

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:	Khadija Banu
2	Student Number:	2527944
3	Email address:	2527944@student.uwstd.ac.uk
4	Programme of Study:	MSc in Cyber Security and Digital Forensics
5	Supervisor:	

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		Yes
2	UWTSD Research Data Management Policy		Yes
3	IEC 62443 / ISA-IEC 62443 standards		Yes
4	GDPR and Data Protection Act 2018		Yes

SECTION C: Details of Research Activity

1	Indicative title:	Forensic Readiness for Critical National Infrastructure During Cyberwarfare: Evaluating Logging and Evidence Collection Gaps.		
2	Proposed start date:	September 2026	Proposed end date:	February 2027
	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:			

ETHICS FORM – COMPUTING STUDENTS ONLY

	● <i>Purpose of Research Activity: The purpose of this research is to investigate the challenges of collecting reliable digital evidence from multi-tenant cloud computing environments. Traditional digital forensic methods often depend on physical access to storage devices, whereas cloud environments use virtualised and shared infrastructure. This creates challenges relating to evidence volatility, data isolation, privacy and chain of custody.</i> ● <i>Proposed Research Question: How can an automated API-based forensic acquisition methodology improve the speed, integrity and tenant isolation of digital evidence acquisition in multi-tenant cloud computing environments?</i> ● <i>Aims of Research Activity: To examine the technical challenges associated with digital forensic evidence acquisition in multi-tenant cloud environments.</i> ● <i>To investigate the limitations of cloud provider management-plane APIs and cloud logging mechanisms for forensic evidence collection.</i> ● <i>To design an automated API-based forensic acquisition methodology that supports evidence preservation while maintaining tenant isolation.</i> ● <i>Objectives of Research Activity: Analyse the effects of resource pooling, dynamic provisioning, virtualisation and data remanence on conventional forensic acquisition.</i> ● <i>Examine CSP management-plane logging, including AWS CloudTrail and Azure Activity Logs, and assess their usefulness as forensic evidence.</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 The purpose of this research is to investigate deficiencies in logging and digital evidence collection within Critical National Infrastructure (CNI), particularly Operational Technology (OT) and Industrial Control Systems (ICS), during simulated cyberwarfare scenarios. The study will examine whether conventional IT-focused forensic techniques are suitable for OT/ICS environments where availability, safety and low latency are critical. The research will use a controlled Hardware-in-the-Loop (HITL) laboratory environment to simulate cyberwarfare activity without interacting with real critical infrastructure. The study will examine the loss of volatile forensic evidence, the effect of active forensic extraction on network latency and controller availability, and the effectiveness of passive evidence collection using out-of-band network tapping. The research aims to develop and evaluate a tool-independent forensic readiness framework that can improve evidence preservation while minimising disruption to OT/ICS operations. The study addresses an important gap identified in existing research, particularly the difficulty of collecting legally useful evidence from PLC and SCADA environments without negatively affecting their operation. (this box should expand as you type)
4	Research Question How can forensic readiness and evidence collection be improved in Critical National Infrastructure OT/ICS environments during simulated cyberwarfare while minimising the impact on system availability and network latency? (this box should expand as you type)
5	Aims of Research Activity Number your aims and link them to your objectives Aim 1: To assess the logging and evidence-gathering deficiencies of PLC and SCADA systems in simulated cyberwarfare scenarios. Aim 2: To evaluate the limitations of conventional IT-based forensic and incident-response techniques when applied to OT/ICS environments. Aim 3: To measure the effects of forensic extraction techniques on evidence acquisition, network latency and controller availability. Aim 4: To develop and evaluate a passive, tool-independent forensic readiness framework using out-of-band network tapping and telemetry collection.

ETHICS FORM – COMPUTING STUDENTS ONLY

	(this box should expand as you type)
6	Objectives of Research Activity Objective 1: Assess the logging capabilities of commercial PLC and SCADA systems and identify at least three evidence-gathering shortcomings associated with volatile memory. Objective 2: Compare at least three incident-response methodologies used for hybrid IT/OT/ICS environments. Objective 3: Measure the operational limitations of conventional IT-based forensic triage techniques by assessing CPU usage, network latency and controller availability. Objective 4: Develop and test a passive forensic-readiness methodology based on out-of-band network tapping and local telemetry aggregation. Objective 5: Test the evidence-capturing capability of the proposed approach against simulated Modbus logic-overwrite attacks in the controlled laboratory environment. (this box should expand as you type)
	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	Data will be collected exclusively within a controlled and physically isolated IT/OT/ICS laboratory environment using a Hardware-in-the-Loop (HITL) testbed. No real Critical National Infrastructure, public infrastructure or live production environment will be used. The experiment will involve industrial controllers, a SCADA/HMI environment and simulated enterprise-network components. A simulated cyberwarfare scenario will be used to generate controlled Modbus logic-overwrite activity against the laboratory PLCs. The purpose is to reproduce the forensic ephemerality problem in a safe environment. Data will be collected using passive out-of-band hardware network taps to capture network traffic in PCAP format. Volatile memory dumps will also be collected from the laboratory PLCs following the simulated incident. Existing IT-focused forensic extraction techniques will be tested for comparison. Wireshark will be used to analyse captured network traffic, including relevant Modbus/DNP3 traffic. KAPE will be used to benchmark conventional IT-centric forensic artifact collection. Python-based tools and libraries, including Pandas and Scikit-Learn, will be used for quantitative analysis of the collected telemetry and experimental results. The principal measurements will include the quantity of forensic evidence successfully acquired, network latency measured in milliseconds, and controller availability. Results from active forensic extraction will be compared with results obtained through passive network tapping and telemetry collection. All data will be artificially generated within the laboratory testbed. No personal participant data, real organisational data or operational CNI data will be collected. (this box should expand as you type)

SECTION D: Scope of Research Activity

Will the research activity include:	YES	NO
--	------------	-----------

ETHICS FORM – COMPUTING STUDENTS ONLY

1	Use of a questionnaire or similar research instrument?	☐	No
2	Use of interviews?	☐	No
3	Use of focus groups?	☐	No
4	Use of participant diaries?	☐	No
5	Use of video or audio recording?	☐	No
6	Use of computer-generated log files?	Yes	☐
7	Participant observation with their knowledge?	☐	No
8	Participant observation without their knowledge?	☐	No
9	Access to personal or confidential information without the participants' specific consent?	☐	No
10	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	No
11	Performance of any acts which may cause embarrassment or affect self-esteem?	☐	No
12	Investigation of participants involved in illegal activities?	☐	No
13	Use of procedures that involve deception?	☐	No
14	Administration of any substance, agent or placebo?	☐	No
15	Working with live vertebrate animals?	☐	No
16	Procedures that may have a negative impact on the environment?	☐	No
17	Other primary data collection methods. Please indicate the type of data collection method(s) below.	Yes	☐
	Controlled experimental data will be collected from a physically isolated IT/OT/ICS laboratory testbed. The research will generate simulated cyberwarfare traffic and Modbus logic-overwrite activity within the test environment. Data will include PCAP network captures, PLC volatile memory dumps, telemetry logs, network latency measurements and controller availability measurements. No data will be collected from real CNI infrastructure or human participants.		

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?	☐	No
2	Adults (over the age of 18 and competent to give consent)?	☐	No
3	Vulnerable adults?	☐	No
4	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	☐	No
5	Prisoners?	☐	No
6	Young offenders?	☐	No

ETHICS FORM – COMPUTING STUDENTS ONLY

7	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	No
8	People engaged in illegal activities?	☐	No
9	Others. Please indicate the participants below, and specifically any group who may be unable to give consent.	☐	No
	Details of any other participant groups: Complete this only if your participants cannot give consent. This includes animals (this box should expand as you type)		

	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?	Ballpark figures are fine, but make sure that you explain how you will identify and contact your participants. 0
11	Who will the participants be?	N/A – no human participants are involved.
12	How will you identify the participants?	N/A – no human participants are involved.

	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?	☐	☐	N/A
14	Will you tell participants that their participation is voluntary?	☐	☐	N/A
15	Will you obtain written consent for participation?	☐	☐	N/A
16	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	N/A
17	If the research is observational, will you ask participants for their consent to being observed?	☐	☐	N/A
18	Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	N/A
19	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	N/A
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?	☐	☐	N/A
21	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	N/A
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 – the research does not involve human participants. All experimental data will be generated within a controlled laboratory testbed.			

	Information for participants:	YES	NO	N/A
24	Will participants be paid?	☐	No	☐
25	Is specialist electrical or other equipment to be used with participants?	☐	No	☐
26	Are there any financial or other interests to the investigator or University arising from this study?	☐	No	☐
27	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	No	☐

ETHICS FORM – COMPUTING STUDENTS ONLY

28	If YES to any question, please provide full details
	N/A – no human participants are involved and therefore no participant payment, participant equipment, deception or participant-related financial interests apply. <i>(this box should expand as you type)</i>

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: N/A – no human participants are involved in the research. <i>(this box should expand as you type)</i>	How you will mitigate the risk to participants: N/A – no human participants are involved.
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	
	The research does not involve human participants or the collection of sensitive personal information. Although the study simulates cyberwarfare techniques and intentionally exploits vulnerabilities within industrial control systems, all activities will take place within a restricted, physically isolated laboratory environment. No real-world CNI systems, public networks or operational infrastructure will be targeted. The simulated malicious activity will be limited to the authorised laboratory testbed. <i>(this box should expand as you type)</i>	
3	Risks to the investigator For example: personal health & safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest	
	Risk to the investigator: The principal risks to the investigator relate to the controlled use of cyberattack simulation techniques, industrial control hardware and forensic tools. There is a potential risk of accidental misconfiguration, unintended system disruption, loss or corruption of experimental data, or accidental connection of the test environment to an external network. <i>(this box should expand as you type)</i>	How you will mitigate the risk to the investigator: All experiments will be conducted in a physically isolated IT/OT/ICS laboratory environment with no Internet connection. The research will use fabricated testbed data rather than real CNI data. Experimental activities will be conducted only on authorised laboratory equipment. Systems will be configured and tested before experimentation, and appropriate laboratory procedures and supervision will be followed. The simulated malicious activity will remain confined to the test environment.
4	University/institutional risks For example: adverse publicity, financial loss, data protection	
	Risk to the University: The main institutional risks are potential damage to laboratory equipment, disruption to university network infrastructure if the test environment were incorrectly connected, data-security issues, and reputational risk associated with the use of simulated cyberattack techniques.	How you will mitigate the risk to the University: The experiment will be performed exclusively within a physically isolated laboratory LAN with no connection to the Internet or operational university networks. Only fabricated experimental data will be used. Access to the laboratory and research data will be restricted to authorised personnel. Cyberattack simulations

ETHICS FORM – COMPUTING STUDENTS ONLY

		will be limited to the controlled testbed and will not target external systems or real infrastructure. The research will follow university ethical, data-management and information-security requirements.
5	Environmental risks For example: accidental spillage of pollutants, damage to local ecosystems	
	Risk to the environment: The research is not expected to create significant environmental risks. The main potential environmental risk would be accidental damage to laboratory hardware resulting in electronic waste.	<i>How you will mitigate the risk to environment:</i> The research will use existing laboratory equipment and controlled experimental procedures. Equipment will be operated within manufacturer and laboratory safety requirements. No hazardous substances, biological materials or environmental pollutants will be used. The experiment will be conducted in an indoor laboratory environment.

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 – the research does not involve human participants. No participant debriefing or feedback is therefore 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 – no human participants are involved in the research. All experimental data will be generated from an authorised and controlled IT/OT/ICS laboratory testbed.
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. No personal participant information will be collected because the study does not involve human participants. Experimental data will be generated within the laboratory testbed and will relate to simulated network traffic, PLC activity, PCAP files, telemetry and volatile memory dumps. Research data will be restricted to authorised members of the research team and will not contain personal participant information. Any potentially sensitive laboratory or institutional information will be treated as confidential and will not be included in the final research outputs without appropriate permission.

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
---	------------	-----------

ETHICS FORM – COMPUTING STUDENTS ONLY

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.	☐	No
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. N/A. The research will use synthetic forensic data generated within an isolated testbed. The intended research data will consist of synthetic volume snapshots, synthetic memory dumps and computer-generated cloud/API logs.		
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),	Yes	No
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. <i>(this box should expand as you type)</i>		

	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)?	☐	No
6	University computers?	Yes	☐
7	Private company computers?	☐	No
8	Home or other personal computers?		No
9	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?		No
10	“Cloud” storage or websites?	Yes	☐
11	Other – specify:	☐	No
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: If possible, save your data on computers that are secure and regularly backed up. Many cloud services only provide GDPR-compliant storage for business customers. An example of suitable text is given below. <i>All data will be kept in password protected cloud storage on the University Office 365 system which</i>		

ETHICS FORM – COMPUTING STUDENTS ONLY

	<i>will not be shared. Audio/visual data will be transcribed and would be shown to participants to check accuracy of reporting. Any USB sticks used to store or transfer data will be password protected. All participants will be given a unique identifier to ensure confidentiality and this list will be kept securely in the password protected folder.</i> All research data will be stored securely using University-approved storage facilities. Where University Office 365 is used, data will be stored in a password-protected University account and will not be publicly shared. Access will be restricted to authorised individuals involved in the research. Experimental data will consist primarily of fabricated laboratory data, including PCAP files, telemetry logs and volatile memory dumps. Research files will be backed up using approved University storage procedures. Where data is transferred between authorised systems, appropriate security measures will be used. Any temporary copies of research data will be securely removed when no longer required. The research data will be retained until completion of the project and then securely deleted in accordance with University data-management requirements.
--	--

Data Protection			
	Will the research activity involve any of the following activities:	YES	NO
13	Electronic transfer of data in any form?	Yes	☐
14	Sharing of data with others at the University outside of the immediate research team?	☐	No
15	Sharing of data with other organisations?	☐	No
16	Export of data outside the UK or importing of data from outside the UK?	☐	No
17	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	No
18	Publication of data that might allow identification of individuals?	☐	No
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): <i>This includes data such as drafts of your thesis as well as experimental or survey data. An example of suitable text is given below.</i> <i>All data will be encrypted and 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 data transfers will be encrypted and password protected. All participants will be given a unique identifier to ensure confidentiality and this list will be kept securely in the password protected folder. The data will be stored until the completion of the project and then deleted. In accordance with the DPA2018, participants will have the right to ask to see what data is held relating to them, and this data will be deleted immediately if the participant requests this, in which case the data will not be used in the project.</i> Electronic transfer of research files may be required between authorised University systems used for the project. Any such transfer will be conducted using University-approved and appropriately secured systems. Research data will not be shared with external organisations and will not intentionally contain personal data. Data will be access-controlled and stored securely. No information identifying individuals will be published as part of the research.		
20	List all who will have access to the data generated by the research activity:		
	<i>Normally the principal researcher, possibly also the supervisor and, if the project has an industrial partner, a representative of that partner. Possibly also external examiner or second marker?</i> The principal researcher will have access to the research data. The research supervisor may also have access where required for supervision, assessment, verification or research governance purposes. Access will be limited to authorised individuals. <i>(this box should expand as you type)</i>		

ETHICS FORM – COMPUTING STUDENTS ONLY

21	List who will have control of, and act as custodian(s) for, data generated by the research activity:	
	Usually the principal researcher. The principal researcher will act as the primary custodian of the research data, subject to the University's research data-management requirements and the oversight of the research supervisor. <i>(this box should expand as you type)</i>	
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. <i>All data will be encrypted and 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, and will be reformatted at the end of the project in order to destroy the data. The data will be stored until the completion of the project and then deleted.</i> Research data will be stored securely using University-approved storage facilities, including University Office 365 where applicable. Data will be protected using account authentication and password controls, with access restricted to authorised individuals. The research data will consist primarily of fabricated laboratory data such as PCAP files, telemetry logs and volatile memory dumps. No research data will be intentionally stored on publicly accessible systems. Any temporary copies created during the analysis will be securely removed when no longer required. Research data will be retained until completion of the research project and then securely deleted in accordance with University data-management requirements. <i>(this box should expand as you type)</i>	
22	Confirm that you have read the UWTSD guidance on data management (see https://www.uwtسد.ac.uk/library/research-data-management/)	Yes
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	Yes

SECTION I: Use of AI tools

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.				
Will the research use AI tools to do any of the following:		YES	NO	N/A
1	Capture data?	☒	No	☐
2	Generate and/or edit text?	☐	No	☐
3	Generate graphics?	☐	No	☐
4	Generate video?	☐	No	☐
5	Generate sound/music?	☐	No	☐
6	Generate code?	☐	No	☐
7	Generate synthetic data?	☐	No	☐
8	Analyse data?	☐	No	☐
9	Analyse personal or sensitive data?	☐	No	☐
10	Classify data?	☐	No	☐

ETHICS FORM – COMPUTING STUDENTS ONLY

11	Do you intend to use the free version of any AI tools?		No	☐
If you have answered YES to any of questions O1-O11, please provide justification detailing why this is necessary for the research.				
12	State which AI tool or tools you will be using, and where they are based (or store their data – you may need to check their webpages or user agreement for this). If you are planning to use Copilot then say if you're using the UWTSD version of it or the public version. You should also show how you are complying with current UWTSD guidance/policy of the use of AI. N/A – no generative AI or other AI-based tools will be used as part of the research data collection, generation, analysis or classification process. The research will use conventional forensic and analytical tools, including KAPE, Wireshark, Python, Pandas and Scikit-Learn, as specified in the research methodology.			

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.uwtss.ac.uk/research/research-ethics/		
1	Signature of applicant:	Khadija Banu	Date: 09-08-2026
2	Supervisor:		Date:
3	Signature:		