

APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise risk of harm, it must be conducted ethically.

The University follows the OECD Frascati manual definition of **research activity**: “creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications”. As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the “principal researcher”.

This form must be completed and approved prior to undertaking any research activity.

SECTION A: About You (Principal Researcher)

1	Full Name:	Smit Brijeshkumar Patel
2	Student Number:	2506590
3	Email address:	2506590@student.uwtsd.ac.uk
4	Programme of Study:	MSc Cybersecurity and Digital Forensics
5	Supervisor:	Ramzi Djemai

SECTION B: Internal and External Ethical Guidance Materials

	Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, location-specific codes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines. You may add rows to this table if needed.		
1	UWTSD Research Ethics & Integrity Code of Practice		☒
2	UWTSD Research Data Management Policy		☒
3			☐
4			☐

SECTION C: Details of Research Activity

1	Indicative title:	Evaluating Cellebrite UFED and UFED Physical Analyzer Against WhatsApp, Signal and Telegram on Android		
2	Proposed start date:	June 2026	Proposed end date:	September 2026
	Introduction to the Research (maximum 300 words in each section) Ensure that you write for a <u>Non-Specialist Audience</u> when outlining your response to the three points below: <i>Purpose of Research Activity</i> <i>Proposed Research Question</i>			

	• <i>Aims of Research Activity</i> • <i>Objectives of Research Activity</i> Demonstrate, briefly, how Existing Research has informed the proposed activity and explain • <i>What the research activity will add to the body of knowledge</i> • <i>How it addresses an area of importance.</i>
3	Purpose of Research Activity This research investigates how effectively commercial forensic tools can acquire digital evidence from end-to-end encrypted (E2EE) messaging applications on modern Android smartphones. Smartphones are now central to everyday life, and encrypted messaging apps such as WhatsApp, Signal and Telegram are used by billions of people worldwide. This creates a fundamental challenge for digital forensic investigators: the same encryption that protects users' privacy also makes it very difficult to recover evidence during criminal or civil investigations. The purpose of this study is to address a gap in the academic literature. No published study identified during the literature review has conducted a controlled evaluation of Cellebrite UFED performance against these three applications on Android 16. The study is scoped to Android alone so that the evaluation can be completed to a consistent standard within the time available. If the Android work is finished with time remaining, the same protocol may be repeated on iOS as an optional extension, but iOS is not part of the planned work. Two Android environments are used for testing. The first is the researcher's own handset, running Android 16, factory reset and configured solely for the study. The second is a set of virtual Android 16 device images created through publicly available cloud-hosted emulator services, which removes the need to purchase additional hardware. All message content is researcher-generated synthetic data exchanged between accounts controlled by the researcher. Existing research shows a widening gap between the encryption used by messaging applications and what forensic tools recover from them. Published comparisons have reported markedly different accuracy figures for the same Signal dataset, and other work has shown that a routine tool update can change what an extraction appears to contain. This research adds reproducible experimental results and practical guidance for forensic practitioners, legal professionals and policy makers.
4	Research Question To what extent can Cellebrite UFED and UFED Physical Analyzer successfully acquire and analyse digital evidence from end-to-end encrypted mobile messaging applications (WhatsApp, Signal and Telegram) on the contemporary Android platform (Android 16), and what are the implications for forensic practice and for the European Union legal framework governing law enforcement processing of personal data, principally Directive (EU) 2016/680?
5	Aims of Research Activity This study evaluates how effectively Cellebrite UFED and UFED Physical Analyzer recover and decode evidential artefacts from WhatsApp, Signal and Telegram on Android 16, and what follows where recovery falls short of documented capability.

6	Objectives of Research Activity O1. Establish what has been tested across mobile acquisition, the Cellebrite platform and encrypted messaging artefacts, what remains untested, and how each application encrypts and stores its data, so that the experimental results can be explained by reference to each application's architecture rather than only reported. O2. Design and execute a controlled extraction across all three applications on identical seeded data under an established forensic methodology. O3. Measure tool performance against a standardised rubric of recovery rate, data integrity (SHA-256 comparison), artefact completeness and acquisition time, and compare the three applications against those criteria. O4. Assess the admissibility and chain-of-custody consequences of the results under Directive (EU) 2016/680, then produce a practitioner framework setting out which acquisition methods to attempt and what must be recorded when a tool returns nothing.
	Proposed data collection methods (maximum 600 words) Provide a brief summary of all the methods that may be used in the research activity to collect data, making it clear what specific techniques may be used. If methods other than those listed in this section are deemed appropriate later, additional ethical approval for those methods will be needed. You do not need to justify the methods here, but should instead describe how you intend to collect the data necessary for you to complete your project.
7	All primary research data will be generated by the researcher under controlled laboratory conditions. No real personal data, criminal data, or third-party communications will be used at any stage. Two Android 16 test environments will be used. The first is the researcher's own Android handset running Android 16. Before any test data is created the handset will be fully factory reset, so that no pre-existing personal content, contacts, accounts, or third-party messages remain on it. It will then be configured from new using test-only accounts created specifically for this study, and it will not be used for personal purposes at any point during the experimental phase. The second environment consists of virtual Android 16 device images generated through publicly available cloud-hosted Android emulator services, which allow a clean device image to be created and exported without the purchase of additional hardware. WhatsApp, Signal, and Telegram will be installed in both environments. A researcher-generated ground-truth dataset will be created in each: a minimum of 200 text messages per application per device pair, 20 image files, 10 audio/video files, and 10 call or voice records per application where supported, plus all associated metadata. All conversations will take place between accounts registered and controlled by the researcher. Because each application requires a telephone number at registration, the test accounts will be registered using virtual telephone numbers obtained from a commercial online SMS verification service. Only the one-time registration code is received through that service; no message content, contact data or acquisition output passes through it at any stage, and each number is used solely to activate a test account. No telephone number belonging to a third party will be used, no message will be exchanged with any other person, and no contact belonging to a third party will be stored on the test devices. Each of the six device-application combinations (3 applications x 2 Android 16 test environments) will be subjected to the Cellebrite UFED acquisition methods available for that device state: logical, file-system, and physical extraction. UFED Physical Analyzer will then decode and parse the extracted data. All acquisition images will be stored on encrypted, access-controlled storage media with SHA-256 hash values recorded at the point of acquisition. Quantitative performance data will be measured against a standardised rubric: Recovery Rate, Data Integrity (SHA-256 comparison), Artefact Completeness, and Acquisition Time. Qualitative analysis of the European Union legal framework, principally Directive (EU) 2016/680 on the processing of personal data by competent authorities for law enforcement purposes, will be conducted through thematic document analysis of primary legislation and case law. Experiments will be conducted in a network-isolated laboratory environment to prevent contamination of test devices. The physical handset will be placed in flight mode with Wi-Fi, mobile data, and Bluetooth disabled, and Faraday shielding will be used where available, so that the device state cannot be altered by remote

ETHICS FORM – COMPUTING STUDENTS ONLY

synchronisation or incoming traffic during acquisition.
If the Android phase is completed with time remaining, an equivalent iOS phase may be added. Any such extension would follow the same synthetic data protocol and the same acquisition rubric, and would collect no additional categories of data.

SECTION D: Scope of Research Activity

	Will the research activity include:	YES	NO
1	Use of a questionnaire or similar research instrument?	☐	☒
2	Use of interviews?	☐	☒
3	Use of focus groups?	☐	☒
4	Use of participant diaries?	☐	☒
5	Use of video or audio recording?	☐	☒
6	Use of computer-generated log files?	☒	☐
7	Participant observation with their knowledge?	☐	☒
8	Participant observation without their knowledge?	☐	☒
9	Access to personal or confidential information without the participants' specific consent?	☐	☒
10	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	☒
11	Performance of any acts which may cause embarrassment or affect self-esteem?	☐	☒
12	Investigation of participants involved in illegal activities?	☐	☒
13	Use of procedures that involve deception?	☐	☒
14	Administration of any substance, agent or placebo?	☐	☒
15	Working with live vertebrate animals?	☐	☒
16	Procedures that may have a negative impact on the environment?	☐	☒
17	Other primary data collection methods. Please indicate the type of data collection method(s) below.		
	Details of any other primary data collection method:	☐	☒
	N/A – this study uses only controlled laboratory experimentation and qualitative document analysis. No other primary data collection methods are used.		

ETHICS FORM – COMPUTING STUDENTS ONLY

If you have ticked NO to every question then the research activity is (ethically) low risk and you may skip section E and continue to section F.

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

SECTION E: Intended Participants

	Who are the intended participants:	YES	NO
1	Students or staff at the University?	☐	☒
2	Adults (over the age of 18 and competent to give consent)?	☐	☒
3	Vulnerable adults?	☐	☒
4	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	☐	☒
5	Prisoners?	☐	☒
6	Young offenders?	☐	☒
7	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	☒
8	People engaged in illegal activities?	☐	☒
9	Others. Please indicate the participants below, and specifically any group who may be unable to give consent.	☐	☒
	Details of any other participant groups:		

	Participant numbers and source Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?	
10	How many participants are expected?	N/A
11	Who will the participants be?	N/A
12	How will you identify the participants?	N/A

	Information for participants:	YES	NO	N/A
13	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	☐	☐	☒
14	Will you tell participants that their participation is voluntary?	☐	☐	☒
15	Will you obtain written consent for participation?	☐	☐	☒
16	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	☒
17	If the research is observational, will you ask participants for their consent to being observed?	☐	☐	☒
18	Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	☒
19	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	☒

ETHICS FORM – COMPUTING STUDENTS ONLY

20	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	☐	☐	☒
21	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	☒
22	If NO to any of above questions, please give an explanation			
	You should be able to tick YES for all of these questions. If not, then explain why not in this box. N/A			

	Information for participants:	YES	NO	N/A
24	Will participants be paid?	☐	☐	☒
25	Is specialist electrical or other equipment to be used with participants?	☐	☐	☒
26	Are there any financial or other interests to the investigator or University arising from this study?	☐	☐	☒
27	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	☐	☒
28	If YES to any question, please provide full details			
	You should be able to tick NO for most of these questions. For any cases that you have ticked YES then provide details in this box. If you are using cameras/voice recorders to record interviews then please state that in this box. N/A			

SECTION F: Anticipated Risks

	Outline any anticipated risks that may adversely affect any of the participants, the researchers and/or the University, and the steps that will be taken to address them.	
1	Risks to participants For example: sector-specific health & safety, emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information. If you have identified in section D that there are no participants then enter N/A and go skip to question 3.	
	Risk to participants: There are always risks. Do not write N/A unless you have no participants. There are no human participants in this research, so there are no risks to participants. All data is researcher-generated synthetic data.	How you will mitigate the risk to participants: N/A – no participants; no mitigation required.
2	If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities	
	This research does not involve human participants, sensitive topics, or real personal data. There are no foreseeable circumstances in which sensitive participant disclosures could arise. However, the research may incidentally surface knowledge about security vulnerabilities in forensic tools or encrypted applications. Any such findings will be handled responsibly in line with established responsible disclosure principles and reported in a balanced, academically appropriate manner.	
3	Risks to the investigator For example: personal health & safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest	

ETHICS FORM – COMPUTING STUDENTS ONLY

	Risk to the investigator: There are always risks. Do not write NA. The primary risk to the investigator is legal misunderstanding regarding the lawful academic use of Cellebrite UFED. A second risk arises from the use of the researcher's own handset as a test device: if the device were not properly reset, personal data belonging to the researcher, or to people who have previously messaged the researcher, could be captured in an acquisition image. There is also a minor risk of digital contamination of test environments or accidental exposure to unintended data if procedures are not followed correctly.	<i>How you will mitigate the risk to the investigator:</i> All experiments will use researcher-generated synthetic data only – no real personal data will be processed. The personal handset will be factory reset before any test account is created and again after data collection ends. Because the reset precedes both account creation and the generation of any test data, the device holds no content relating to the researcher or to any third party at any point during acquisition, and no such data can be captured in an acquisition image. Any residual personal artefact nonetheless encountered will be deleted immediately and will not be analysed or reported. Cellebrite UFED will be used within the University's Digital Forensics Laboratory under academic licence and within the scope of the approved ethics protocol. The investigator will seek guidance from the supervisor if any legal ambiguities arise during the study.
4	University/institutional risks For example: adverse publicity, financial loss, data protection	
	Risk to the University: There are always risks. Do not write NA. There is a reputational risk if the research is perceived as facilitating unlawful surveillance or misuse of forensic tools. There is also a minor data security risk if acquisition images were lost or accessed by unauthorised parties, even though all data is synthetic.	<i>How you will mitigate the risk to the University:</i> The research will be conducted strictly within the approved ethics framework and under academic licence conditions for all software tools. No real personal data will be processed. All acquisition images will be stored on AES-256 encrypted, password-protected external storage held securely by the researcher, accessible only to the principal researcher and supervisor. Cloud-hosted Android emulator services and the online SMS verification service used to obtain test telephone numbers will both be used in accordance with their published terms of service. Nothing will be uploaded to the emulator services beyond what is required to create a clean device image, and nothing will be sent to the SMS service beyond a request for a virtual number. No acquisition output, message content or research data will be uploaded to any third-party service. Should the terms of service of any messaging application prohibit registration by virtual number, that application will instead be registered using a physical SIM controlled by the researcher. The research proposal clearly documents the lawful and academic nature of the study.
5	Environmental risks For example: accidental spillage of pollutants, damage to local ecosystems	

ETHICS FORM – COMPUTING STUDENTS ONLY

	Risk to the environment: This research involves no chemical substances, biological agents, fieldwork, or physical hardware beyond standard computing equipment. There are no foreseeable environmental risks.	How you will mitigate the risk to environment: No specific environmental mitigation is required. Standard institutional IT disposal procedures will be followed for any storage media at the end of the project.
--	---	--

SECTION G: Feedback, Consent and Confidentiality

If you have identified in section D that there are no participants then enter skip this section and continue to section H.

1	Feedback What de-briefing and feedback will be provided to participants, how will this be done and when?
	You don't need to email your participants with your final report. A good alternative is to set up an email address that they will be able to contact for further details or results. N/A – there are no human participants in this research, and therefore no debriefing or feedback process is required.
2	Informed consent Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded in accordance with prevailing data protection legislation.
	If you are using a paper questionnaire then you should have the participants sign an appropriate consent form. These forms will count as personal data and should be noted as such in section J. If you are using an online questionnaire, then you should have a screen before the questions start that acts as a consent form, informing participants that by clicking on the NEXT button they are providing consent. N/A – there are no human participants. No consent forms are required. The research uses only researcher-generated synthetic data and no individuals are involved in data collection.
3	Confidentiality / Anonymity Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.
	Do not collect names unless you really need them. Do not name participants or organisations in any research publications (including the thesis) without their explicit permission. N/A – there are no human participants and no personal data is collected. Full anonymity is guaranteed by design, as all data is synthetic and researcher-generated. No individuals will be named in the thesis or any publications arising from this research.

SECTION H: Data Protection and Storage

	Does the research activity involve personal data (as defined by the General Data Protection Regulation 2016 “GDPR” and the Data Protection Act 2018 “DPA”)?	YES	NO
1	“Personal data” means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Any video or audio recordings of participants is considered to be personal data.	☐	☒

ETHICS FORM – COMPUTING STUDENTS ONLY

	If YES, provide a description of the data and explain why this data needs to be collected:		
2	This includes audio/video data of participants, but can also include IP addresses and usernames. Names, addresses and emails also count, as do consent forms. This research does not involve personal data as defined by UK GDPR and the Data Protection Act 2018. All data used is researcher-generated synthetic data created under controlled laboratory conditions. No real names, addresses, communications, or identifiers relating to any natural person will be collected or processed at any stage.		
	Does it involve special category data (as defined by the GDPR)?	YES	NO
3	“Special category data” means sensitive personal data consisting of information as to the data subjects’ – (a) racial or ethnic origin, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),	☐	☒
	(e) physical or mental health or condition, (f) sexual life, (g) genetics, (h) biometric data (as used for ID purposes),		
	If YES, provide a description of the special category data and explain why this data needs to be collected:		
4	What counts as ‘sensitive’ will differ between cultures. Any information on behaviour that is not in accordance with cultural norms would count as sensitive personal data. N/A – this research does not involve special category data. No real personal data of any kind is processed.		

	Will data from the research activity (collected data, drafts of the thesis, or materials for publication) be stored in any of the following ways?	YES	NO
5	Manual files (i.e. in paper form)?	☐	☒
6	University computers?	☒	☐
7	Private company computers?	☐	☒
8	Home or other personal computers?	☒	☐
9	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	☒	☐
10	“Cloud” storage or websites?	☒	☐
11	Other – specify:	☐	☒
12	For all stored data, explain the measures in place to ensure the security of the data collected, data confidentiality, including details of backup procedures, password protection, encryption, anonymisation and pseudonymisation:		
	All data will be kept in password protected cloud storage on the University Office 365 system which will not be shared. Any USB sticks used to store or transfer data will be password protected. All research data (virtual device images, acquisition outputs, analysis files, and thesis drafts) will be stored on AES-256 encrypted, password-protected external storage media held securely by the principal researcher. Thesis drafts will additionally be saved to the University’s password-protected Office 365 storage. No unencrypted copies will be made. All storage devices will be reformatted securely at the end of the project, and the personal handset used as a test device will be factory reset once data collection is complete. SHA-256 hash values will be recorded for all acquisition images at the point of creation to ensure integrity throughout the research period.		

ETHICS FORM – COMPUTING STUDENTS ONLY

Data Protection			
	Will the research activity involve any of the following activities:	YES	NO
13	Electronic transfer of data in any form?	☒	☐
14	Sharing of data with others at the University outside of the immediate research team?	☐	☒
15	Sharing of data with other organisations?	☐	☒
16	Export of data outside the UK or importing of data from outside the UK?	☒	☐
17	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	☒
18	Publication of data that might allow identification of individuals?	☐	☒
19	If YES to any question, please provide full details, explaining how this will be conducted in accordance with the GDPR and Data Protection Act (2018) (and/or any international equivalent):		
	No personal data as defined by UK GDPR is generated or processed in this research. All experimental data is synthetic and researcher-generated. Thesis drafts will be stored in the password-protected University Office 365 system and will not be shared outside the research team. Any encrypted storage devices used to transfer or store acquisition images will be AES-256 password-protected. All data will be retained until the completion of the project and then securely deleted. Question 16 is answered YES because two external services with servers that may be located outside the UK are used. The first is the cloud-hosted emulator service through which clean virtual Android device images are created and downloaded; the only data involved is a synthetic Android device image containing no personal data of any kind. The second is the online SMS verification service used to obtain virtual telephone numbers for the test accounts; the only data involved is a one-time registration code. No acquisition output, message content, research data or thesis material will be transferred outside the UK.		
20	List all who will have access to the data generated by the research activity:		
	The principal researcher (Smit Brijeshkumar Patel) and the dissertation supervisor. The external examiner and second marker may access the submitted thesis. There is no industrial partner and no other party will be given access to the research data.		
21	List who will have control of, and act as custodian(s) for, data generated by the research activity:		
	The principal researcher (Smit Brijeshkumar Patel) will control and act as custodian for all data generated by the research activity.		
22	Give details of data storage arrangements, including security measures in place to protect the data, where data will be stored, how long for, and in what form.		
	All acquisition images, virtual device images, analysis files and thesis drafts will be stored on AES-256 encrypted, password-protected external storage media held securely by the principal researcher. Thesis drafts will additionally be held in the University's password-protected Office 365 storage. No unencrypted copies will be made. SHA-256 hash values will be recorded for all acquisition images at the point of creation. Data will be retained until the completion and assessment of the project, after which all storage media will be securely reformatted and the handset used as a test device will be factory reset.		
22	Confirm that you have read the UWTSD guidance on data management (see https://www.uwtسد.ac.uk/library/research-data-management/)	☒	
23	Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding	☒	

SECTION I: Use of AI tools

ETHICS FORM – COMPUTING STUDENTS ONLY

Use of generative AI and other AI-based tools There are a number of ethical issues relating to the use of generative AI and other AI-based tools, including data security, output bias, and output errors. In general you should assume that any generative AI or other AI-based tool that you pay to use is more secure and accurate than one which is free to use.		YES	NO	N/A
Will the research use AI tools to do any of the following:				
1	Capture data?	☐	☒	☐
2	Generate and/or edit text?	☐	☒	☐
3	Generate graphics?	☐	☒	☐
4	Generate video?	☐	☒	☐
5	Generate sound/music?	☐	☒	☐
6	Generate code?	☐	☒	☐
7	Generate synthetic data?	☐	☒	☐
8	Analyse data?	☐	☒	☐
9	Analyse personal or sensitive data?	☐	☒	☐
10	Classify data?	☐	☒	☐
11	Do you intend to use the free version of any AI tools?	☐	☒	☐
If you have answered YES to any of questions O1-O11, please provide justification detailing why this is necessary for the research.				
12	N/A – NO has been answered to all of questions 1 to 11, so no justification is required.			

SECTION J: Declaration

	The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants. In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/		
1	Signature of applicant:	Smit Brijeshkumar Patel	Date: 5 th August 2026
2	Supervisor:	Ramzi Djemai	Date: 5 th August 2026
3	Signature:	Ramzi Djemai	