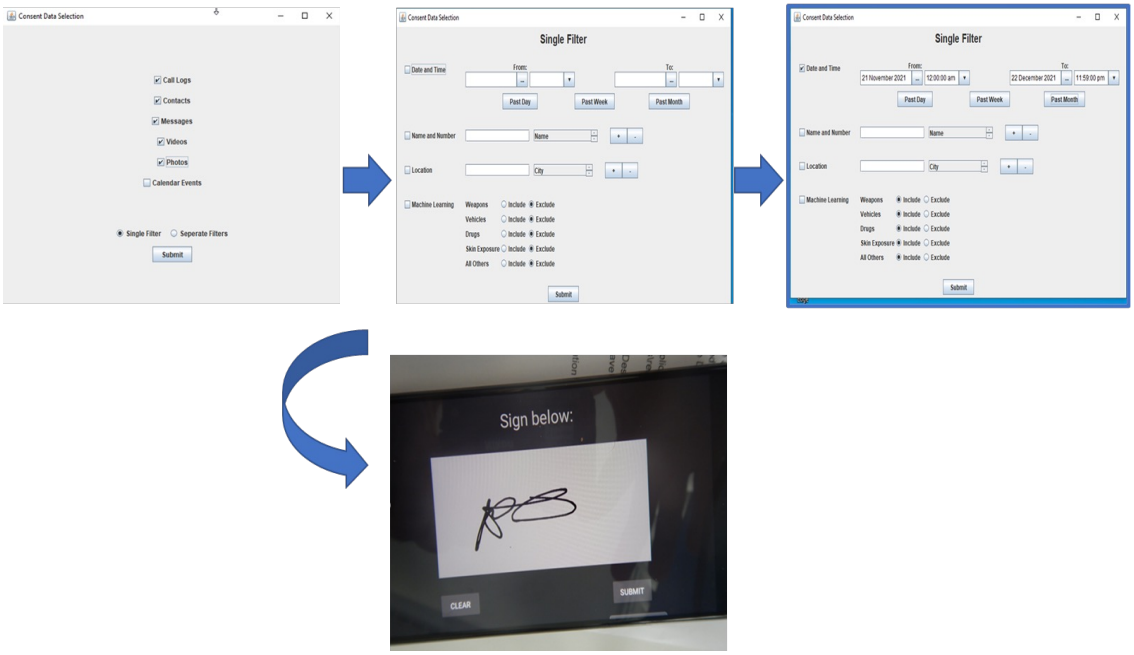
CJTEC

Figure 1–Displays a screenshot of a directory tree of exported images from the Samsung device. It shows a directory tree on the left and 2 photos on the right—one a 7-paneled Australian spider chart photographs and the other a photograph of grocery items.



To obtain the exported results, the user is presented with a series of filter screens for the selection of data to which the owner can consent. The workflow of this process is illustrated in **Figure 2**.

Figure 2–Displays the owner consent dialogue boxes in TDES as installed on the device. There are 4 images illustrating the process flow. The first one shows the type of data that can be chosen for filtered extraction, the second and third images present fields to define the filtering process (date and time frame, name and phone number associated with the investigation, and the fourth images shows the consent field, which requires a signature from the device's owner to enable data extraction.



Differences Between TDES and Other Industry Tools

TDES requires the user to manually enter the IMEI number into the app, which is an unusual action. Most commercial mobile forensic tools locate the IMEI when the device is connected to the computer hosting the tool. Requiring the user to find the IMEI leads to additional and unnecessary human interaction with the device, which is counter to sound forensic practice. Also, IMEI numbers contain around 15 characters, which provides an opportunity for error when the user manually enters the number.

TDES requires the user to manually type in the computer's IP address, which is highly unusual and prone to user error as noted above with the IMEI number. Instead, the number should be available on screen to the user to which they can respond either "yes" or "no."

The exported results did not meet expectations. Further detail is provided in the following results section.

Results

Testing Parameters

Testing parameters were designed before gaining access to the TDES tool and on the assumption that the conditions outlined in the paper by Aggarwal et al. (2019) could be reproduced.

- Attributes of files for testing included:
  - Files in root folder
  - Files in subfolders
  - Compressed files/folders
  - Encrypted files/folders
  - Symbolic links and extended attributes/ alternate data streams
- Data stream verification of each image, showing the contents of the root directory.
- Metadata verification demonstrating the correct interpretation of the file metadata, as represented by the file creation time.
- Operational design of the tool for examiners when performing casework included:
  - Implementation
  - Functionality
  - Usability
  - User interface
  - Reporting format
- Test in backup position acquisition for iOS (iPhone).
- Replicate tests in rootkit mode for Android (Samsung).
- Reliability included:
  - Testing of multiple common file types encountered in digital forensic science
  - Testing of user-defined settings.
  - Inclusion of data that meet the test query (i.e., acquire any and all data that are date/time stamped within the specified time interval, excluding all other data, as per the proverbial search warrant).
  - Exclusion of data that do not meet the test query (i.e., exclude any and all data that are date/time stamped outside of the specified time interval, as per the proverbial search warrant).
  - Results on altered files included:
    - Deleted files
    - Altered files (e.g., altered file extension)
    - Encrypted files
  - Forensic soundness (interference).
  - Alteration of data within the test query.
  - Alteration of extraneous data.
  - Overall impact and explainability of original evidence.
- Reporting included the following metadata:
  - File name
  - File type
  - File path
  - File size
  - File created/modified/access times
  - Attribute flags
  - Hash (MD5) value of the file

Unfortunately, once the tool was accessed, it became apparent that the testing parameters could not be executed as described, and some elements needed to be excluded because of insufficient time and budget.

CJTEC

Reference Tool

The reference tools chosen for the comparison were Cellebrite and Axiom (Magnet). Cellebrite and Axiom are regarded as the industry standard mobile forensic tools in the United States. Depending on availability and time, other tools that could be selected for comparison included MSAB suite, Open Text (EnCase), Hex Editor, Paraben, and Oxygen. The selected forensic tools operate with a write block preventing the loading of an agent or other data to the device. However, there are known (and unknown) differences in performance among all tools, and no tools are able to acquire 100% of all data from all devices. Cellebrite and Axiom were the only tools used in this test for reference.

Test Outcomes and Expectations

TDES does not have an acquisition function that would allow for more extensive analysis and confirmation of findings. The research paper referred to "off-device" analysis, which refers to the exported data.

The TDES software operates quite differently relative to other commercially available mobile forensic tools. Most tools require downloading an installation file from a website to an examiner's computer. The file is executed by the computer, which installs the drivers automatically onto the device when the device is connected to the computer. In this process, the computer either identifies the make and model of the device or the examiner selects the device's make and model through an interactive menu. Once the data are extracted or the process is completed, the computer program removes the tool's artifacts from the device.

TDES functions differently because it is a manual operation driven by the operator. Once the analysis is complete, artifacts from TDES remain on the phone and will be detectable later when a forensic analysis is performed.

TDES does not allow for a forensic copy of the data because it requires network and Bluetooth functionality to be enabled on the device when viewing iPhones. Failure to isolate the device from connection to the environment (e.g., the telephone subscriber network, IT networks, other devices) does not reflect sound forensic practice and is counter to recommended practice.

TDES does not allow the export of data from other messaging apps. According to the paper by Aggarwal et al. (2019), TDES is expected to extract the data types in **Table 2**. Additional apps were also included in the evaluation, which have been highlighted in blue.

CJTEC

Table 2–TDES expectations vs. verification results

Data Type	Metadata Type	Aggarwal et al.		Verification	
		iOS	Android	iOS*	Android
Photos	Date and Time	Yes	Yes	Not Tested	Unconfirmed**
	Location	Yes	Yes	Not Tested	Unconfirmed
	Album Type	Yes	Yes	Not Tested	Unconfirmed
	Album Type	Yes	Yes	Not Tested	Unconfirmed
Videos	Date and Time	Yes	Yes	Not Tested	Unconfirmed
	Location	Yes	Yes	Not Tested	Unconfirmed
Contacts	Name	Yes	Yes	Not Tested	Unconfirmed
	Number	Yes	Yes	Not Tested	Unconfirmed
	Area Code	Yes	Yes	Not Tested	Unconfirmed
	Email	Yes	Yes	Not Tested	Unconfirmed
Calendar Events	Date	Yes	Yes	Not Tested	Not Tested
Reminders	Date	Yes	Yes	Not Tested	Not Tested
Photos	Third-Party Apps	No	Yes	Not Tested	Unconfirmed
Messages/SMS/ MMS	Date and Time	No	Yes	Not Tested	Unconfirmed
	Contact Number	No	Yes	Not Tested	Yes
Call Logs	Incoming Calls	No	Yes	Not Tested	Yes
	Outgoing Calls	No	Yes	Not Tested	Yes
	Missed Calls	No	Yes	Not Tested	Unconfirmed
	Date and Time	No	Yes	Not Tested	Yes
Notes	Search String	No	No	Not Tested	Not Tested
	Date and Time	No	No	Not Tested	Not Tested
Voice Memos	Date and Time	No	No	Not Tested	Not Tested
Web History	Date and Time	No	No	Not Tested	No
Emails	Date and Time	No	No	Not Tested	No
Facebook Messages	Date and Time	No	No	Not Tested	No
WhatsApp Messages	Date and Time	No	No	Not Tested	Yes
LinkedIn Messages	Date and Time	No	No	Not Tested	No
WeChat Messages	Date and Time	No	No	Not Tested	Not Tested
Viber Messages	Date and Time	No	No	Not Tested	Yes
Telegram Messages	Date and Time	Not Tested	Not Tested	Not Tested	No
Signal Messages	Date and Time	Not Tested	Not Tested	Not Tested	No
Line Messages	Date and Time	Not Tested	Not Tested	Not Tested	No
TikTok	Date and Time	Not Tested	Not Tested	Not Tested	Not Tested
Snapchat	Date and Time	Not Tested	Not Tested	Not Tested	Not Tested

* The verification test for iOS was unable to be completed in the available time because the TDES software would not function, possibly due to the later version of iOS on the iPhone.

** Unconfirmed refers to the "data type" exported. The contents of files (e.g., photos, videos, messages etc) were exported; however, it was unclear if the associated metadata were also included in the export. The testing project was terminated before it could be established that the metadata had been exported correctly. Further, more time and additional analysis would have revealed a definitive result on whether the metadata were exported.

CJTEC

The inability to extract data from communications apps represents a flaw in the capability of the TDES software because most mobile communications are sent via third-party apps:

- In 2017, it was estimated that 22 billion texts were sent worldwide every day, referring to the native device app (SMS and iMessage), not including app-to-app messaging.[2,3]
- When compared with a year earlier in 2016, between Facebook Messenger and WhatsApp, a combined 60 billion messages were sent per day,[4] and by 2022, WhatsApp alone accounted for over 100 billion messages sent per day.[5,6]
- Even when fully functional to their current specifications (user-created data, internet- related data, third-party application data), most messaging communications are not going to be visible to an investigator when using the TDES tool because it cannot process and extract data from the most popular third-party messaging apps.

Table 3 lists the number of active users for common mobile phone communications apps.

Table3–Number of active users per communications app[7]

App	Users (millions)
WhatsApp	2,000
Facebook Messenger	1,300
WeChat	1,206
QQ	648
Telegram	433
Snapchat	400
Skype	300
Viber	260
Microsoft Teams	115
Line	84
KakaoTalk	52
Tango	38
Signal	20
Slack	12
Discord	7

2. Vermont State Highway Safety Office. (2019). *Worldwide texting statistics*. Retrieved from https://shso.vermont.gov/sites/ghsp/files/documents/Worldwide%20Texting%20Statistics.pdf
3. Domo. (n.d.). *Data never sleeps 5.0*. Retrieved from https://www.domo.com/learn/infographic/data-never-sleeps-5
4. Goode, L. (2016, April 12). Messenger and WhatsApp process 60 billion messages a day, three times more than SMS. *The Verge*. Retrieved from https://www.theverge.com/2016/4/12/11415198/facebook-messenger-whatsapp-number-messages-vs-sms-f8-2016
5. Dean, B. (2022, January 5). WhatsApp 2022 user statistics: How many people use WhatsApp? Backlingo. Retrieved from https://backlinko.com/whatsapp-users
6. Zuckerberg, M. (2020, October 29). *Facebook, Inc. (FB) third quarter 2020 results conference call*. Retrieved from https://s21.q4cdn.com/399680738/files/doc_financials/2020/q3/FB-Q3-2020-Earnings-Call-Transcript.pdf
7. Haqqi, T. (2021, January). *15 most popular instant messaging apps*. Retrieved from https://www.yahoo.com/video/15-most-popular-instant-messaging-102552363.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAI0LnKXB6E72qh2RWEvxucSTH0ICQr1VnNG2FKsamC8u1Wr8JySZskR3Ac1taeZE3D6ExYcBejx4_n0WaPeRP1TdXt1jRL7PDbJ9AzoC0Y314a3PTuypGF9LxdDy24k6LZoA3Er4QVe9oWHJPsmTIA5GukPbF2FzQ-pyuIGBBNFI

Process Efficiency

The process of using TDES took no longer than a few minutes once the user was familiar and experienced with using the tool. However, configuration of the software on the computer took several hours before the tool was able to recognize the device and the analysis could begin.

As noted above, different methods of operation of TDES are required for the iPhone (iOS) and the Samsung (Android). Apple (46%) and Samsung (29%) combined represent 75% of U.S. mobile phone usage according to survey respondents.[8] However, LG (9%), Motorola (5%), and Google (4%) phones all use Android operating systems, although some variation in operating "flavor" and configuration can be expected among manufacturers. Similar results were obtained when U.S. domestic smartphone market share shipments were analyzed.[9]

Test Findings

On December 23, 2021, as a result of the challenges encountered in successfully installing the TDES software, including the necessity to locate, download, and install some freeware files from the internet, testing was concluded at an early phase gate. It was determined that further testing and/or troubleshooting could not be completed without considerable resources directed toward future development of the tool. The following milestone from the statement of work functioned as a stop gate:

- Milestone 2: Test and evaluate TDES on each device; assess initial functionality; provide email update.

Extraction Efficiency and Efficacy

Additional images of firearms were added to the devices once they arrived at the lab for testing. Filters selected for firearms and TDES were able to identify and select these images on the Samsung device to the exclusion of other images present on the Samsung phone. The iPhone was not tested for this capability because of the aforementioned reasons.

Exported Information

Appendix A – Android Report – TDES Manual provides a step-through process that the user follows to extract data from phones.

- TDES allowed access to:
  - Calendar
  - Phone call logs
  - Contacts
  - Photos, media, and files (the file type[s] was not specified)
- TDES permitted:
  - "… TDES app to make and manage phone calls …"
  - "… TDES app to send and view SMS messages …"
  - Enabling transmissions is an unusual function and warrants further investigation. It is unusual that a device can be facilitated to perform its normal functions during examination.

8. Statistica. (2022). *What brand is your (primarily used) smartphone?* Retrieved from https://www.statista.com/forecasts/997241/smartphone-by-brand-in-the-us
9. Counterpoint. (2022). *US smartphone market share: By quarter*. Retrieved from https://www.counterpointresearch.com/us-market-smartphone-share/

- TDES displayed, albeit without content:
  - Messages that could be bookmarked
  - Viewed contents of messages, although it is unclear what this means

TDES allows videos to be viewed and played during the process of selection and export. However, it is unclear what impact viewing messages, files, etc., and playing videos would have on metadata if an investigator at a scene of a crime performed this function.

When using the filtering option, photos can be viewed and selected in gallery view. All files of interest are then exported following signed consent of the owner. However, notably, it appears that no metadata were exported. If metadata were exported, they could not be easily located.

According to the reference paper (Aggarwal et al., 2019), TDES uses SHA-1 hashing to ensure data integrity, which is transferred to the TDES Manager. The hashing function was not apparent on testing, which may have occurred because the validation test ended early, and the hashing function could not be investigated. Calculating hash values for each file is a fundamental digital forensic principle; the inability to calculate these values introduces a reasonable doubt about the reliability of the digital evidence.

The device data, including the graphic files, are exported in HTML format, which is an unsuitable format for further analysis. Conducting further analysis would require exporting of the SQL databases in which the data are stored.

The exported files partially met expectations (see **Appendix A – Android Report – TDES Manual**). The following file types were visible and could be exported:

- SMS messages
- Messages, which were bookmarked based on the selection criteria, although message content was not immediately visible
- Videos
- Photos
- Photos (imbedded within communications)
- Calendar
- Phone logs
- Contacts

Once the files have been identified for export, the user is presented with a consent function that allows the device owner to consent to the export of the files. The owner provides consent by signing an on-screen "user consent" signature panel after TDES has been installed and the filters applied to limit the data. The software installation needs to be simple; otherwise, it will be an inconvenience to the owner. Although the process of obtaining the owner's expressed consent addresses one of the major issues in mobile forensic science using a process that involves additional interaction with the evidential device is questionable because it introduces a reasonable doubt about the reliability of the evidence. Sound forensic practice requires minimal interaction with a target device that is a primary source of evidence.

Conclusion

FSU Concept

The FSU proposal set out to build a mobile device triage tool for the rapid, onsite identification and extraction of selected data at the scene of a crime in real time. This capability is needed because of the ubiquity of mobile devices and their ability to both intentionally and passively document events surrounding an incident, such as an accident, intimidation and coercion, or a homicide. In many situations, the owner of the mobile device is willing to provide the investigator with access to the specific data related to the incident and for which a documented consent agreement is provided. However, at the same time, witnesses and victims are often reluctant to provide such consent because they are concerned about potential compromise of their privacy given that the investigator might have access to data of a personal nature that are irrelevant to the incident. TDES provides the following features:

- Documented consent of the device owner to extraction of relevant information in the form of data on the device.
- Defined limits on the data that can be selected for export and visualized by the investigator based on time, location, and image type.
- Machine learning for the rapid identification of images that might be relevant to the investigation, for example, images of firearms relevant to a homicide investigation or detection of skin in cases of child exploitation.

Verification Recommendation: The verification project found that the TDES is not yet ready for use in operational settings. This finding is consistent with comments from the developers who advised that it is at an alpha stage of development.

Current State of the TDES Tool

The developers advised that they completed work on the tool in mid-2019 and that the tool would be unlikely to work if presented with devices, in this case iPhone and Samsung, that were more recent models or if the operating systems had been updated to later than 2019 versions. They recommended, albeit after test data had been already loaded onto the devices, that the respective iOS and Android operating systems should be returned to the versions that were current in 2019. This issue highlights a continuing challenge for mobile forensic science mobile phone manufacturers are continually updating their operating systems and shipped apps (and installing new apps). In addition, device owners typically install third-party apps. On average, apps are updated approximately once per month. Further, new versions or major revisions of apps are usually issued annually. Manufacturers of mobile device forensic tools are constantly investing in research and tool updates to keep up with the pace of change in the consumer market. Therefore, a tool such as TDES might be successful at the time that it is issued, but without continued investment, it will quickly become obsolete.

The concept of the TDES is generally sound, although it would require substantial investment to reach the beta stage where it can be fully tested and validated. TDES will then require ongoing investment to ensure that it continues to meet the contemporary requirements of mobile forensic science as mobile devices, their operating systems, and new applications are developed. When decisions are made regarding further investment and development in TDES, consideration should be given to the role of smartphones in Internet of Things ecosystems where the handheld smartphone and other mobile devices are often used to control the system.

Alternatively, given that 3 years have now passed since the latest iteration of TDES, an evaluation of current commercial offerings could be undertaken to understand their capabilities and whether they meet the objectives of TDES. If they do not meet TDES's objectives, then consideration could be given to supporting an investment in a similar capability for those commercial tools.

Recommendations for Future Development

Partway through the verification project, a member of the TDES research team responded to a request for some clarification on the tool. Advice was provided that work on the tool was completed by the middle of 2019 and was, in the opinion of the research team, a "… fully functioning system." The working system was platformed on the device and Windows computer systems available at that time.

In their response, the researchers anticipated that using later models of devices and operating systems might be challenging because of changes in libraries. In addition, TDES also included some open-source software that performs certain tasks with the TDES operation, which may have also required updating. To evaluate TDES's performance on the devices, which had by this time already been seeded with test data in their existing operating system versions, the researchers recommended that the devices' operating systems be restored to earlier versions that were current in 2019. It was further recommended that similar actions be taken with the computer system used for the TDES application. However, it was not possible to restore the devices' operating systems because the data seeding had been completed, testing had commenced, and both time and budget were finite. However, the computer system was adapted by creating a bootable solid-state drive with Windows 10 and used as the operating environment for the TDES application. Also of note, the timing of the TDES testing project coincided with reduced availability of the research team.

During the verification of TDES, the Criminal Justice Testing and Evaluation Consortium program identified the importance of technical communication between the developers and the verifier early in the evaluation planning process as an "opportunity for improvement" for future testing. This process will strengthen the experimental design and assist with forecasting potential challenges.

If the TDES tool is to be further developed, future development should focus on four areas:

- A robust acquisition function in which the data are exported in a format that facilitates further analysis should be included.
- TDES does not permit the creation of a forensic copy (image), as other commercial tools do, because TDES requires network and Bluetooth to be enabled when viewing iPhones. Further development work should be directed to the ability to operate TDES when the phone is isolated from its environment, therefore reducing the possibility of remote interference with the device and the data contained within it. Taking these steps will reduce the effect on the admissibility of evidence by addressing the concerns with introducing a potential reasonable doubt surrounding the evidence.
- Noting that most messages worldwide are sent app to app, further development of TDES should include the ability to extract data contained within popular communications apps, such as WhatsApp, Messenger, WeChat, QQ, and Telegram.
- Ongoing maintenance and support are necessary for digital evidence tools, especially mobile phones, so that they can meet the challenges presented by a rapidly evolving mobile device consumer market.

CJTEC

Suggested Citation

Reedy, P., Parsons, M. N., Planty, M., Ropero-Miller, J. (2022). *Verification Report: Targeted Data Extraction Systems (TDES) for Mobile Devices.* National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. https://cjtec.org/

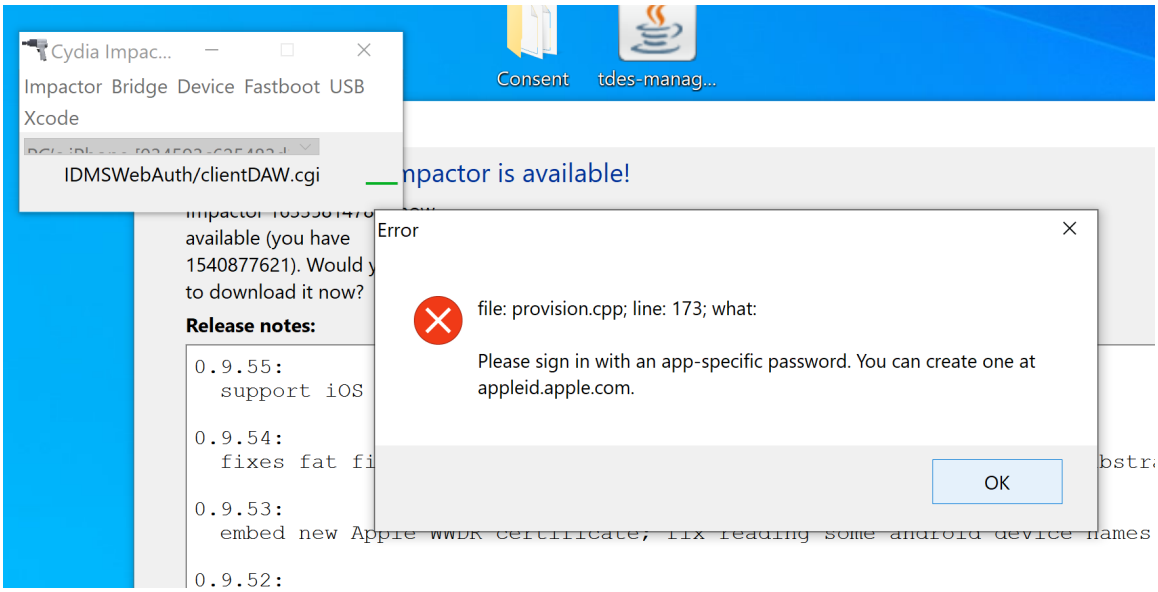
CJTEC would like to thank Paul Reedy, Forensic Scientist and Founder of 4th Street Global, for his expertise and insights in developing this document.

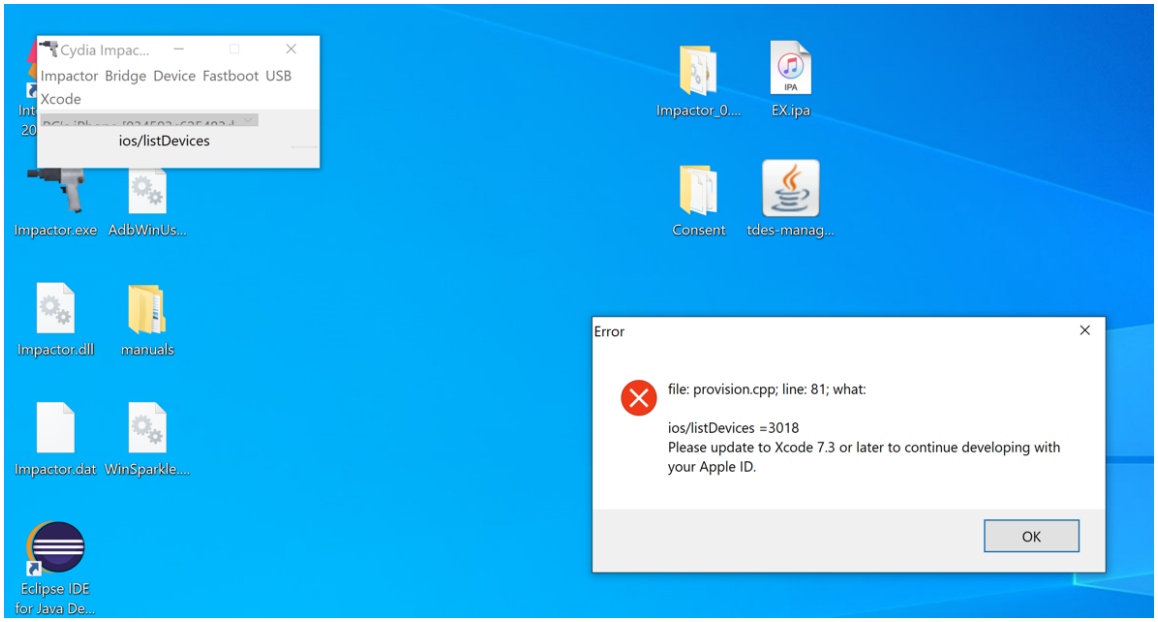
This publication was made possible by Award Number 2018-75-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

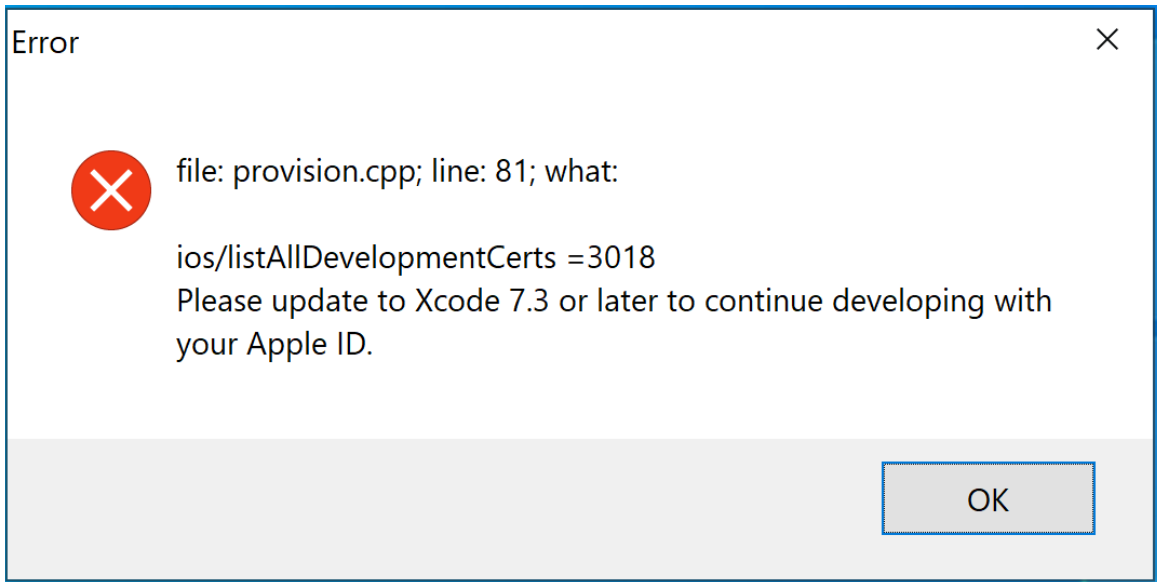
CJTEC

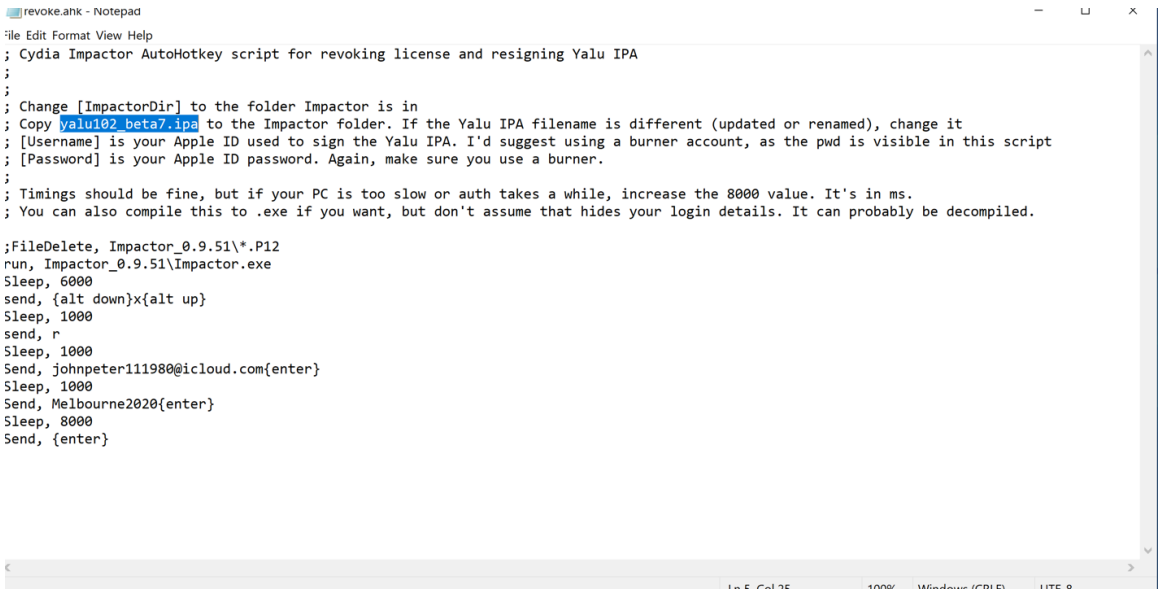
Appendix A: Android report – TDES manual

Errors encountered to rectify the Alpha version Android software:



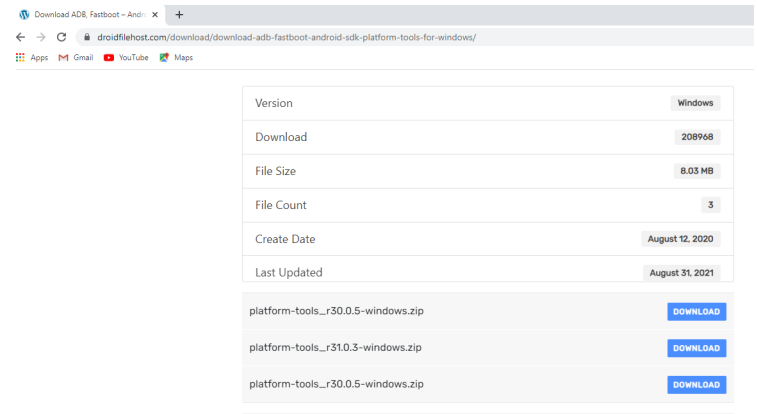
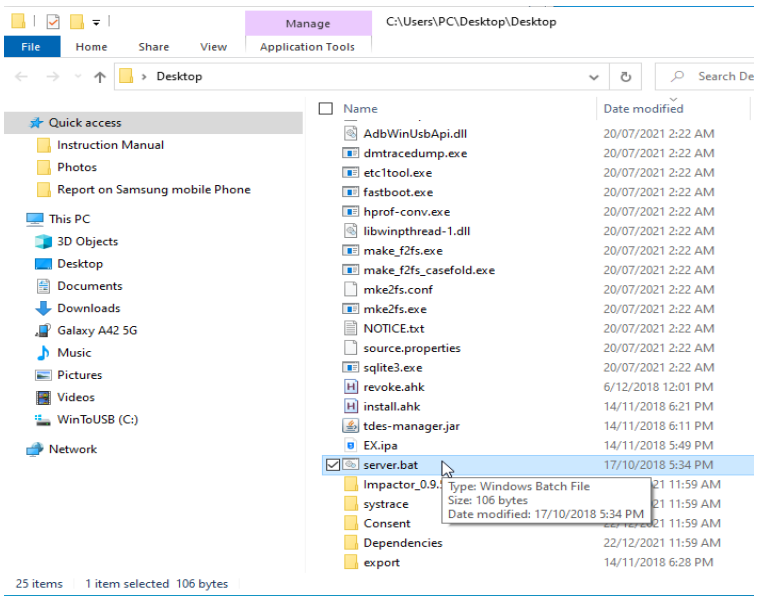



Error
file: provision.cpp; line: 81; what:
ios/listAllDevelopmentCerts =3018
Please update to Xcode 7.3 or later to continue developing with your Apple ID.
OK

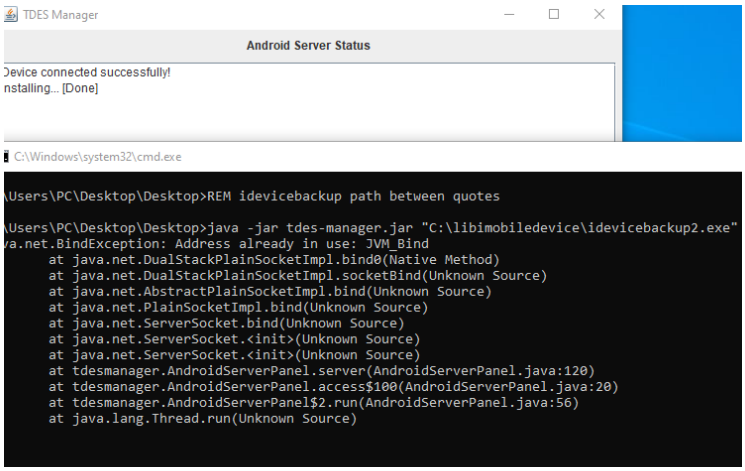
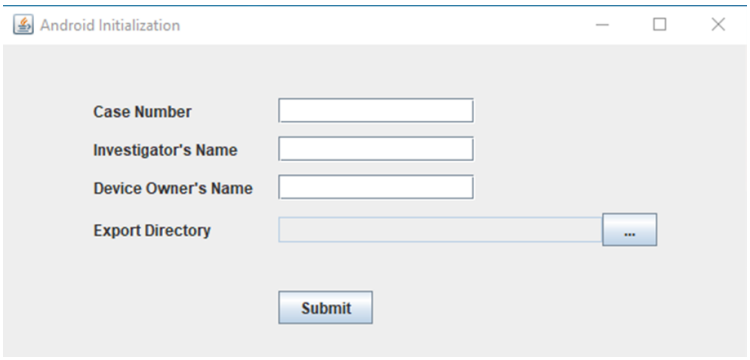
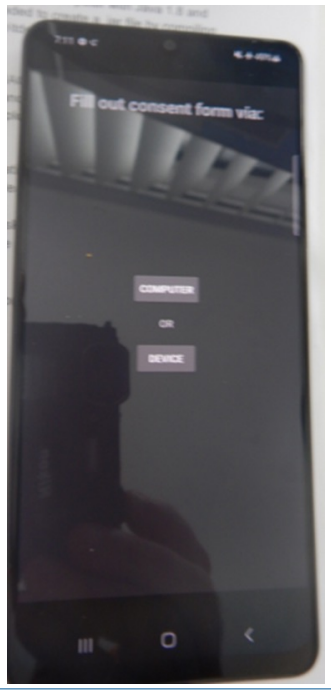

revoke.ahk - Notepad
File Edit Format View Help
; Cydia Impactor AutoHotkey script for revoking license and resigning Yalu IPA
;
;
; Change [ImpactorDir] to the folder Impactor is in
; Copy yalu102_beta7.ipa to the Impactor folder. If the Yalu IPA filename is different (updated or renamed), change it
; [Username] is your Apple ID used to sign the Yalu IPA. I'd suggest using a burner account, as the pwd is visible in this script
; [Password] is your Apple ID password. Again, make sure you use a burner.
;
; Timings should be fine, but if your PC is too slow or auth takes a while, increase the 8000 value. It's in ms.
; You can also compile this to .exe if you want, but don't assume that hides your login details. It can probably be decompiled.
;FileDelete, Impactor_0.9.51*.P12
run, Impactor_0.9.51\Impactor.exe
Sleep, 6000
send, {alt down}x{alt up}
Sleep, 1000
send, r
Sleep, 1000
Send, johnpeter111980@icloud.com{enter}
Sleep, 1000
Send, Melbourne2020{enter}
Sleep, 8000
Send, {enter}

CJTEC

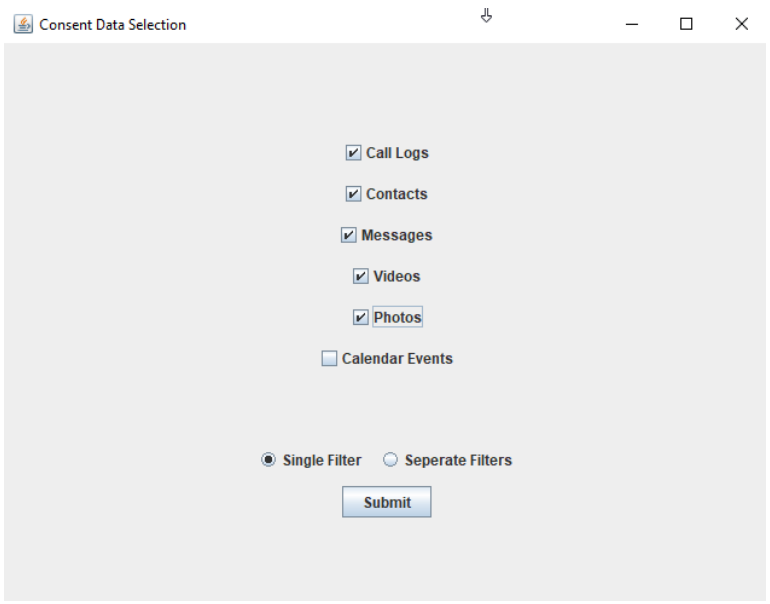
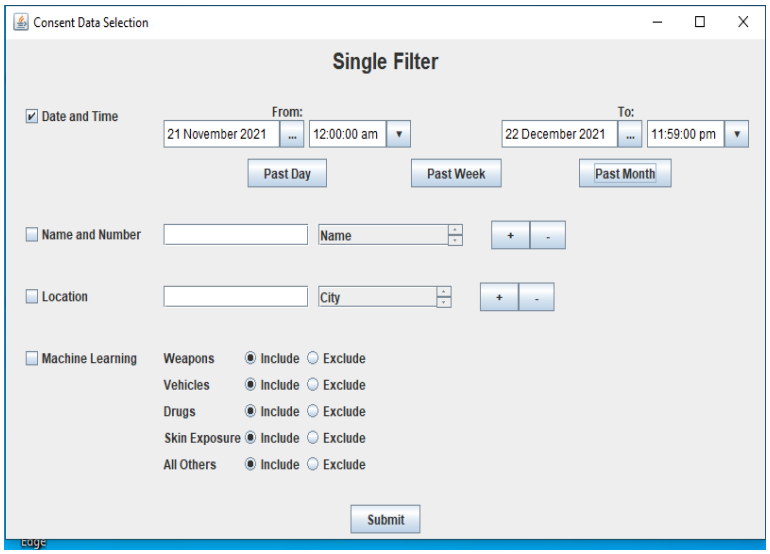
Table X–

Instructions	Screen Shot assessment	Comments
Require to download files from the internet as per screenshot and install them in the root folder of the Desktop folder.	platform-tools_r31.0.3-windows - https://droidfilehost.com/download/download-adb-fastboot-android-sdk-platform-tools-for-windows/ 	
Commands required to execute the application	Screen Shot 	

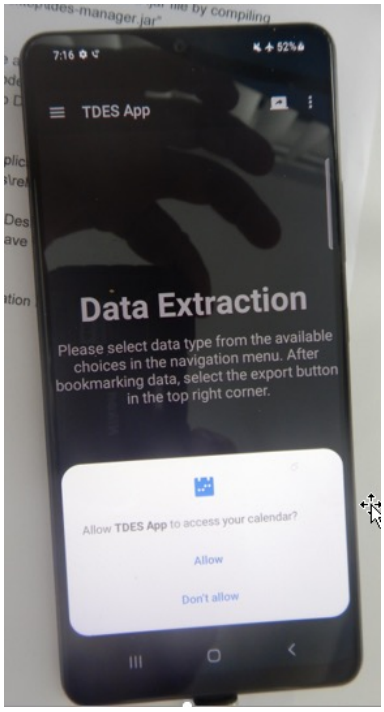
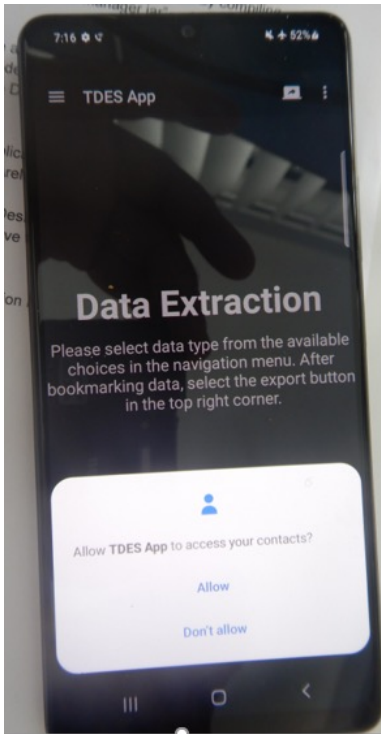
CJTEC

Instructions	Screen Shot assessment	Comments
C:\Users\PC\Desktop\Desktop\server.bat		
Populate desired fields		
Select computer from the Samsung Device		

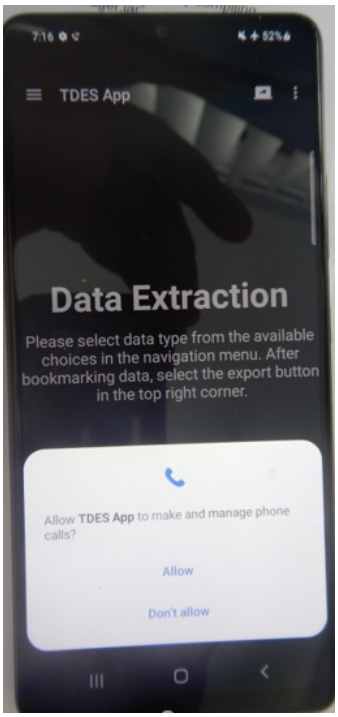
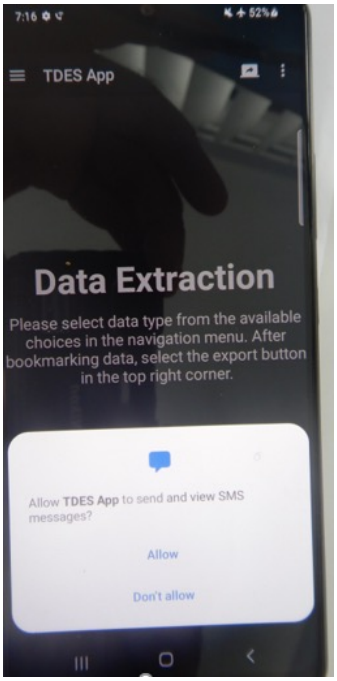
CJTEC

Instructions	Screen Shot assessment	Comments
Then the following screen appears on the computer	 	
Signed on the Samsung Phone		

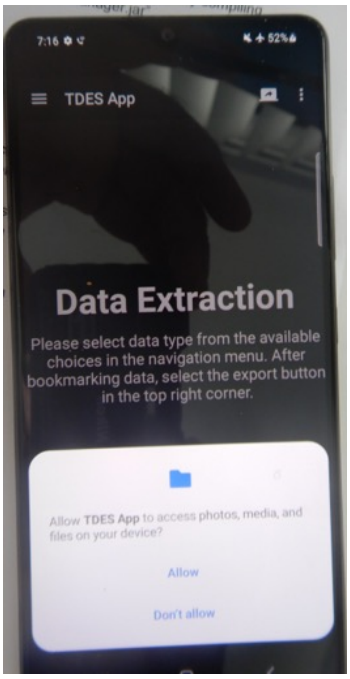
CJTEC

Instructions	Screen Shot assessment	Comments
Allow TDES APP to access Calendar		
Allow TDES App to access your contacts		

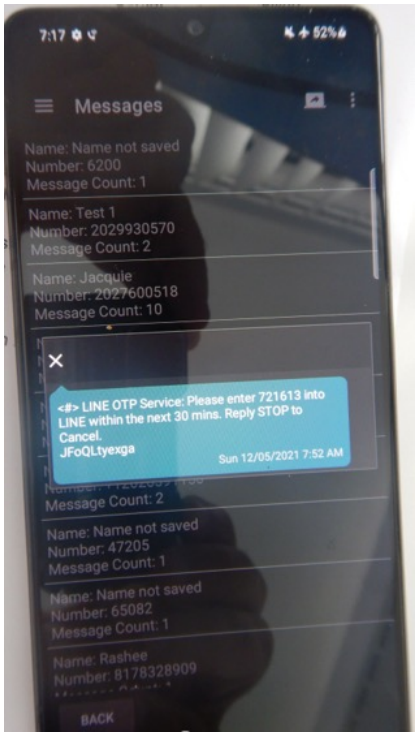
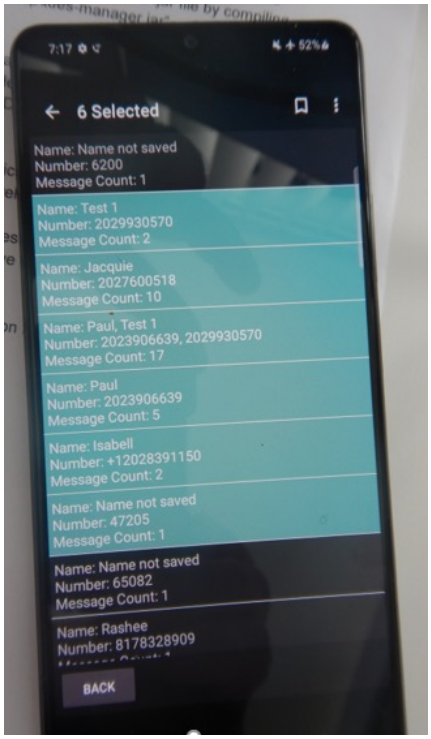
CJTEC

Instructions	Screen Shot assessment	Comments
Allow TDES APP to manage Phone Calls		
Allow TDES App to send and view SMS		

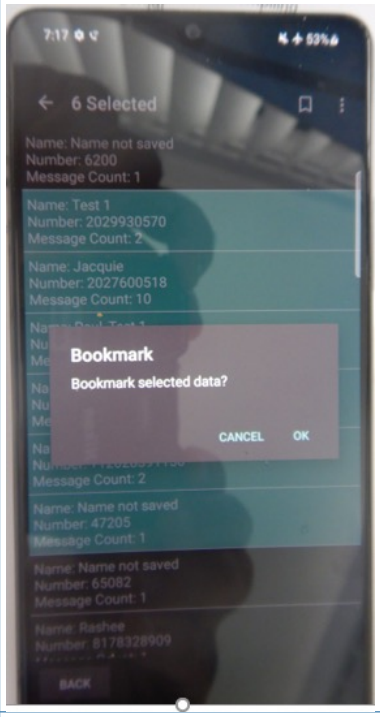
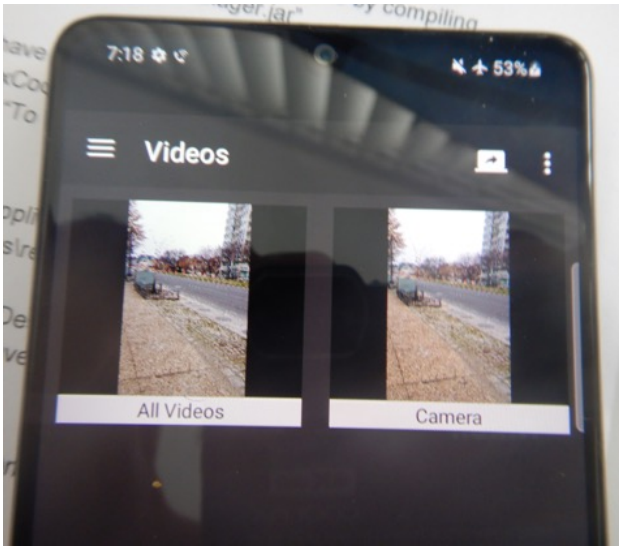
CJTEC

Instructions	Screen Shot assessment	Comments
Allow TDES App to access photos, media and files from the device		
Messages displayed		

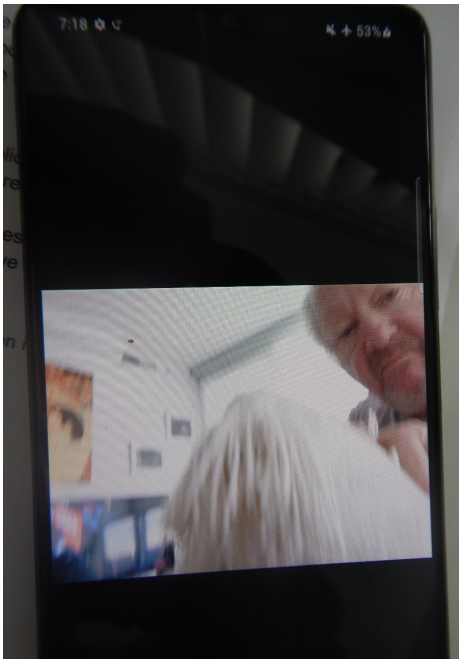
CJTEC

Instructions	Screen Shot assessment	Comments
Viewed comments of messages		
Selected 6 messages to Book Mark		

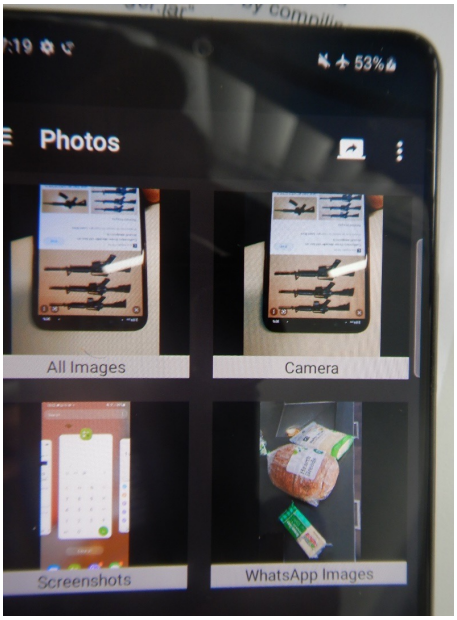
CJTEC

Instructions	Screen Shot assessment	Comments
A screen appeared to Book mark messaging		
Viewing Videos		

CJTEC

Instructions	Screen Shot assessment	Comments
Viewing videos/Camera		
Video can play on the phone while viewing		

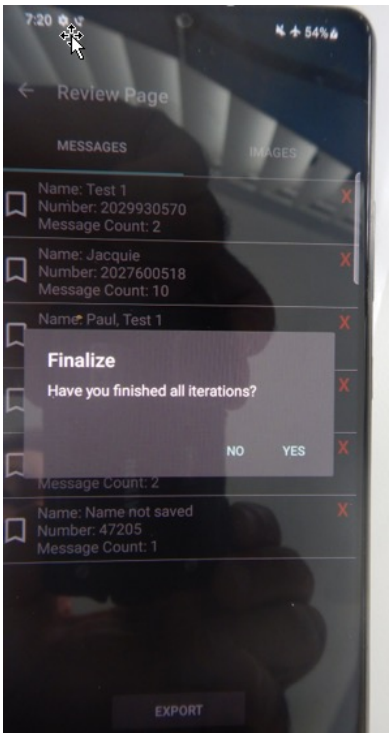
CJTEC

Instructions	Screen Shot assessment	Comments
Testing Filter Option		
Viewing Photos in gallery View		

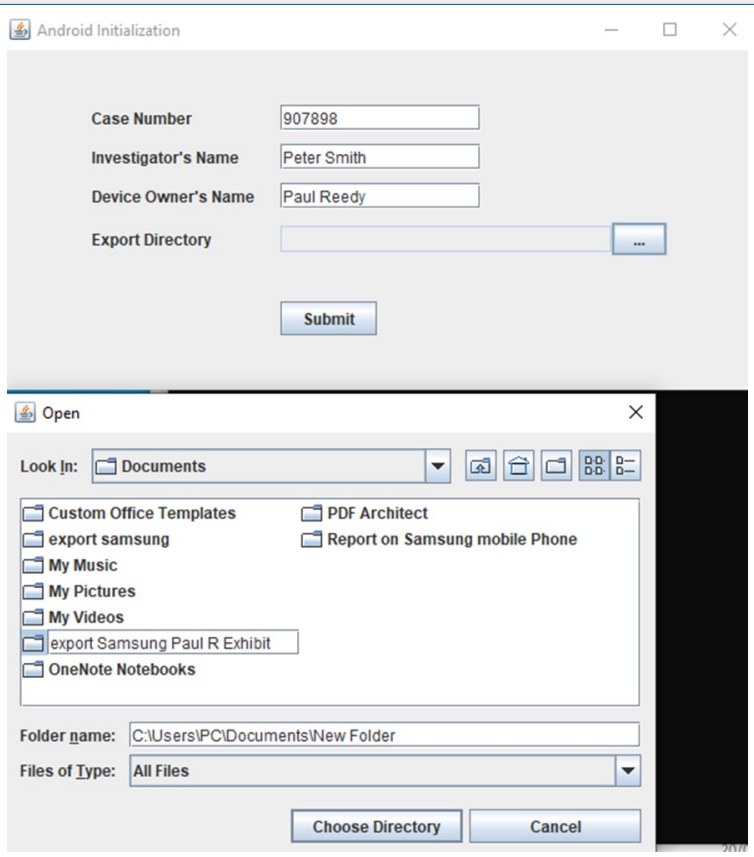
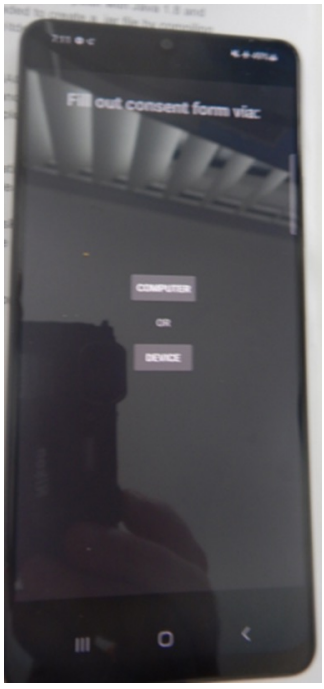
CJTEC

Instructions	Screen Shot assessment	Comments
Selecting Photos		
Reviewing the page		

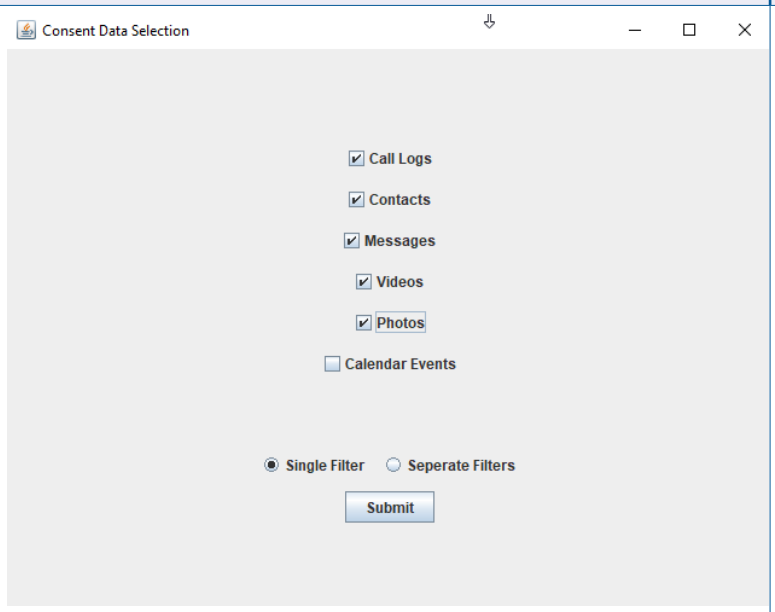
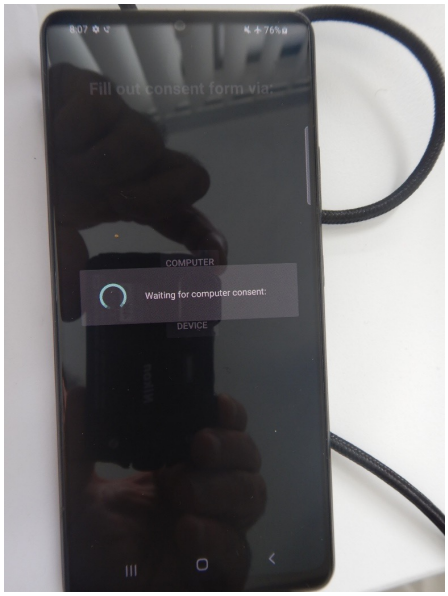
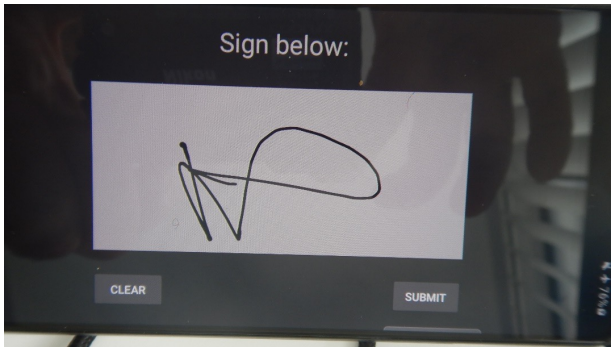
CJTEC

Instructions	Screen Shot assessment	Comments
Finished alterations		
Unable to export files on SSD		

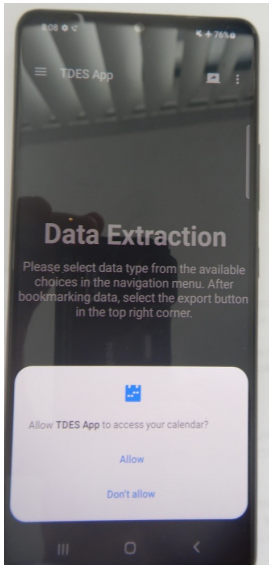
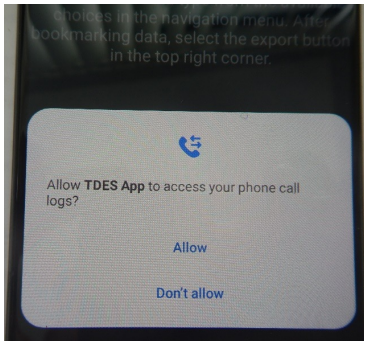
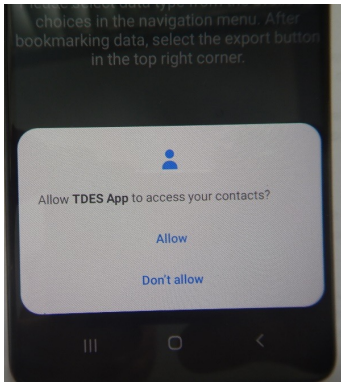
CJTEC

Instructions	Screen Shot assessment	Comments
New Examination started		
Selecting the export folder to create files too.		
Select computer from the Samsung Device		

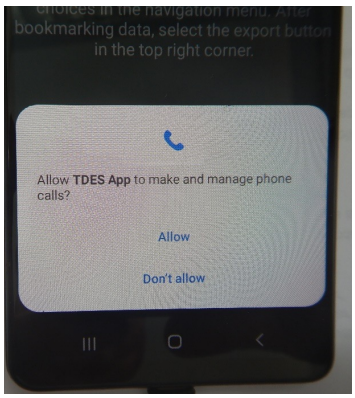
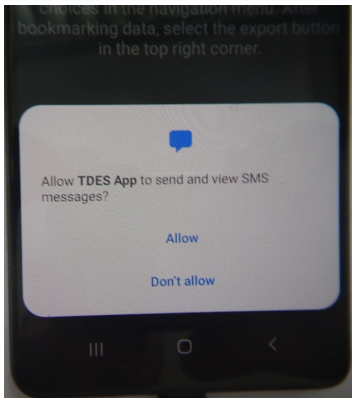
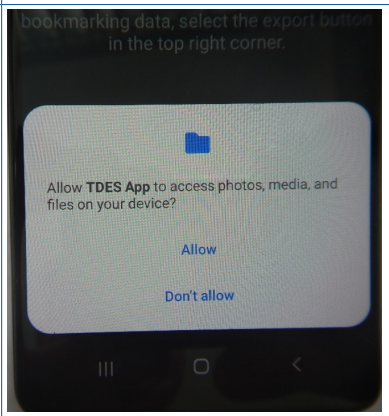
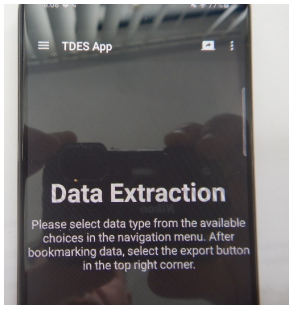
CJTEC

Instructions	Screen Shot assessment	Comments
Then the following screen appears on the computer		
		
		

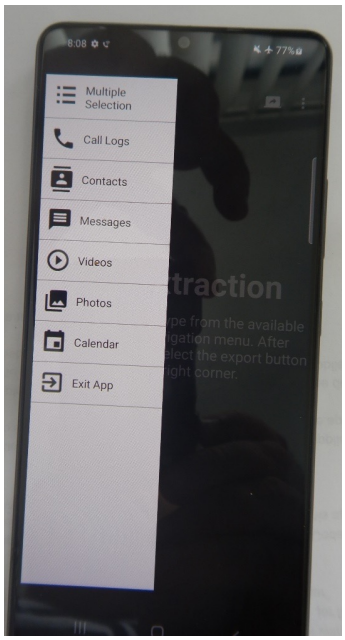
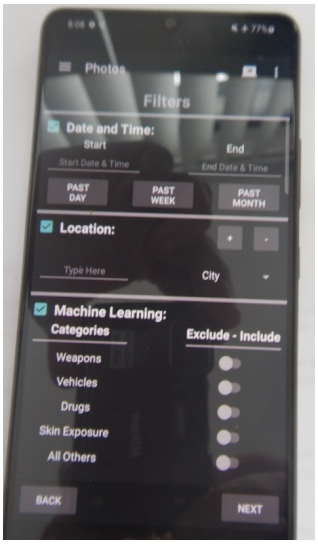
CJTEC

Instructions	Screen Shot assessment	Comments
		
		
		

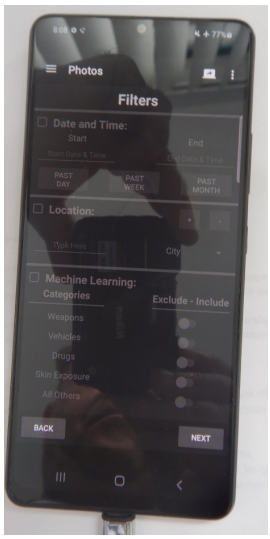
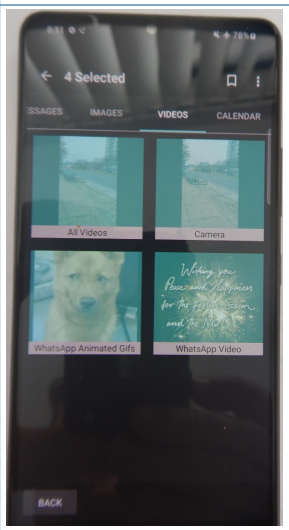
CJTEC

Instructions	Screen Shot assessment	Comments
		
		
		
		

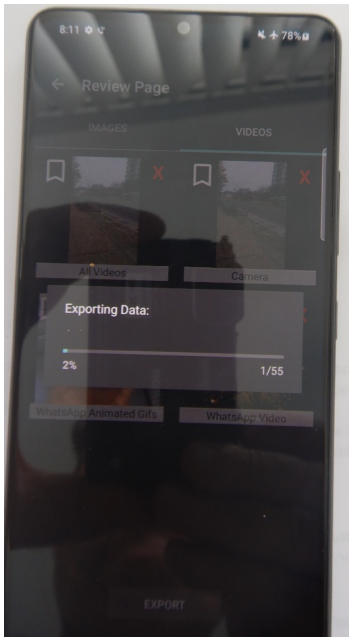
CJTEC

Instructions	Screen Shot assessment	Comments
		
		

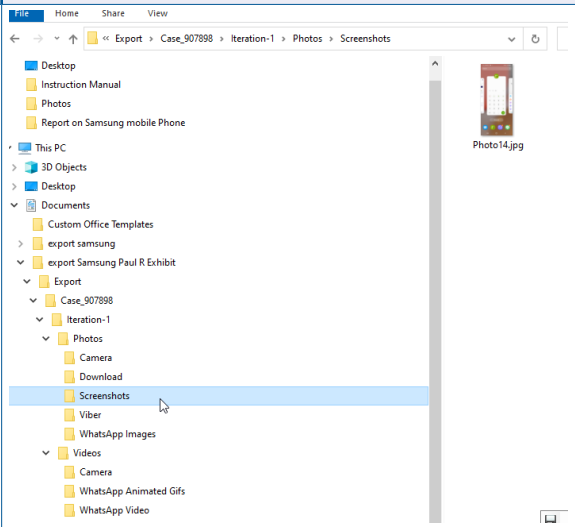
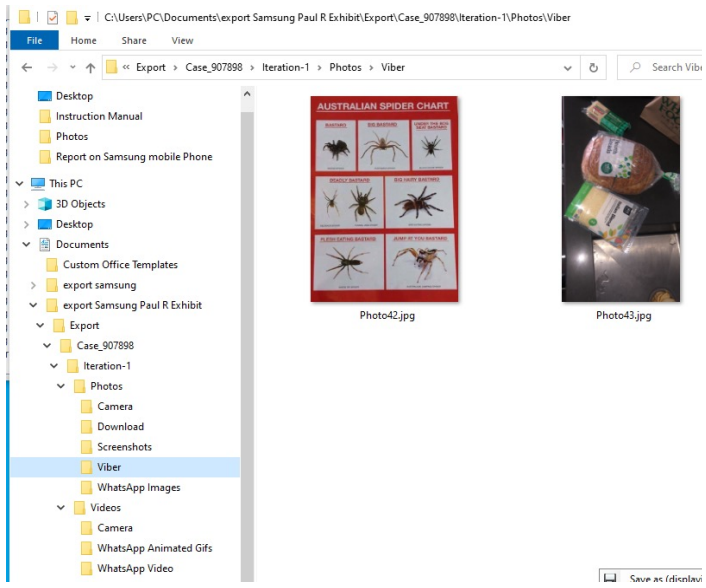
CJTEC

Instructions	Screen Shot assessment	Comments
		
		
		

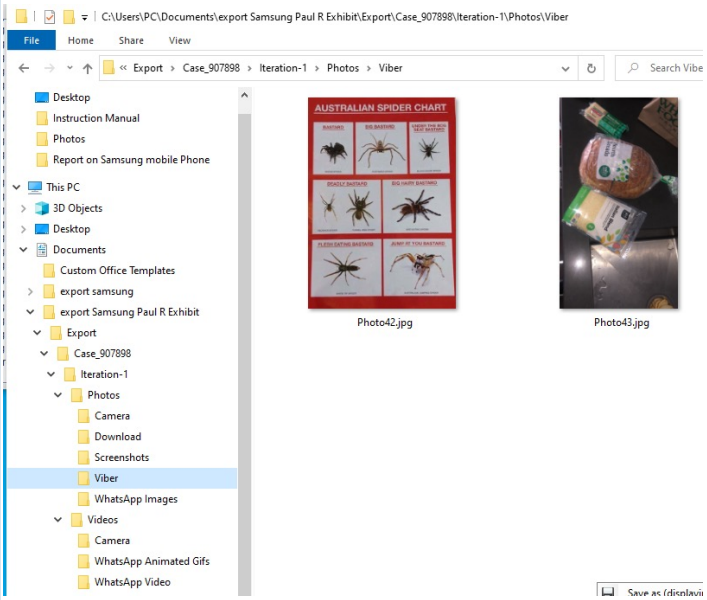
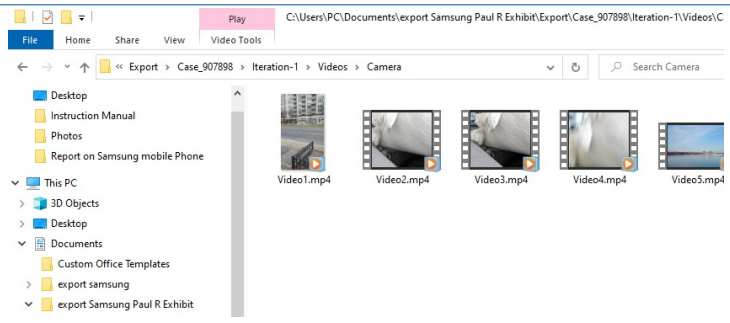
CJTEC

Instructions	Screen Shot assessment	Comments
		
		

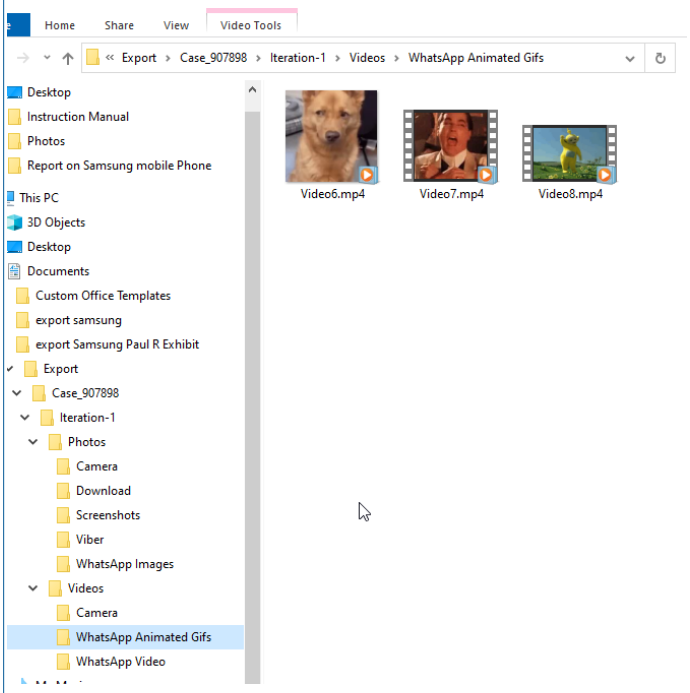
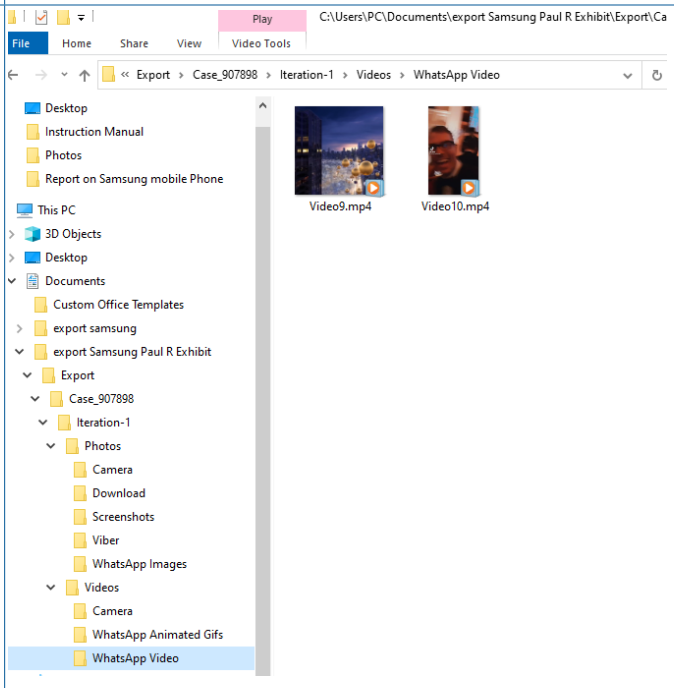
CJTEC

Instructions	Screen Shot assessment	Comments
		
		

CJTEC

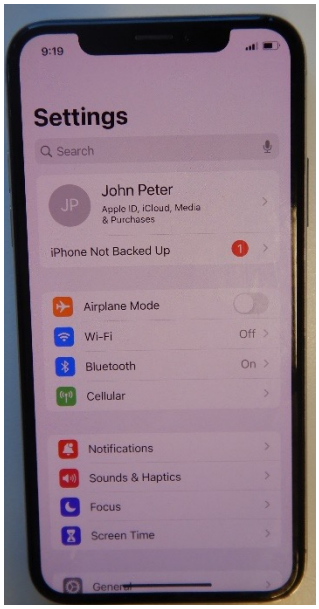
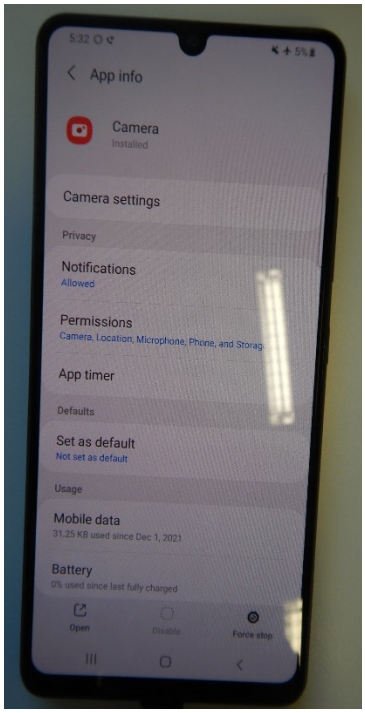
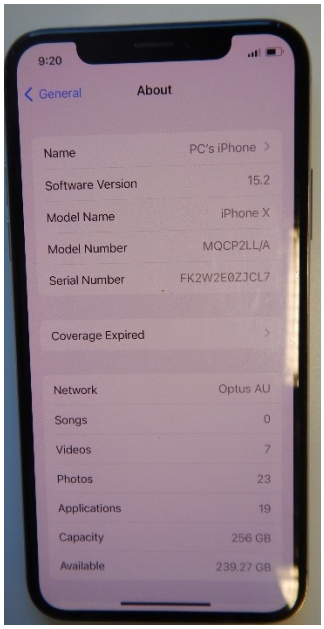
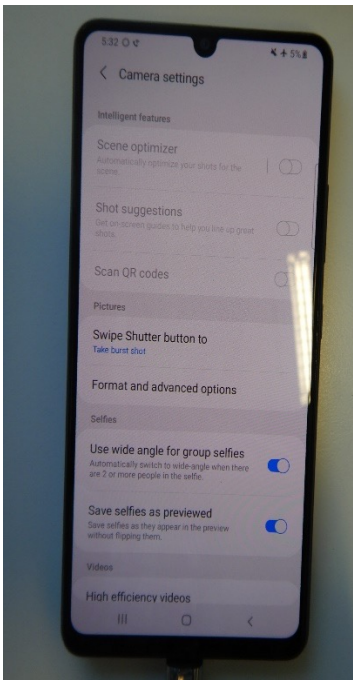
Instructions	Screen Shot assessment	Comments
		
		

CJTEC

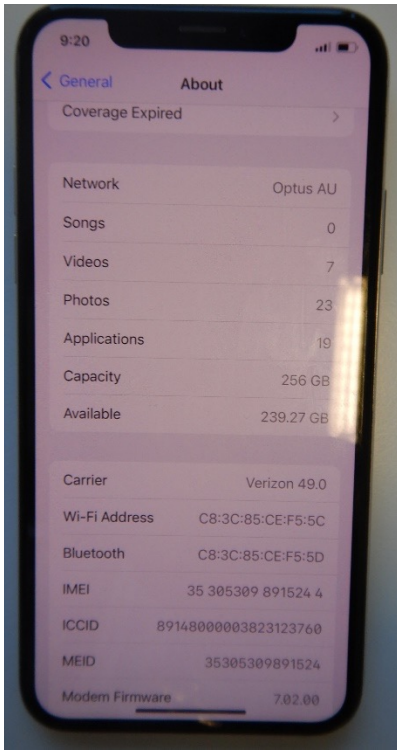
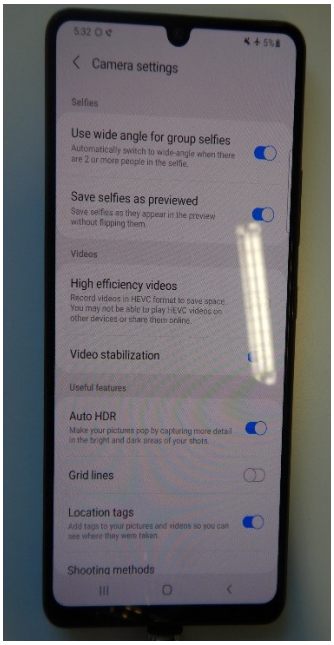
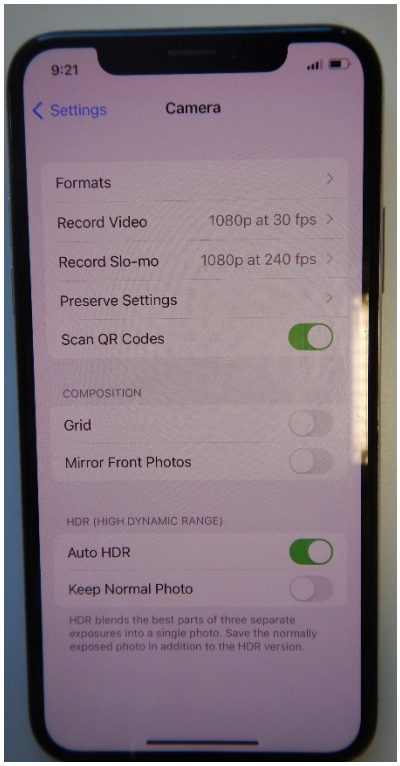
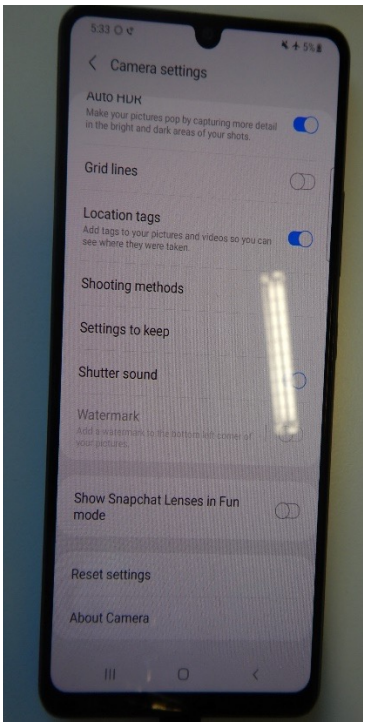
Instructions	Screen Shot assessment	Comments
		
		
CONCLUSION	No metada exported from the files selected. This software requires more development.	

CJTEC

Appendix B: Camera Settings

iPhone Camera Settings	Samsung Camera settings
	
	

CJTEC

iPhone Camera Settings	Samsung Camera settings
	
	

CJTEC

iPhone Camera Settings	Samsung Camera settings