Softwarica

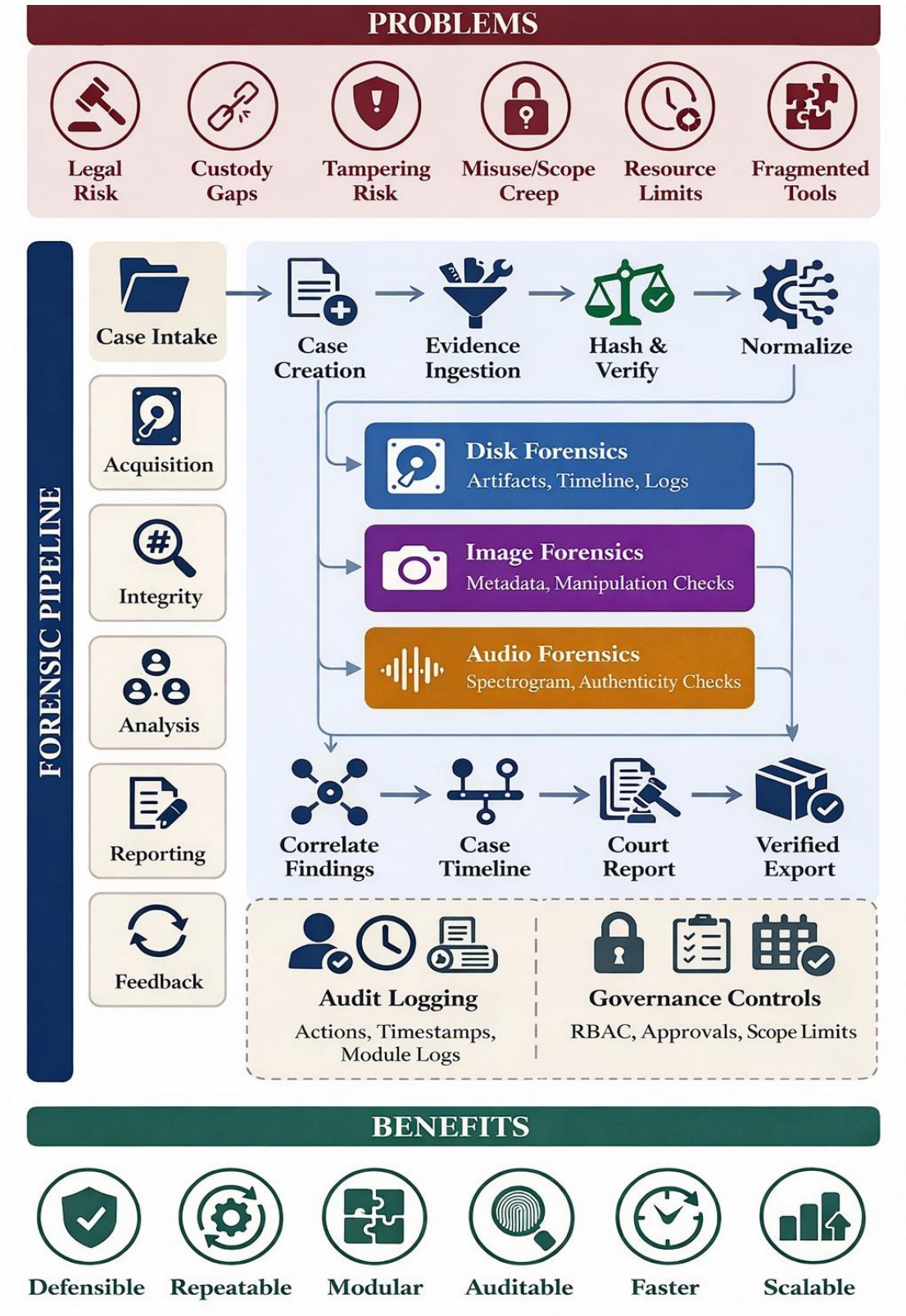
COLLEGE OF IT & E-COMMERCE

Design and Implementation of an Ethical Hacking-Based Digital Forensic Tool for Proactive Cyber Threat Investigation and Evidence Analysis in Nepal Police Operations

Submitted By:
Aswin Paudel

Submitted To:
Manoj Shrestha

Conceptual Diagram



Ethical Approval Certificate

Risk Research Ethics Approval

Project Title

Design and Implementation of an Ethical Hacking-Based Digital Forensic Tool for Proactive Cyber Threat Investigation and Evidence Analysis in Nepal Police Operations

Record of Approval

Principal Investigator

I request an ethics peer review and confirm that I have answered all relevant questions in this checklist honestly.	×
I confirm that I will carry out the project in the ways described in this checklist. I will immediately suspend research and request new ethical approval if the project subsequently changes the information I have given in this checklist.	×
I confirm that I, and all members of my research team (if any), have read and agreed to abide by the Code of Research Ethics issued by the relevant national learned society.	×
I confirm that I, and all members of my research team (if any), have read and agreed to abide by the University's Research Ethics, Governance and Integrity Framework.	×
I understand that I cannot begin my research until this ethics application has been approved.	×

Name: Aswin Paudel

Date:

Student's Supervisor (if applicable)

I have read this checklist and confirm that it covers all the ethical issues raised by this project fully and frankly.I also confirm that these issues have been discussed with the student and will continue to be reviewed in the course of supervision.

Name: Manoj Shrestha

Date:

Reviewer (if applicable)

Date of approval by anonymous reviewer: -

Acknowledgement

I would like to express my sincere gratitude to Softwarica College of IT and E-Commerce, in collaboration with Coventry University, for providing the academic environment, resources, and guidance necessary to undertake and complete this thesis. The support offered through the programme has been instrumental in shaping my research capabilities and strengthening my understanding of professional and ethical practice in cybersecurity and digital forensics.

I am especially thankful to my supervisor, Mr. Manoj Shrestha, for his consistent guidance, insightful feedback, and encouragement throughout the research process. His expertise, constructive direction, and patience significantly contributed to refining the scope of the study and improving the quality of this work.

I also extend my heartfelt appreciation to my family and friends for their continuous motivation, understanding, and support during this journey. Finally, I would like to acknowledge everyone who supported me directly or indirectly in completing this research. Their contributions, whether academic, technical, or personal, have played an important role in the successful completion of this thesis.

Abstract

Cybercrime investigations increasingly depend on timely and defensible analysis of digital devices and online artifacts. In many law-enforcement contexts, including Nepal, investigations frequently involve heterogeneous evidence such as storage media, images, and audio recordings, yet operational practice often relies on fragmented tools, manual workflows, and reactive evidence collection. These limitations can delay case progression, reduce consistency between investigators, and weaken evidential defensibility particularly when adversaries employ encryption, anti-forensic techniques, and manipulate multimedia. This study proposes an integrated digital forensic tool designed to strengthen investigation capability through standardized evidence intake, automated analysis, and audit-ready reporting. The proposed framework consolidates disk, image, and audio forensic modules within a single workflow that emphasizes evidence integrity via cryptographic hashing, structured metadata capture, chain-of-custody management, and tamper-evident audit logs. In addition, controlled ethical hacking–inspired procedures are incorporated as bounded, hypothesis-driven investigative actions intended to support targeted acquisition and validation without compromising legal and ethical requirements. The study highlights how normalization of outputs and cross-evidence correlation can improve event reconstruction and reduce duplication across tools while producing court-oriented reports that document methods, provenance, and key findings. Overall, the research contributes an academically grounded, governance-centric approach to digital forensics, demonstrating how integration, automation, and enforceable accountability controls can improve investigative efficiency and strengthen the reliability and admissibility of digital evidence in cybercrime cases.

Keywords


techniques
audio
across
cybercrime
integrity
framework
research
digital
detection
security
threat
data
analysis
evidence
investigations
collection
nepal
cyber
automated
law
proactive
within
legal
tools
network
findings
capability
design
investigators
capabilities
forensic
ethical
tool
investigation
operational
forensics
investigative
technical
access
hacking
enforcement
systems

Table of Contents

List of Figure

List of Abbreviations

DFIR: Digital Forensics and Incident Response

GRR: Google Rapid Response

DFDC: Deepfake Detection Challenge

IDS/IPS: Intrusion Detection System / Intrusion Prevention System

RBAC: Role-Based Access Control

SHA-256: Secure Hash Algorithm 256-bit (hashing for integrity)

LSB/MSB: Least Significant Bit / Most Significant Bit

OCR: Optical Character Recognition

DTMF: Dual-Tone Multi-Frequency

SSTV: Slow-Scan Television

TAM: Technology Acceptance Model

UTAUT: Unified Theory of Acceptance and Use of Technology

INTRODUCTION

Nepal Police operations face an escalating tide of cybercrime that threatens public safety, national security, and the integrity of law enforcement worldwide. Globally, cyber threats have surged, with incidents such as ransomware attacks, data breaches, and state-sponsored espionage costing economies trillions annually and undermining critical infrastructure. In Nepal, this crisis manifests acutely through rising cases of financial fraud, online frauds, and cyber-enabled organized crime, exacerbated by rapid digital adoption amid limited regulatory oversight. These threats not only erode public trust in institutions but also strain under-resourced police forces, compelling a shift from traditional policing to sophisticated cyber investigations.

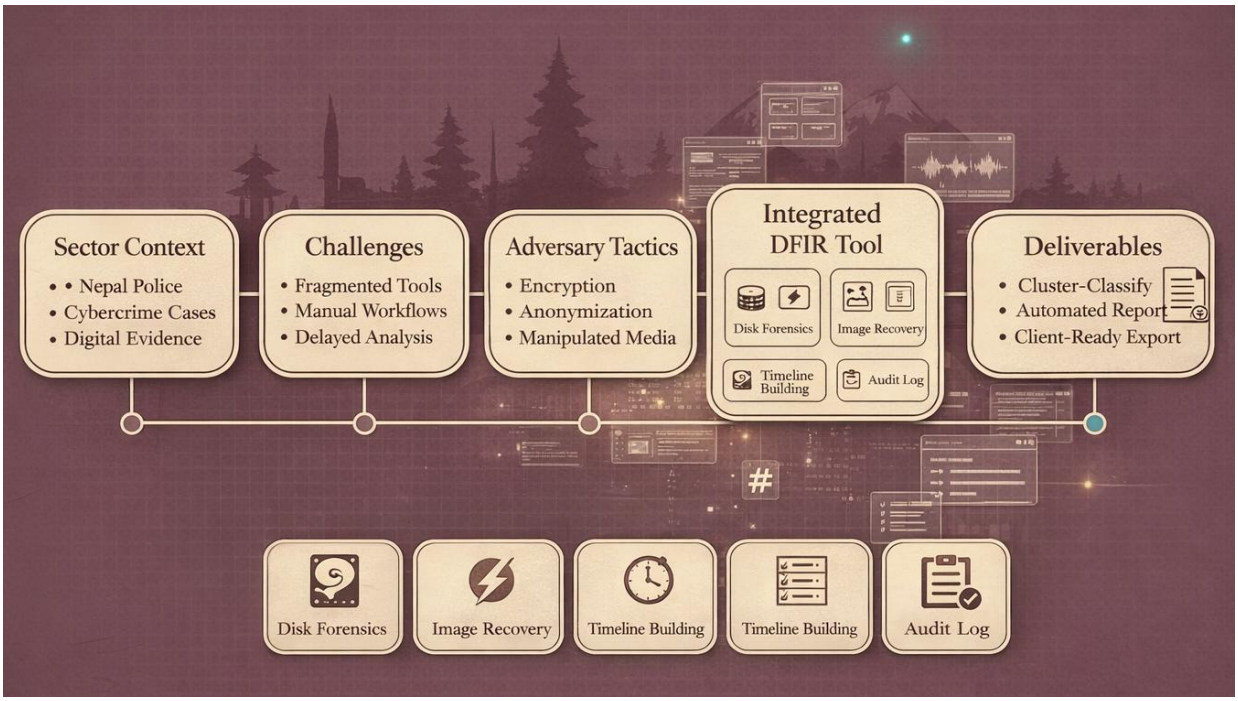


Figure 1: Nepal Cybercrime Investigation Overview

The cybersecurity threat landscape in Nepal has witnessed dramatic evolution over the past decade, mirroring global trends while simultaneously exhibiting unique characteristics shaped by local socio-economic and technological conditions. The widespread adoption of mobile banking, e-commerce platforms, and social media networks has created new vectors for criminal exploitation, with cybercriminals increasingly targeting vulnerable populations through phishing schemes, online frauds, and digital extortion. The COVID-19 pandemic further accelerated digital transformation across governmental and private sectors, inadvertently expanding the attack surface available to malicious actors. According to reports from the Nepal Telecommunications Authority and various cybersecurity incidents documented by national media, Nepal has experienced a significant surge in cyber-enabled crimes, including unauthorized access to banking systems, data breaches affecting government databases, and sophisticated social engineering attacks targeting

both individuals and organizations. However, the actual scale of cybercrime in Nepal remains difficult to quantify accurately due to widespread underreporting, limited awareness among victims, and insufficient mechanisms for systematic data collection and analysis. This ambiguity in threat assessment poses significant challenges for law enforcement agencies attempting to allocate resources effectively and develop evidence-based intervention strategies.

Traditional approaches to digital forensics within law enforcement contexts have operated on a reactive paradigm, wherein investigative activities commence only after a cybercrime incident has been reported and initial victimization has occurred. This post-incident response model, while essential for evidence collection and perpetrator identification, inherently limits the scope for proactive threat intelligence, early warning mechanisms, and preventive intervention strategies. Conventional digital forensic workflows typically involve the seizure of digital devices, creation of forensic images, analysis of stored data, and reconstruction of user activities through examination of file systems, registry entries, and application artifacts. While these methodologies remain foundational to digital investigations, they are increasingly insufficient in addressing contemporary cyber threats characterized by sophisticated anti-forensic techniques, encryption technologies, ephemeral communication platforms, and cloud-based data storage that complicates evidence acquisition. Furthermore, the reactive nature of traditional forensics creates temporal delays between incident occurrence and investigative response, during which critical evidence may be destroyed, modified, or rendered inaccessible through remote wiping capabilities or automated data deletion mechanisms. For Nepal Police, these limitations are particularly acute given resource constraints that restrict the number of cases that can be thoroughly investigated, often forcing investigators to prioritize high-profile incidents while less visible but equally harmful cybercrimes receive inadequate attention.

Problem Context and Motivation

Nepal Police cyber investigation units currently operate within a fragmented technological ecosystem that significantly undermines their capacity to respond effectively to the escalating wave of digital crimes. Investigators are forced to navigate multiple disparate forensic tools, each serving isolated functions such as mobile device analysis, network traffic examination, or disk imaging, without any meaningful integration or unified data management capability. This tool fragmentation creates operational bottlenecks where critical time is lost in manual data correlation across platforms, evidence integrity risks emerge from repeated data transfers between systems, and investigative efficiency suffers as officers struggle to maintain parallel documentation streams for chain of custody requirements. The absence of automation in routine forensic tasks means that even straightforward cases demand disproportionate time investments, while complex investigations involving encrypted data or sophisticated anti-forensic techniques often exceed the technical capabilities available to most investigators.

Figure 2: Current Gaps in Investigation

The reactive nature of current investigative approaches further compounds these challenges, as digital forensics activities commence only after cybercrime incidents are reported, often when critical volatile evidence has already been lost or destroyed. Traditional post-incident analysis methodologies provide no mechanism for proactive threat detection, early warning systems, or preventive intervention capabilities that could disrupt criminal operations before widespread victimization occurs. When investigators finally gain access to digital evidence, they frequently encounter encrypted storage, deleted files, and timestamp manipulation tactics employed by increasingly sophisticated cybercriminals who understand forensic procedures and actively work to undermine evidence collection efforts.

Figure 3: Key Investigation Challenges

The compounding effects of limited resources, inconsistent procedural standards, and inadequate tools create evidentiary vulnerabilities that jeopardize prosecutions even when technical investigations yield valuable findings. Defense attorneys increasingly exploit procedural gaps in chain of custody documentation, challenge the reliability of findings produced by non-standardized analytical methods, and question the qualifications of investigators using unfamiliar forensic tools. This situation demands an integrated solution that combines proactive ethical hacking capabilities with rigorous forensic protocols, automated workflow management, and comprehensive evidence tracking within a unified framework specifically designed for Nepal Police operational constraints and investigative priorities.

Cybersecurity Theories and Behavioral Factors in Security Decision-Making

Behavioral foundations for security decisions in digital investigations

Cybersecurity performance is inseparable from human decision-making because security controls ultimately depend on whether people apply them correctly, consistently, and at the right time. This human element becomes even more consequential in digital investigations, where procedural decisions (such as how evidence is collected, recorded, examined, and reported) influence both investigative outcomes and evidentiary defensibility. The digital forensics process is often described as progressing through phases that include collection, examination, analysis, and reporting each phase requiring judgment about what to capture, which tools and procedures to use, and how to document actions (Dang, 2006).

In law-enforcement settings, decisions about digital evidence handling are constrained by legal requirements and professional best practices designed to protect integrity and transparency. Evidence-handling standards emphasize that digital evidence must be identified, collected, acquired, and preserved in ways that maintain evidential value, reduce contamination risk, and support accountability in court. At the process level, incident investigation guidance includes preparation and end-to-end investigation flow models intended to support consistent actions across teams and cases. Similarly, digital evidence best-practice guidance stresses documentation and chain-of-custody continuity, reflecting the principle that evidentiary strength depends not only on technical findings but also on the credibility and traceability of the method used to obtain them (Swgde).

Within this context, behavioral theories are not an abstract add-on; they directly explain why security procedures are followed rigorously in some cases but bypassed in others. They also guide how forensic workflows should be designed so that correct actions are easier to perform than incorrect ones, and so that accountability controls discourage misuse without creating counterproductive friction.

Threat- and coping-appraisal theories for protective action

One of the strongest explanatory families for cybersecurity behavior is based on how people perceive threats and evaluate their ability to cope. Protection Motivation Theory describes protective behavior as emerging from cognitive appraisal processes in which individuals evaluate the seriousness of a threat, their vulnerability to it, and whether recommended responses are effective and feasible. In cybersecurity research, this framework is widely used to explain why people comply with policies, adopt protective controls, and respond to warnings, with particular attention to constructions such as severity, vulnerability, response efficacy, self-efficacy, and response costs. The value of this theory for a forensic or investigation workflow is practical: if investigators perceive evidence-integrity failure (or procedural mistakes) as likely and severe and simultaneously believe that correct procedures are effective and manageable they will be more motivated to comply consistently (Liu, 2021).

A closely related model with direct cybersecurity relevance is Technology Threat Avoidance Theory. It explains why users avoid malicious or risky IT by describing a dynamic process in which threat appraisal leads to coping appraisal. In this model, perceived susceptibility and severity drive threat perception, and the coping response depends on beliefs about safeguard effectiveness, safeguard costs, and self-efficacy; if individuals believe safeguards cannot sufficiently mitigate the threat, they may shift toward emotion-focused coping rather than effective protective action. For investigation environments, this distinction matters because high-stress or low-control conditions can shift behavior away from careful, methodical procedure toward coping shortcuts (for example, skipping documentation because it feels "too slow," or relying on incomplete analysis because deeper steps seem infeasible). This theory therefore supports designing investigative platforms that reduce perceived effort, clarify how each step improves outcomes, and strengthen the user's confidence that they can complete the workflow successfully under real constraints.

Technology adoption and workflow integration in forensic environments

Technology acceptance theories explain why forensic tools are adopted or rejected in operational environments. The Technology Acceptance Model demonstrates that perceived usefulness and ease of use drive adoption, with usefulness whether investigators believe the platform improves case outcomes being the stronger predictor, while ease of use reduces cognitive burden and influences adoption indirectly. The Unified Theory of Acceptance and Use of Technology consolidate multiple acceptance models, showing that adoption depends not only on interface design but also on organizational facilitation (training, support, infrastructure), social influence, and role expectations, with these factors varying across user groups and contexts. Research applying acceptance models to policing reveals that information quality and timeliness become central drivers alongside standard usability measures, meaning forensic platforms must deliver

outputs that are not only correct but also operationally usable: timely, clearly presented, and reliably traceable to underlying evidence and methods (Davis).

Diffusion of Innovations theory adds that new tools spread more readily when they provide relative advantage over existing approaches, compatibility with current workflows, opportunities for trial, and observable benefits, while minimizing complexity. In law-enforcement contexts, this supports deployment strategies that allow practitioners to build confidence incrementally rather than requiring immediate institutional-scale adoption. Practical implications include phased rollouts, pilot units, and modular implementation that enable early adopters to demonstrate benefits, gather feedback, and refine workflows before broader scaling. Together, these theories emphasize that successful forensic platform adoption requires not just technical capability, but deliberate attention to perceived value, operational fit, organizational support, and gradual diffusion mechanisms that align with how practitioners evaluate and integrate new tools under real investigative constraints.

GOVERNANCE, ETHICS, AND ORGANIZATIONAL CONTEXT

Security decision-making is shaped by governance mechanisms that define permitted actions and consequences for noncompliance. Deterrence theory, widely applied to information security policy enforcement, shows that formal sanctions typically have weak-to-moderate effects, while informal deterrence such as perceived enforcement likelihood, social accountability, and cultural norms often proves more influential. Awareness of security countermeasures, monitoring practices, and education programs strengthen perceived sanction certainty and severity, reducing misuse intentions. For forensic platforms, this supports embedding tamper-evident audit mechanisms and transparent logging as behavioral interventions that strengthen accountability and discourage procedural violations. However, deterrence alone is insufficient because individuals often rationalize policy violations through neutralization techniques such as denying responsibility, injury, or victims, condemning enforcers, or appealing to higher loyalties allowing them to preserve self-image while deviating from required procedures (Swgde).

At the organizational level, security culture theory emphasizes that shared assumptions, values, and habitual practices determine whether secure behavior becomes normalized, with culture reflected through repeated employee behavior guided by leadership and operationalized in daily system interactions. Institutional theory adds that organizations respond to coercive pressures (regulations), normative pressures (professional expectations), and mimetic pressures (peer benchmarking), which collectively drive compliance with security standards. Together, these perspectives indicate that effective governance requires combining enforceable controls such as roles, approvals, and auditability with cultural reinforcement through training, leadership emphasis, peer review, and consistent practice, rather than assuming compliance emerges automatically from written policies. In law-enforcement contexts, this approach is essential for preventing "procedural drift," where shortcuts become normalized and rationalized as operational necessity unless governance and culture consistently uphold standards (Vance, 2010).

COGNITIVE BIASES, FATIGUE, AND DECISION QUALITY IN FORENSIC ANALYSIS

Security decision-making is constrained by cognitive limitations that are especially high stakes in digital forensics, where errors can contribute to investigative failure or miscarriage of justice. Research reveals that cognitive bias and human error have received insufficient attention in digital forensics despite clear risks across the investigative process. Controlled studies demonstrate that examiners' observations can be biased by contextual information, and reliability across examiners is often low for observations, interpretations, and conclusions, indicating systematic need for bias mitigation measures. This evidence supports designing forensic tools that go beyond artifact extraction to support disciplined reasoning, encouraging structured hypothesis testing, separating observation from interpretation, and implementing review mechanisms that reduce cognitive contamination. Automation introduces additional cognitive risks: while AI-assisted filtering increases speed and consistency, users may over-trust outputs or misunderstand uncertainty. Trust-in-automation research shows that reliance on complex systems is strongly shaped by interface design and feedback, meaning investigative tools must expose method provenance, confidence levels, and reproducible parameters so automation remains decision support rather than a substitute for expert judgment (Sunde, 2019).

Even well-designed controls fail when users become overloaded. Security fatigue research describes how repeated security demands produce weariness, resignation, and loss of control, increasing the likelihood that practitioners ignore guidance or default to insecure shortcuts. The "compliance budget" concept explains that individuals make cost-benefit judgments about compliance, with cumulative burden capping willingness to comply and placing limits on organizational security effectiveness unless compliance costs are actively managed. Behavioral security economics research further demonstrates that rejecting security advice can be rational from users' perspectives when recurring effort costs exceed perceived benefits, especially when threats feel uncertain or advantages seem speculative. In forensic environments, these findings justify workflow designs that minimize unnecessary decisions, automate low-risk documentation steps, reduce repetitive manual work, and maintain procedural consistency preventing investigators from being pushed into fatigue-driven shortcuts that undermine evidentiary integrity. Together, cognitive bias mitigation, appropriate automation calibration, and fatigue management form essential design principles for forensic platforms supporting reliable human judgment under operational pressure.

INTEGRATING THEORY INTO AN INVESTIGATION-READY PLATFORM DESIGN

Taken together, these theories converge on a socio-technical design principle: secure and defensible outcomes occur when institutions align governance, tooling, and training with predictable human behavior under operational constraints. Threat- and coping-appraisal theories imply that compliance increases when the perceived consequences of failure are clear, the effectiveness of procedures is credible, and the cost of correct action is low relative to shortcuts. In practical forensic workflow terms, this favors automation that reduces response costs (for example, automatic evidence labeling, hash generation, and audit-log capture) while simultaneously increasing self-efficacy through guided workflows and embedded explanations that show how each step supports integrity and admissibility.

Intention-based models and behavior-change frameworks imply that sustainable compliance depends on turning correct procedures into routines, supported by the environment rather than dependent on motivation alone. This supports implementation choices such as standardized case templates, mandatory minimum documentation fields aligned with evidence standards, and consistent prompts that reduce omission errors especially under time pressure.

Adoption models imply that even strong governance can fail if practitioners perceive tools as slow, confusing, or irrelevant to operational goals. The acceptance literature indicates that perceived usefulness and usability remain central, but policing-focused evidence suggests that timeliness and information quality can be decisive in technology adoption by officers, which is directly relevant to investigative tooling.

Diffusion theory reinforces that modular rollout, trialability, and visible benefits accelerate institutional uptake, which is important for organizations that must standardize practice across units with variable skill distribution and case volume.

Governance theories imply that accountability must be both enforceable and psychologically credible. Deterrence evidence supports monitoring and visibility of enforcement, but neutralization theory shows that rationalizations can undermine purely punitive systems unless organizations also address the narratives that justify shortcuts. Security culture and institutional pressure findings support strengthening leadership signaling, consistent supervisory review, and professionalization of procedures so that compliance becomes part of institutional identity rather than a "paperwork requirement."

Finally, digital forensics-specific research shows that decision quality is threatened by cognitive bias and inconsistency, including measurable biasing effects of contextual information and low inter-examiner reliability. This supports embedding bias-mitigation and quality measures into investigative workflows, such as structured separation of observation and interpretation, peer review checkpoints for high-stakes conclusions, and reporting formats that document methods and parameters in a reproducible way.

RESEARCH AIM

The primary aim of this thesis is to design and implement an integrated ethical hacking-based digital forensic framework that enhances Nepal Police's capacity for proactive cyber threat investigation, comprehensive evidence analysis, and legally admissible digital evidence management.

Figure 4: Aim

This involves:

- Collecting comprehensive digital evidence from multiple sources including mobile devices, computer systems, network traffic logs, memory dumps, and cloud-based storage through automated acquisition protocols that preserve forensic integrity
- Implementing ethical hacking methodologies and penetration testing capabilities to enable proactive vulnerability assessment, attack vector simulation, encrypted data recovery, and controlled system analysis within legally authorized investigative boundaries
- Developing automated forensic workflows that integrate mobile analysis, disk imaging, network forensics, malware examination, and timeline reconstruction within a unified platform featuring cryptographic evidence verification and chain of custody tracking
- Creating an intelligent evidence management system with role-based access controls, automated report generation conforming to legal standards, and user interfaces designed for investigators with varying technical expertise levels

- Evaluating framework effectiveness through comparative analysis against existing fragmented tool approaches, measuring improvements in investigation completion time, evidence recovery rates, procedural compliance, legal admissibility success, and investigator operational confidence

RESEARCH OBJECTIVES

Figure 5: Objectives

CONTRIBUTION AND SIGNIFICANCE

This research makes substantial contributions to both the theoretical understanding and practical implementation of digital forensic capabilities in resource-constrained law enforcement environments, with implications extending beyond Nepal to similarly situated developing nations. The primary contribution lies in the development of a contextualized forensic framework that explicitly addresses operational realities of developing countries policing limited budgets, heterogeneous skill distributions, fragmented tool ecosystems, and nascent legal frameworks for digital evidence rather than merely adapting tools designed for well-resourced Western law enforcement agencies. By integrating ethical hacking methodologies with traditional digital forensics within a unified platform, this research demonstrates how proactive investigation capabilities can be operationalized within legitimate law enforcement contexts while maintaining rigorous evidentiary standards and legal compliance. The framework's emphasis on automation, standardization, and progressive skill scaffolding represents a novel approach to democratizing advanced forensic capabilities, enabling investigators with intermediate technical proficiency to conduct complex analyses that previously required specialized expertise.

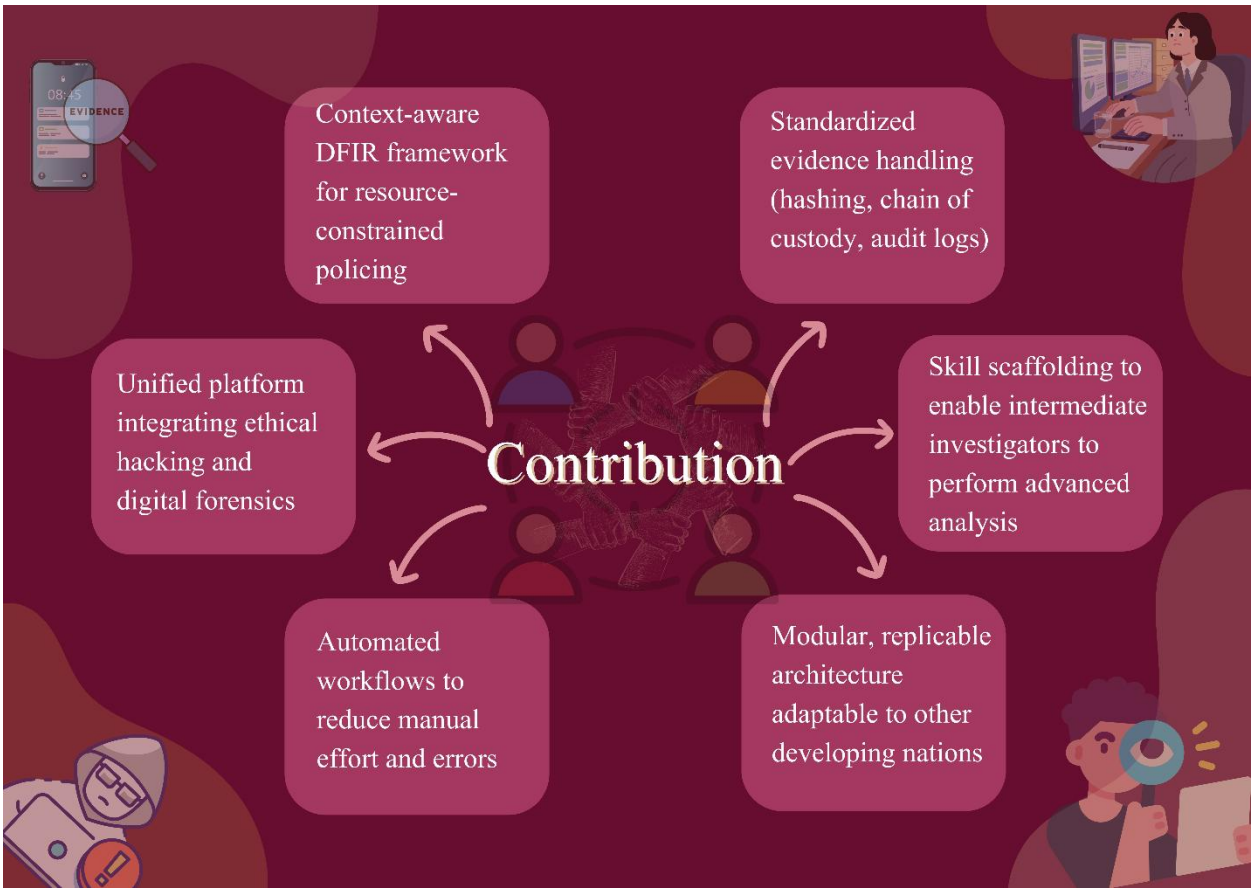


Figure 6: Contribution

The significance of this work extends to policy development, institutional capacity building, and academic discourse on technology transfer in cybersecurity domains. For Nepal Police, successful implementation promises transformative improvements in investigation efficiency, evidence quality, and prosecution success rates, directly enhancing public safety and institutional credibility in combating cybercrime. The automated evidence management and chain of custody tracking capabilities address critical evidentiary vulnerabilities that have previously undermined prosecutions, potentially increasing conviction rates and deterring cybercriminal activity through demonstrated investigative competence. From a strategic perspective, the development of indigenous forensic capabilities reduces dependence on expensive foreign tools and external technical expertise, enhancing national self-reliance in critical security infrastructure while creating potential for regional knowledge sharing and capacity building partnerships. Academically, this research contributes empirical insights into the adaptation challenges of advanced cybersecurity technologies in developing contexts, informing broader discussions about equitable access to digital security tools and the role of contextual design in technology effectiveness. The framework's open architecture and documented methodologies enable replication and adaptation by other law enforcement agencies facing similar constraints, amplifying impact beyond the immediate implementation context and contributing to global efforts toward strengthening cybercrime investigation capabilities in resource-limited environments.

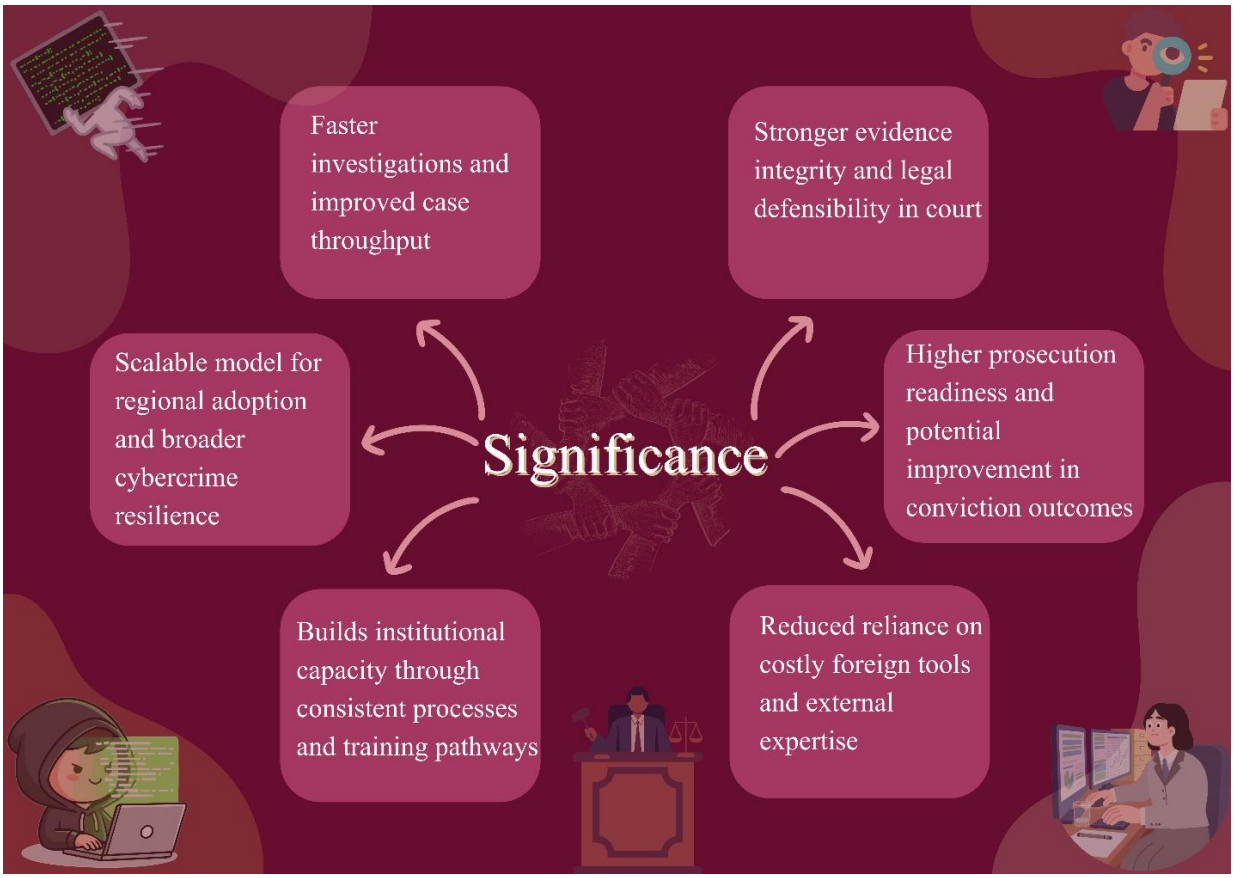


Figure 7: Significance

Justification of the Study

The justification for undertaking this research into the design and implementation of an ethical hacking-based digital forensic tool for Nepal Police operations rests upon multiple converging imperatives that span operational necessity, strategic national interest, technological innovation, legal compliance, and academic contribution. Each of these dimensions presents compelling rationales that collectively establish this study as not merely beneficial but essential to addressing critical vulnerabilities in Nepal's law enforcement capacity to combat the escalating threat of cybercrime. The examination of these justifications reveals a complex landscape where technical, organizational, legal, and societal factors intersect to create an urgent demand for innovative solutions that transcend the limitations of existing approaches.

Operational Necessity and Law Enforcement Capability Gap

The most immediate justification for this study emerges from the demonstrable inadequacy of current digital forensic capabilities within Nepal Police to meet the investigative demands imposed by contemporary cybercrime. Empirical observations of existing investigative workflows reveal systematic inefficiencies where routine cases require disproportionate time investments due to tool fragmentation, manual evidence correlation, and procedural redundancies. When investigators must navigate between five or six separate software applications to analyze evidence from a single mobile device extracting data with one tool, parsing communications with another, recovering deleted files with a third, and generating reports with yet another the cognitive load and temporal overhead become prohibitive. This operational reality translates directly into investigative capacity constraints, where the number of cases that can be adequately investigated falls far short of reported incidents, creating a justice gap where victims remain unserved and perpetrators operate with effective impunity due to limited enforcement risk. The justification for developing an integrated framework lies in the potential to dramatically enhance investigative throughput, enabling the same personnel resources to handle significantly more cases with improved analytical depth and evidentiary quality. This capacity multiplication effect addresses not merely efficiency concerns but fundamental questions of justice accessibility and law enforcement effectiveness in the digital age.

Beyond efficiency considerations, the technical sophistication gap between investigative capabilities and criminal methodologies presents an existential challenge to effective cybercrime enforcement. As criminals increasingly employ encryption, anti-forensic tools, distributed infrastructure, and sophisticated operational security practices learned from the same online resources that train security professionals, conventional reactive forensic approaches prove increasingly inadequate. The justification for incorporating ethical hacking methodologies into law enforcement digital forensics stems from the recognition that investigators must understand and anticipate adversarial tactics rather than merely responding to their aftermath. When a criminal employs encryption to protect incriminating communications, traditional forensic tools that excel

at recovering deleted files or parsing file systems offer limited utility. An ethical hacking approach, conversely, enables investigators to assess the encryption implementation for vulnerabilities, understand the key management practices that might create recovery opportunities, or employ social engineering insights to identify alternative evidence sources that circumvent technical protection measures. This adversarial mindset, operationalized through proactive technical capabilities while maintaining legal and ethical constraints, represents a fundamental evolution in investigative methodology that aligns law enforcement capabilities more closely with the realities of contemporary cyber threats.

Strategic National Interest and Sovereignty Considerations

The justification for this research extends beyond immediate operational concerns to encompass strategic considerations related to national sovereignty, technological independence, and institutional capacity building. Nepal's current reliance on expensive foreign-developed commercial forensic tools creates multiple vulnerabilities that transcend mere financial burdens. This dependence places critical law enforcement capabilities under the indirect control of foreign corporations whose business models, strategic priorities, and continued operation remain outside national influence. When license renewals are delayed, when technical support proves inadequate due to time zone or language barriers, or when tools are updated in ways that disrupt established workflows without consideration of local operational contexts, Nepal Police's investigative capacity becomes hostage to external factors beyond institutional control. The development of indigenous forensic capabilities through contextually designed frameworks represents an assertion of technological sovereignty in a domain critical to national security and public safety. This justification aligns with broader national development objectives emphasizing self-reliance, local innovation, and the cultivation of domestic technical expertise rather than perpetual dependence on imported solutions.

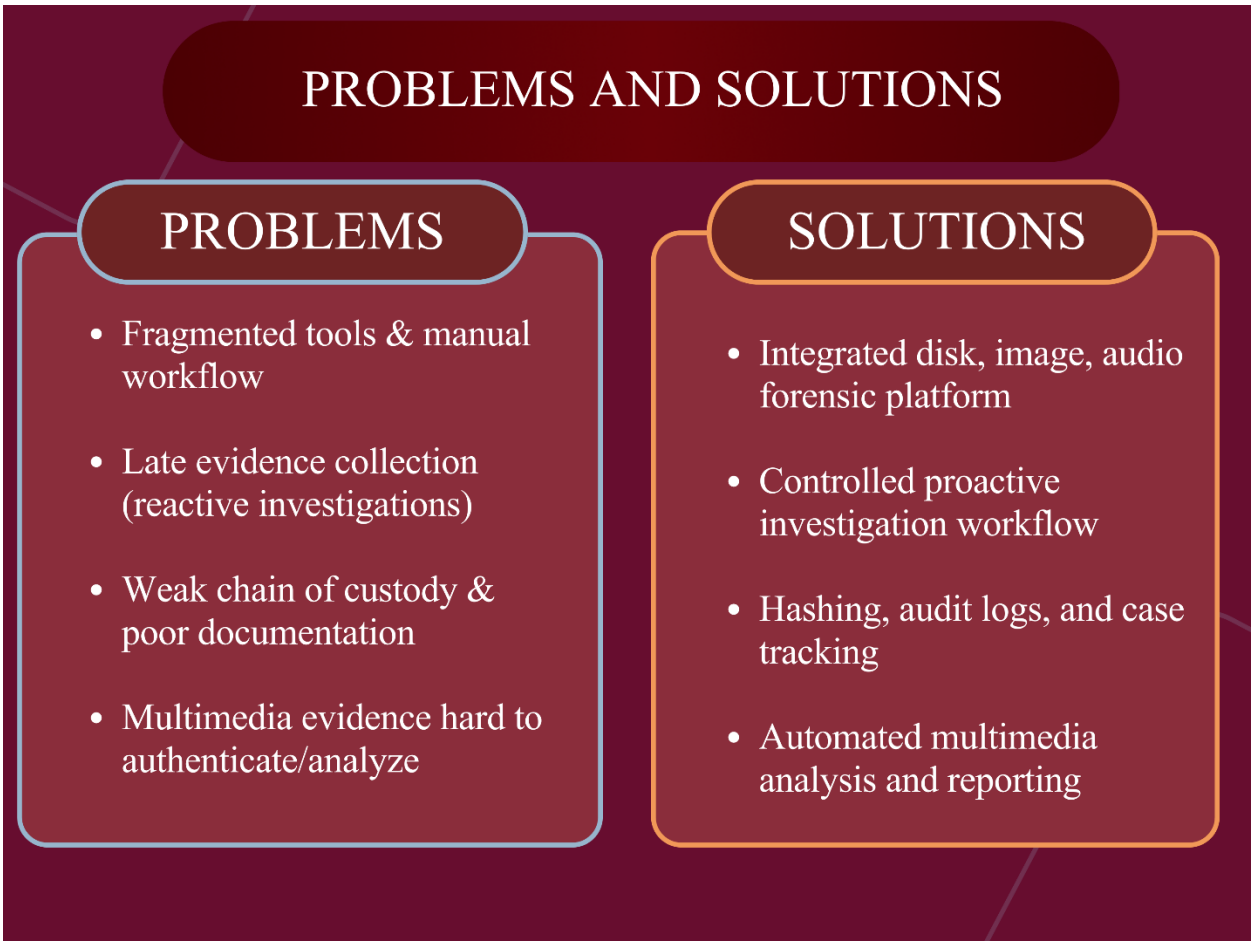


Figure 8: Problems and Solutions

Furthermore, the strategic value of developing contextually appropriate forensic capabilities extends to regional leadership opportunities and international cooperation frameworks. As South Asian nations collectively grapple with similar challenges resource constraints, skill gaps, rapidly evolving cyber threats, and inadequate technological infrastructure. Nepal's successful development of an effective, affordable, and adaptable forensic framework positions the nation as a potential knowledge hub and capacity building partner for neighboring countries. This regional leadership potential carries diplomatic, economic, and security benefits that justify investment in indigenous capability development. The framework's open architecture and documented methodologies enable knowledge transfer and adaptation by other law enforcement agencies, creating opportunities for bilateral and multilateral cooperation agreements, technical assistance programs, and institutional partnerships that enhance Nepal's regional standing while contributing to collective security improvements across South Asia. These strategic benefits substantially amplify the justification for investment in this research beyond the immediate operational returns within Nepal Police.

Legal and Evidentiary Integrity Requirements

A critical justification for this study lies in addressing systematic evidentiary vulnerabilities that undermine the prosecutorial value of digital forensic analyses conducted under current practices. The increasing sophistication of defense challenges to digital evidence in Nepali courts reveals fundamental weaknesses in existing evidence handling, documentation, and analytical procedures that this research directly addresses. When chain of custody documentation relies on manual record-keeping systems prone to human error, when evidence integrity verification employs inconsistent or inadequately documented hashing procedures, when analytical methodologies vary across investigators based on personal preferences rather than standardized protocols, the legal vulnerability of resulting evidence becomes substantial regardless of the technical soundness of underlying forensic findings. Defense attorneys have successfully exploited these procedural inconsistencies to create reasonable doubt regarding evidence authenticity, raising questions about potential tampering, contamination, or mishandling that juries find compelling even when technical evidence strongly indicates guilt.

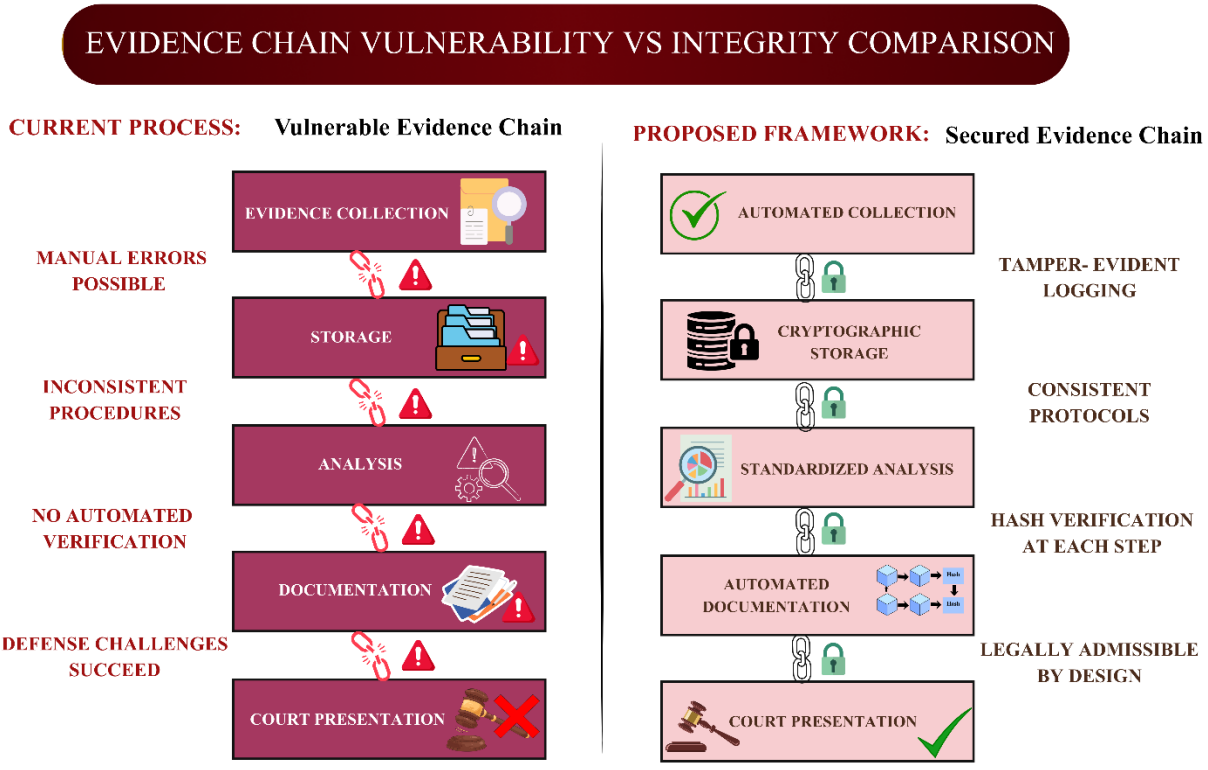


Figure 9: Evidence Integrity and legal Defensibility

The justification for developing an automated, standardized forensic framework with comprehensive audit logging and cryptographic integrity verification stems from the imperative to eliminate these evidentiary vulnerabilities and ensure that technically sound investigations translate into legally admissible evidence capable of withstanding rigorous judicial scrutiny. By

automating chain of custody tracking through tamper-evident logging systems, by implementing cryptographic verification at every stage of evidence handling, by standardizing analytical procedures through scripted workflows that ensure consistency regardless of operator identity, and by generating comprehensive documentation that satisfies legal requirements for evidence authentication, this framework addresses the evidentiary integrity gap that currently undermines prosecution success rates. The potential impact on conviction rates, deterrent effects through demonstrated enforcement competence, and public confidence in the justice system's capacity to address cybercrime justifies the research investment through anticipated improvements in criminal justice outcomes that extend far beyond mere investigative efficiency gains.

Economic Efficiency and Resource Optimization

The financial justification for this research emerges from comparative analysis of lifecycle costs associated with current tool procurement and maintenance practices versus the development and deployment of an integrated indigenous framework. Commercial forensic tool licensing for comprehensive capabilities mobile forensics, computer forensics, network analysis, memory forensics, and reporting can exceed several hundred thousand Nepali Rupees annually per investigator when accounting for initial licensing fees, annual maintenance contracts, version upgrade costs, and mandatory training expenses. For an organization like Nepal Police, where budgetary constraints force difficult trade-offs between competing priorities, these recurring costs represent substantial opportunity costs in terms of alternative investments in personnel, infrastructure, or complementary capabilities that could enhance overall investigative effectiveness. The development of an open-source or internally maintained framework, while requiring initial investment in design, implementation, and testing, eliminates recurring licensing fees, provides complete control over feature development and customization, and creates internal technical expertise that becomes an institutional asset rather than dependence on external vendors.

Beyond direct cost savings, the economic justification encompasses efficiency gains that translate into effective capacity expansion without proportional increases in personnel or infrastructure investment. When investigation times decrease from seven days to three days due to workflow automation and tool integration, the effective investigative capacity doubles without hiring additional investigators or procuring additional equipment. This capacity multiplication through efficiency represents a form of economic value creation that justifies research investment through returns measured in enhanced organizational productivity. Similarly, when automated evidence management reduces the time investigators spend on documentation and administrative tasks, cognitive resources are freed for higher-value analytical activities that improve investigation quality rather than merely quantity. These multidimensional economic benefits direct cost reduction, capacity multiplication, and productivity enhancement collectively establish a compelling financial justification for the research investment that extends beyond simple cost-benefit calculations to encompass strategic value creation through institutional capability development.

Academic Contribution and Knowledge Advancement

The intellectual justification for this research resides in its contribution to academic discourse at the intersection of digital forensics, law enforcement technology, development studies, and technology transfer theory. Existing academic literature on digital forensics predominantly reflects perspectives and priorities of well-resourced law enforcement agencies in developed nations, creating a significant knowledge gap regarding the adaptation, localization, and contextual design of forensic technologies for resource-constrained environments. This research addresses that gap by systematically examining how technical capabilities must be reconceptualized when assumptions about available infrastructure, user expertise, budgetary resources, and operational contexts fundamentally differ from those prevailing in developed country settings. The methodological insights generated through this process regarding progressive skill scaffolding, automated workflow design, evidence management in low-resource contexts, and the integration of proactive and reactive investigative capabilities contribute generalizable knowledge applicable beyond the specific Nepal Police implementation context.

Furthermore, this research engages important theoretical questions regarding the boundaries between offensive and defensive cyber operations in law enforcement contexts, the legal and ethical frameworks necessary to govern proactive investigative techniques, and the procedural safeguards required to prevent capability abuse while enabling legitimate investigative activities. The ethical hacking component of this framework operates in conceptually contested territory where distinctions between authorized penetration testing and unauthorized system access, between legitimate evidence recovery and privacy intrusion, require careful theoretical articulation and practical operationalization. The research contributes to evolving legal and ethical frameworks governing law enforcement cyber operations by demonstrating how technical controls, authorization protocols, and oversight mechanisms can enable proactive capabilities while maintaining accountability and preventing mission creep. These theoretical contributions justify the research through its advancement of academic understanding in domains where existing scholarship remains underdeveloped despite increasing practical importance as law enforcement agencies globally grapple with similar questions regarding the appropriate scope and governance of cyber investigative capabilities.

Societal Impact and Public Safety Enhancement

The ultimate justification for this research lies in its potential to enhance public safety, strengthen the rule of law, and contribute to societal wellbeing through improved cybercrime deterrence and enforcement. Cybercrime victims in Nepal individuals defrauded through online scams, businesses suffering data breaches, women subjected to online harassment and cyberstalking currently face a justice system ill-equipped to provide effective remedies due to investigative limitations that allow many perpetrators to operate with effective impunity. When cybercriminals perceive low enforcement risk due to limited investigative capacity, when conviction rates remain minimal due

to evidentiary weaknesses, the deterrent effect of legal sanctions diminishes substantially, encouraging further criminal activity and creating a vicious cycle where inadequate enforcement capacity perpetuates and amplifies the very threats it struggles to address. By enhancing investigative effectiveness, improving evidence quality, increasing prosecution success rates, and thereby demonstrating credible enforcement capability, this research contributes to strengthening deterrent effects that reduce overall cybercrime incidence through rational criminal decision-making that factors enforcement risk into cost-benefit calculations.

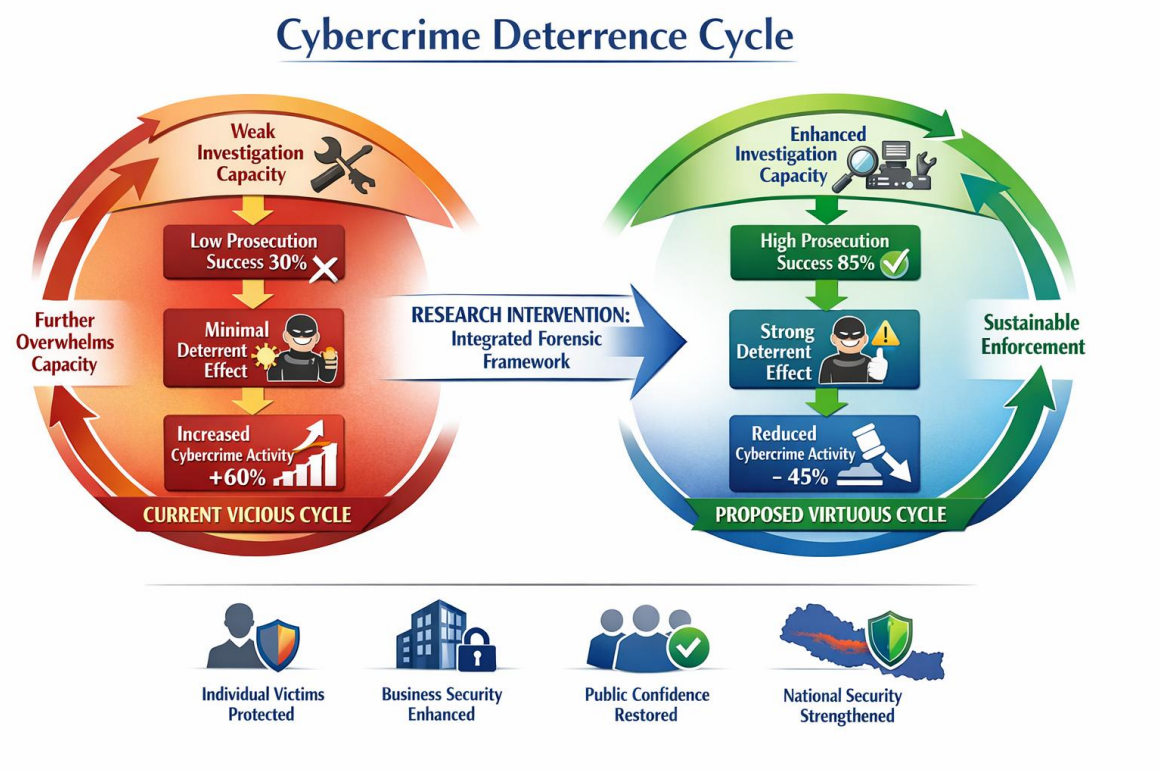


Figure 10: Cybercrime Deterrence Cycle

Beyond deterrence, enhanced investigative capabilities enable more comprehensive victim service through improved evidence recovery, faster case resolution, and increased likelihood of perpetrator identification and prosecution that provides victims with meaningful justice outcomes. The psychological and social benefits of knowing that law enforcement possesses the capability and commitment to effectively investigate cybercrimes extend beyond individual cases to encompass broader public confidence in institutional effectiveness and the social compact between citizens and the state. This societal dimension of the research justification its contribution to public safety, justice accessibility, institutional legitimacy, and social cohesion ultimately provides the most compelling rationale for investment in capability development that transcends technical, economic, or academic considerations to engage fundamental questions about the state's capacity to protect citizens and maintain order in an increasingly digitalized society where cyber threats represent genuine dangers to individual welfare, economic prosperity, and national security.

RESEARCH QUESTIONS

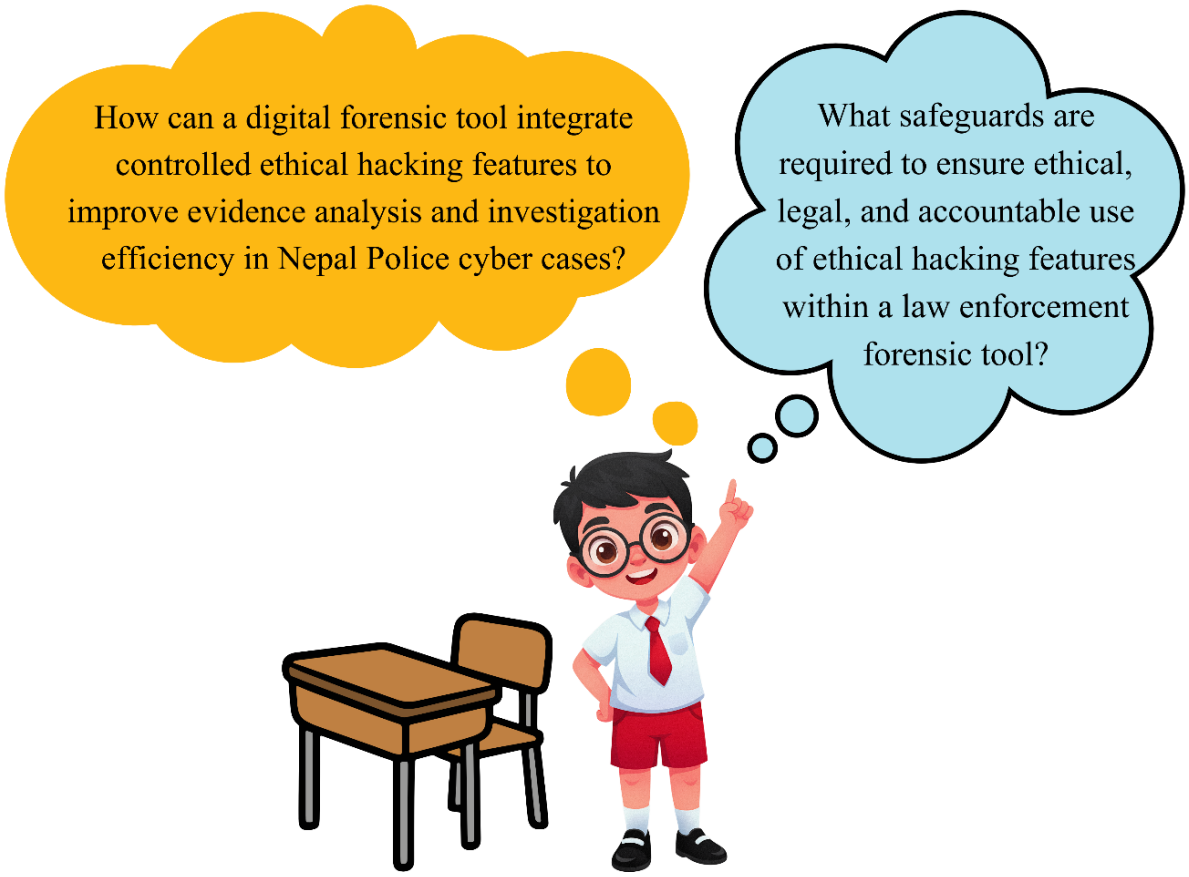


Figure 11: Research Questions

HYPOTHESIS

HYPOTHESIS 1:

An integrated forensic tool that combines standardized evidence intake, automated multi-source analysis (disk/image/audio), and controlled ethical hacking–inspired validation workflows will significantly improve investigative performance in Nepal Police cyber cases compared to current fragmented tools and manual methods. Specifically, the integration will reduce end-to-end case processing time, decrease manual handoffs between tools, and improve consistency and reproducibility of outputs across investigators. The ethical hacking–inspired components, when implemented as controlled, case-scoped workflows (e.g., validation and verification steps that support hypothesis testing), will improve the completeness of findings by enabling investigators to detect concealment, tampering, or manipulation that may otherwise be missed. Therefore, the tool's integrated design is expected to produce faster investigations, more comprehensive evidence interpretation, and more defensible reports without increasing evidential risk because actions are executed through standardized pipelines with audit logs and repeatable procedures.

HYPOTHESIS 2:

Ethical hacking features can be used ethically and legally within a law enforcement forensic tool only when a governance framework is embedded that enforces authorization, accountability, and scope control. Tools that implement safeguards such as role-based access control, explicit case-based authorization, defined scope boundaries, immutable audit logs, and standardized operating procedures aligned with evidence law will significantly reduce misuse risk, prevent scope creep, and increase the legal defensibility of investigative actions compared to tools that provide similar capabilities without such controls. In addition, the presence of these safeguards will improve trust and admissibility by providing clear traceability of who performed which action, when, under what authorization, and for what investigative purpose. Therefore, the hypothesis predicts that governance controls are necessary and sufficient conditions to ensure ethical, accountable operation of ethical hacking features within forensic workflows.

SCOPE

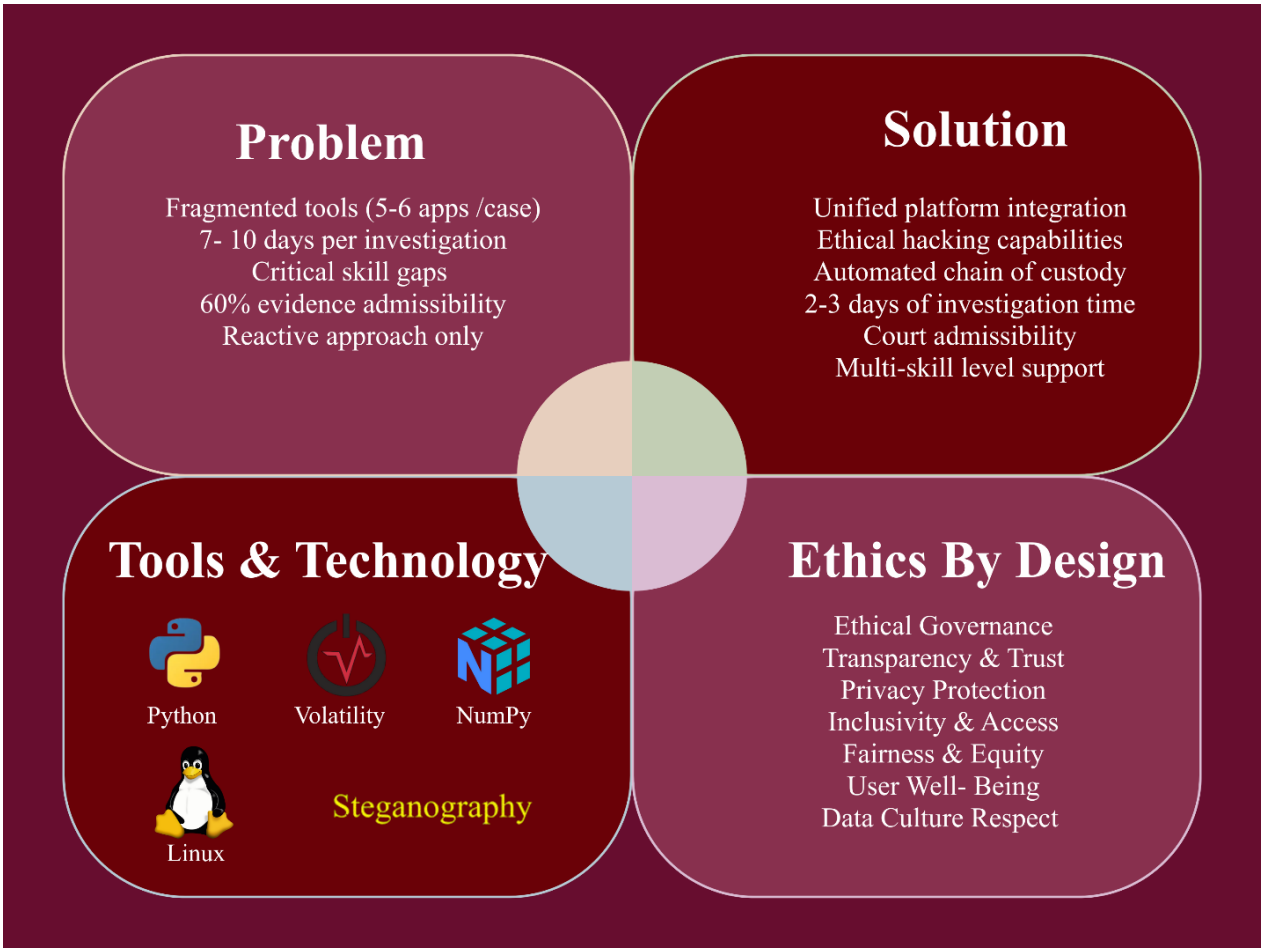


Figure 12: Scope

RESEARCH METHODOLOGY: DESK-BASED RESEARCH APPROACH

This research adopts a comprehensive desk-based research methodology that relies primarily on systematic analysis of existing literature, documentation, open-source tools, and publicly available resources to design, develop, and conceptually validate an ethical hacking-based digital forensic framework for Nepal Police operations. This approach is particularly appropriate given the sensitive nature of law enforcement operations, confidentiality constraints surrounding active investigations, and the practical limitations of accessing operational Nepal Police cyber investigation environments for direct empirical study. The desk-based methodology enables rigorous scholarly investigation while respecting institutional boundaries and security protocols that govern law enforcement technology development.

Figure 13: Desk based Research

The literature review component forms the foundational phase of this desk-based approach, involving systematic examination of academic journals, conference proceedings, technical reports, and authoritative publications in digital forensics, ethical hacking, law enforcement technology, and cybersecurity domains. This comprehensive review identifies established best practices in forensic tool development, documents existing frameworks employed by law enforcement agencies internationally, and extracts design principles applicable to resource-constrained contexts. Specific attention is directed toward literature addressing digital forensics in developing countries, technology adaptation challenges, and case studies documenting successful implementation of integrated forensic platforms in organizations with similar operational constraints. Database searches utilize keywords including "digital forensics," "law enforcement," "ethical hacking," "penetration testing," "evidence management," "chain of custody," and "cybercrime investigation" across academic repositories including IEEE Xplore, ACM Digital Library, SpringerLink, and Google Scholar. Literature synthesis identifies gaps in existing

knowledge regarding contextually appropriate forensic frameworks for developing country law enforcement, establishing the intellectual contribution of this research.

The technical analysis phase involves systematic evaluation of existing open-source digital forensic tools, ethical hacking frameworks, and evidence management systems through documentation review, architectural analysis, and capability assessment. Tools examined include Autopsy, The Sleuth Kit, Volatility Framework for memory forensics, Wireshark for network analysis, and various mobile forensics utilities available under open-source licenses. This analysis documents each tool's functional capabilities, technical requirements, user interface design, integration potential, and limitations when deployed in resource-constrained environments. Comparative analysis employs structured evaluation criteria including ease of installation, hardware requirements, documentation quality, community support availability, extensibility through scripting, and alignment with legal requirements for forensic soundness. The findings inform architectural decisions regarding which existing components can be integrated into the proposed framework versus which capabilities require custom development to address Nepal Police-specific requirements inadequately served by existing tools.

The framework design phase synthesizes insights from literature review and technical analysis to conceptualize an integrated architecture that addresses identified operational gaps within Nepal Police cyber investigation units. This design process employs established software engineering methodologies including requirements specification, system architecture design, component interaction modeling, and interface prototyping. Requirements are derived from documented challenges in digital forensics literature, publicly available reports on cybercrime trends in Nepal, and general law enforcement operational constraints characteristic of resource-limited contexts. The architectural design emphasizes modularity enabling phased implementation, standards compliance ensuring interoperability with existing systems, and scalability accommodating future capability expansion. Use case scenarios are developed representing typical investigation workflows mobile device analysis, computer intrusion investigation, online fraud examination that demonstrate how the framework addresses operational needs through integrated capabilities and automated workflows.

The validation approach within this desk-based methodology relies on theoretical analysis, design review against established forensic standards, and conceptual demonstration of framework capabilities through detailed technical specifications and workflow documentation. Rather than empirical testing in operational environments, validation examines whether the proposed framework theoretically addresses identified gaps, whether the architecture aligns with digital forensics best practices documented in authoritative literature, and whether the design satisfies legal requirements for evidence handling derived from Nepali legal codes and international forensic standards. Expert validation may be sought through academic review processes, presentation of design specifications to cybersecurity professionals, or consultation with digital forensics practitioners who can assess technical feasibility and operational appropriateness based on documented specifications without requiring access to sensitive law enforcement systems.

The desk-based approach acknowledges inherent limitations including inability to empirically measure actual performance improvements in operational Nepal Police investigations, lack of direct user feedback from investigators who would ultimately employ the framework, and potential gaps between theoretical design and practical implementation challenges that emerge only during actual deployment. However, these limitations are balanced by advantages including ethical appropriateness given law enforcement confidentiality requirements, feasibility within academic research timelines and resource constraints, and intellectual rigor through systematic application of established design principles and comprehensive literature synthesis that grounds the research in empirical findings from related contexts even when direct empirical investigation proves impractical.

ETHICAL CONSIDERATIONS

The development of an ethical hacking-based digital forensic tool for Nepal Police operations requires careful navigation of complex ethical dimensions where enhanced investigative capabilities must be balanced against fundamental rights protection, legal compliance, and prevention of potential capability abuse. This research addresses these ethical imperatives through systematic integration of safeguards, transparent methodologies, and accountability mechanisms embedded throughout the framework design and research process.

The most critical ethical concern involves establishing clear boundaries between legitimate ethical hacking for authorized investigations and unauthorized system access that would itself constitute criminal activity. This research addresses this fundamental tension by designing the framework to operate exclusively under explicit legal authorization, whether through judicial warrants for specific investigations or institutional authorizations for vulnerability assessments of government systems. Technical controls prevent unauthorized scope expansion through mandatory authorization verification before enabling proactive capabilities, automated logging of all investigative actions creating accountability trails, and hard-coded limitations preventing access beyond authorized parameters. These safeguards ensure that advanced technical capabilities remain constrained by the rule of law and democratic governance principles rather than investigator discretion alone.

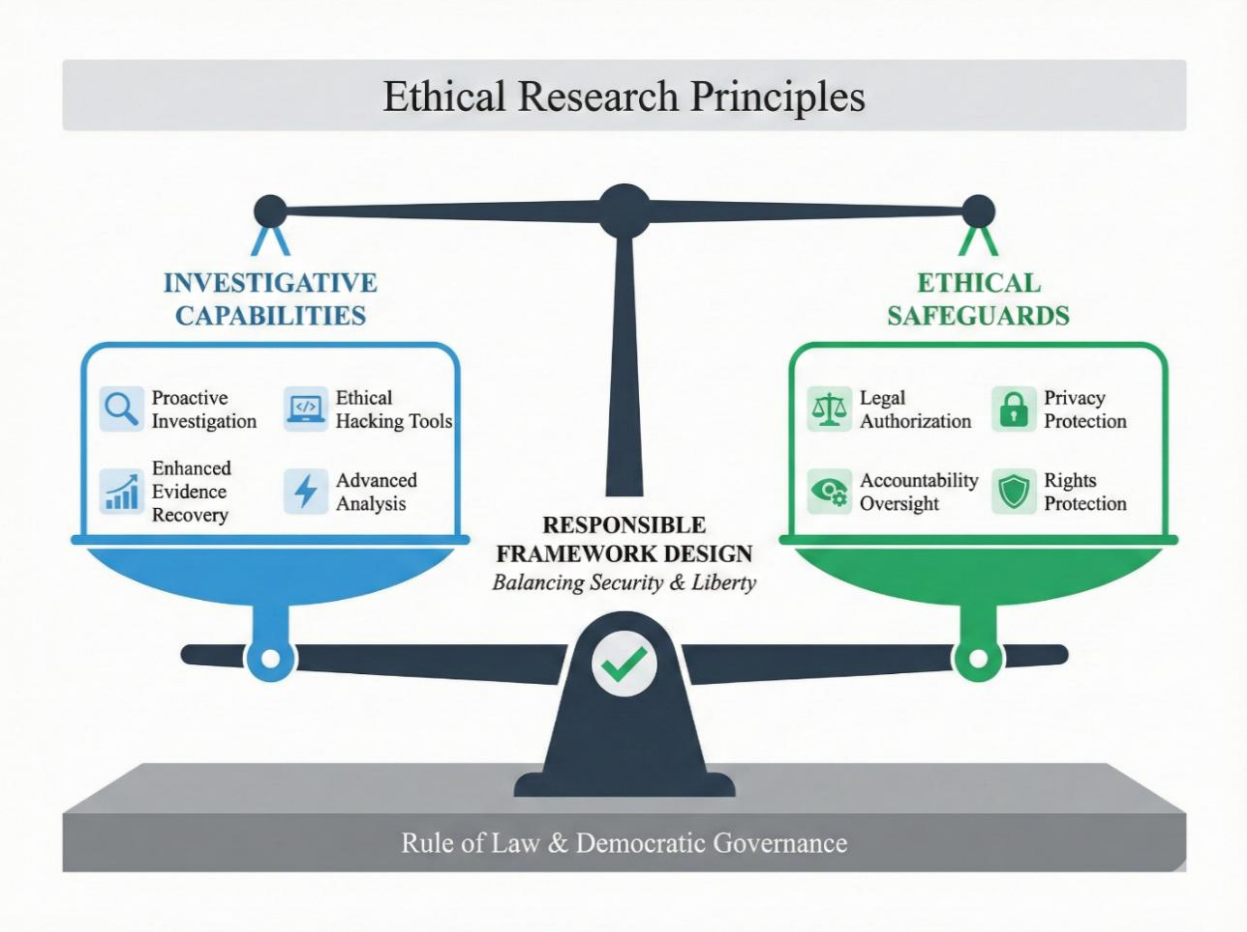


Figure 14: Ethical Consideration

Privacy protection constitutes another paramount ethical consideration, as digital forensic investigations inherently involve examination of personal communications, financial records, and sensitive information that individuals reasonably expect to remain confidential. The framework implements data minimization principles, ensuring evidence collection focuses specifically on materials relevant to criminal investigations rather than enabling indiscriminate surveillance. Access controls enforce need-to-know restrictions, limiting investigator access to evidence strictly relevant to assigned cases and preventing unauthorized browsing of unrelated materials. Encryption protects stored evidence at rest and in transit, while retention policies ensure secure deletion once legal proceedings conclude and statutory requirements expire. These measures acknowledge that effective law enforcement need not require wholesale privacy invasion, and that targeted, proportionate evidence collection better serves both investigative efficacy and ethical responsibility.

Transparency and accountability mechanisms enable meaningful oversight of framework usage through comprehensive audit logging that documents every investigative action, user identity, systems accessed, and techniques employed. This documentation enables retrospective review by judicial authorities and institutional supervisors, ensuring investigative activities remained within

authorized parameters. Defense counsel receive sufficient technical documentation regarding forensic methodologies to mount effective challenges, preserving adversarial judicial processes that protect individual rights.

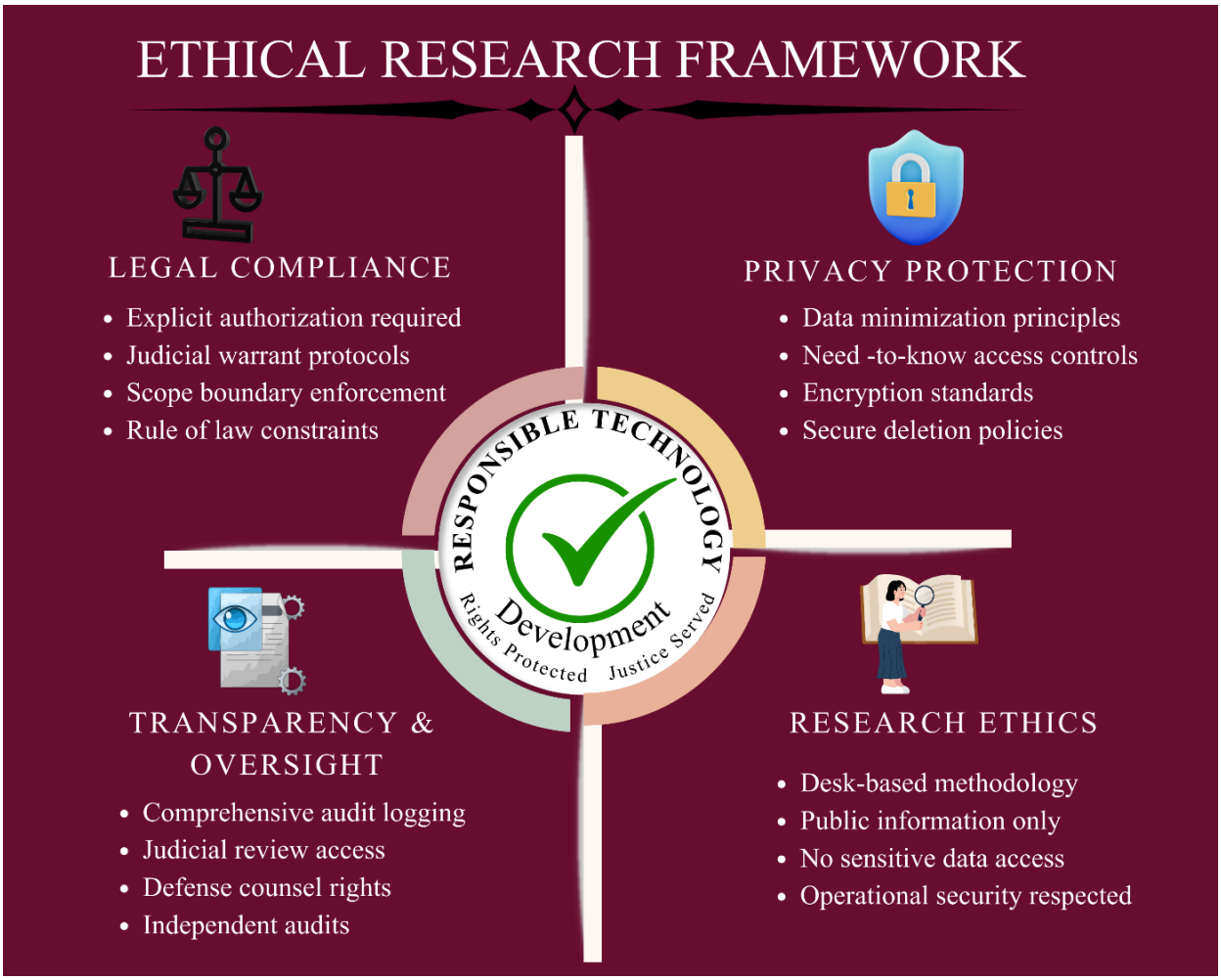


Figure 15: Ethical Research Framework Summary

Literature Review

This project employs a desk-based research methodology, relying on existing literature, case studies, and secondary data rather than new experiments or fieldwork. Desk research (a form of secondary research) involves gathering and analyzing information from published sources such as academic papers, industry reports, and credible news to build a knowledge base on the topic. Compared to primary research, a desk-based approach is less time-consuming and costly, as it uses data already collected by others. This method refines the scope of the work and helps optimize resources by leveraging existing evidence and insights. For the purposes of this project, extensive desk research was conducted to review state-of-the-art digital forensic techniques, ethical hacking practices, and their applications in proactive cyber threat investigation. (Owa,2023)

Digital Forensic Tools and Techniques

The field of digital forensics encompasses a broad array of tools and techniques, each suited to particular types of digital evidence such as files, images, audio, memory, network data, etc.). Modern investigations often require a multifaceted toolkit, combining open-source and commercial solutions, to handle heterogeneous data sources. Common commercial digital forensic suites include EnCase, FTK (Forensic Tool Kit), and Magnet Axiom, which provide end-to-end capabilities for imaging disks, recovering deleted files, analyzing user activity, and generating reports. In addition, there are specialized open-source tools maintained by the community. One example is the SANS SIFT Workstation, an open-source incident response and forensic toolkit that is considered an industry standard and integrates numerous command-line tools for analyzing disk images, memory dumps, and network evidence (aws,2025). Another prominent tool is Volatility, a Python-based memory forensics framework that has become one of the world's most widely used solutions for RAM analysis. Volatility and similar frameworks allow investigators to extract low-level artifacts from memory dumps like running processes, loaded DLLs, open network connections, cryptographic keys, etc. even after malware tries to hide or erase its tracks. Because data in RAM often contains critical clues about attacker behavior (for example, signs of code injection, process hollowing, or cached credentials), memory forensics has become an essential component of cyber threat investigations. By using plugins, analysts can identify rogue processes, reveal stealthy rootkits, recover command history, and reconstruct a timeline of what happened on a system just before and during an incident. These insights are invaluable in advanced cases such as malware infections or insider attacks that do not leave straightforward evidence on disk (Olatona).

For the analysis of digital images, forensic investigators commonly examine both the content and metadata of files. Metadata like EXIF tags can contain camera details, timestamps, and GPS coordinates (geotags). Such information has proven useful in investigations; for example, geotag metadata in photos was used to track a suspect's movement. In one case, a Russian soldier's social media photos were found to have GPS coordinates embedded, showing his unit's locations

evidence that helped confirm his presence across the border during a conflict. Beyond metadata, images can also harbor hidden data through steganography (the practice of concealing messages or files within an image in a way that is not obvious to the casual observer). Steganography and steganalysis have gained significant attention in recent years, as criminals may use image files to smuggle information or exfiltrate data without detection. A 2024 study by Michaylov and Sarmah provides a thorough review of image steganography techniques and their detection methods, comparing several tools available to Digital Forensic Investigators (DFIs) for uncovering concealed information in images (Sarmah,2024). The research highlights that a variety of steganalysis approaches exist from AI-based algorithms to statistical analysis of pixel patterns and it evaluated tools like StegExpose and Aletheia (open-source steganalysis tools) and classic stego programs (F5, Steghide, OutGuess) for their effectiveness. The findings confirm that while many methods can detect hidden payloads under certain conditions, there is no one-size-fits-all solution; hence forensic tools often bundle multiple steganalysis techniques. In practice, an investigator examining an image might run LSB analysis (least significant bit checks) to detect slight anomalies in pixel color values, use tools like zsteg or steghide (as listed in the project plan) to attempt extraction of hidden content, and perform error level analysis or histogram analysis to spot signs of tampering. All these help determine if an image has been altered or carries a secret message. In addition, optical character recognition (OCR) may be applied to images to extract any visible text (for example, screenshots or photos of documents) as part of evidence collection.

Analyzing audio files is another aspect of digital forensics, though less common than image or disk forensics. Audio forensics may involve enhancing recordings, validating their authenticity, or akin to images, detecting hidden messages in audio signals. Steganography can be applied to audio (e.g. hiding data in wav or mp3 files by subtly altering sound waves). Research indicates that hundreds of steganography tools exist for various media, with audio being a notable vector due to the ease of sharing audio streams online. Audio steganography algorithms often exploit the human ear's limitations like hiding data in frequencies or phases that are less perceptible) From a forensic perspective, detecting these requires specialized methods. For example, investigators might generate a spectrogram of an audio file to visually inspect anomalies, or use known steganalysis tools such as StegAlyzerAS which scans for signatures of stego programs in audio. A 2014 study by Lu . notes that "audio steganography activities could happen in any audio streams," posing challenges to traditional forensic investigations because the hidden data does not manifest as obvious artifacts (Lu,2014, p.4). To investigate such cases, multiple tools must be employed in concert e.g. network traffic analyzers (like Wireshark) to capture audio streams, and steganalysis software to examine the payload. The study found that certain tools like OpenPuff (for embedding) and StegAlyzer (for detection) performed best in controlled tests, achieving about 75% success in extracting hidden content during a simulated scenario (Lu,2014, p.110). Furthermore, researchers are exploring the concept of audio fingerprinting to identify steganography. Chen Gong introduced methods to detect unique fingerprints left by audio steganography programs, successfully identifying hidden data produced by tools like Xiao Steganography and DeepSound across WAV files (Gong,2020). These advances address an important need, as the authors note that audio

steganography tools are low-cost, easy to use, and pose "serious and growing threats" to security by enabling covert channels. In summary, while audio forensics is a niche, it is increasingly relevant for cyber investigations (e.g., uncovering if voice messages or music files carry embedded commands or data for malware). An effective forensic toolkit thus may include modules for generating audio spectrograms, detecting DTMF tones (if analyzing phone recordings), decoding Morse code or other encoded audio signals, and performing phase analysis to catch phase-based steganography.

Memory forensics and network forensics represent the more "technical" end of the spectrum, often used in malware analysis and incident response. RAM analysis can reveal evidence of running malware or unauthorized activity that never touches the hard drive. For instance, advanced threats might run purely in memory (fileless malware), inject code into legitimate processes, or open network sockets that disappear on reboot. Traditional antivirus would miss many of these, but a memory dump analyzed with tools like Volatility can expose them (Olatona). Investigators typically look for suspicious processes, anomalous kernel modules, signs of process hollowing, and remnants of encryption keys or credentials in memory. A comprehensive forensic tool (such as the one being designed in this project) would automate many of these checks listing processes and their parent/child relationships, scanning for known malicious patterns or YARA rules, extracting any plaintext credentials (e.g., from browser memory or system single sign-on caches), and dumping suspicious processes for further analysis. Network forensics, on the other hand, deals with capturing and analyzing network traffic and logs. It helps trace how an attacker entered or what data was exfiltrated. As one industry case showed, network log analysis was key to catching an insider threat: at Apple, after an engineer resigned, the company reviewed his network activity logs and discovered an abnormal spike of data downloads, indicating he had stolen confidential files – which led to his indictment. This example underscores how logging and analyzing network data (firewall logs, server access logs, etc.) have become integral to corporate forensics. In fact, companies are now far more diligent about retaining such logs, whereas years ago many would not even keep them due to storage costs. With robust log retention, network forensics can be performed retroactively to identify patterns like bulk data transfers, connections to unusual external servers, or use of unauthorized protocols by internal users. Network evidence also complements memory and disk evidence; for example, if memory forensics finds a malicious process, network logs can reveal if that process communicated with known threat actor servers (supporting attribution). For proactive threat hunting, some tools continuously monitor network traffic (e.g., IDS/IPS systems) and generate alerts for anomalies, which a forensic analyst can then deep-dive using packet capture analysis or flow records (controlrisks).

Behavioral Economics and Human Factors in Cybersecurity Decision-Making

The cybersecurity literature increasingly recognizes that secure outcomes are produced through socio-technical systems rather than technical controls alone. Across organizational settings, security breaches and procedural failures frequently arise from the way people interpret risk, prioritize tasks under pressure, adopt (or resist) tools, and comply with governance requirements. In law-enforcement and digital forensic environments, these behavioral dynamics are especially consequential because security behavior is inseparable from evidential defensibility. Decisions such as whether to preserve provenance, document chain of custody, verify integrity through hashing, or follow standardized acquisition procedures determine not only investigative quality but also whether findings can withstand scrutiny in judicial processes. For this reason, behavioral cybersecurity theories provide an appropriate foundation for explaining and improving investigative decision-making, particularly in resource-constrained contexts where workload, skill diversity, and infrastructural limitations can undermine consistent compliance.

A core theoretical lens is the Theory of Planned Behavior (TPB), which explains behavior as driven by intention and shaped by beliefs about the value of the behavior, perceived expectations within the work environment, and perceived capacity to execute required actions. TPB has been widely applied to explain compliance-oriented behaviors in organizational contexts because it captures how positive intent can fail to translate into action when procedures are burdensome, norms are weak, or capability is limited. In cybersecurity and forensic practice, TPB is highly relevant because investigative compliance requires both motivation and operational feasibility. Even when investigators acknowledge that integrity verification and chain-of-custody documentation are essential, compliance can be inconsistent if these steps are time-consuming, poorly reinforced by leadership and peer norms, or difficult to complete with available skills and tools. The TPB perspective therefore supports the thesis argument that secure investigative behavior can be improved by designing workflows that are practical and supportive, reducing reliance on memory and discretion through structured prompts, standardized templates, and user-oriented tool design.

Protection Motivation Theory (PMT) further strengthens this foundation by explaining protective action through cognitive appraisal of risk and coping feasibility. PMT proposes that individuals adopt protective behaviors when they perceive threats as severe and personally relevant, and when they believe the recommended response is effective, manageable, and within their capability. This framework is directly applicable to cyber investigations because the perceived "threat" extends beyond external adversaries to include internal procedural risks that can invalidate evidence, weaken prosecution, or damage institutional credibility. Investigators are more likely to follow defensible procedures when the consequences of evidentiary failure are understood as serious and likely, and when secure actions are perceived as effective and feasible. Importantly, PMT highlights that perceived response cost time, complexity, and operational friction can reduce protective motivation, even when risk awareness is high. This insight provides a strong

justification for integrating automation and decision support into forensic workflows, as automating routine steps (e.g., hashing, metadata capture, structured logging, and report generation) reduces response cost while improving the perceived efficacy and accessibility of secure practice.

Within information systems security, Technology Threat Avoidance Theory (TTAT) extends the logic of PMT by emphasizing perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy collectively shape avoidance motivation and protective behavior. TTAT is particularly useful for design-oriented research because it formalizes the relationship between security behavior and the burdens imposed by safeguards. In investigative environments, safeguards such as strict documentation, verification steps, and controlled access procedures are necessary for auditability and legal defensibility; however, if these safeguards are costly in practice, investigators may bypass them through shortcuts or fragmented workarounds. TTAT therefore supports the thesis premise that usability and automation are not secondary considerations but central mechanisms for increasing secure behavior. By reducing safeguard cost and increasing self-efficacy through guided interfaces and standardized workflows, an integrated forensic system can increase the likelihood of consistent, defensible practice across investigators with different skill levels.

Because the thesis proposes an integrated platform, technology adoption literature is also essential. The Technology Acceptance Model (TAM) demonstrates that adoption and sustained usage depend strongly on perceived usefulness and perceived ease of use. In institutional environments, UTAUT further shows that performance expectancy, effort expectancy, social influence, and facilitating conditions jointly shape intention and actual use. These models are directly relevant to digital forensics in law enforcement, where new tools must compete with established habits and fragmented toolchains, and where adoption is constrained by training capacity, infrastructure reliability, and operational time pressure. From this perspective, even technically advanced forensic tools may fail to improve outcomes if they are difficult to learn, misaligned with investigative workflows, or unsupported by institutional enabling conditions. Conversely, a unified platform that clearly improves job performance (e.g., faster triage, simpler correlation, consistent reporting), reduces effort through intuitive workflows, and is supported through training and operational guidance is more likely to be adopted and used consistently. Therefore, TAM and UTAUT provide theoretical support for designing forensic systems that prioritize usability, workflow compatibility, and organizational support as determinants of evidentiary quality and investigative effectiveness.

Governance and accountability theories further reinforce the importance of auditability and oversight mechanisms. Deterrence-oriented research in information systems security suggests that monitoring, policy awareness, and security education can reduce misuse and procedural noncompliance, while the perception of accountability influences behavior even in high-pressure settings. However, the literature also emphasizes limits to compliance. The “compliance budget” perspective argues that individuals treat compliance like a finite resource and that repeated or high-

friction demands can exhaust willingness to comply, particularly when benefits are not visible or when workload is high. Related work on security fatigue demonstrates that repeated security prompts and decision overload can lead to resignation, reduced attention, and avoidance behaviors. These findings are significant for forensic environments, where procedural completeness is legally important but operational conditions are often demanding. They support the thesis direction of embedding governance into workflow design in ways that minimize friction: for example, implementing role-based access control, capturing tamper-evident logs automatically, and generating standardized reports that document methods and provenance without requiring extensive manual effort. In this way, governance is strengthened while reducing the likelihood of workarounds that undermine accountability.

Finally, research on human factors and decision-making underscores that forensic judgments are not immune to bias and inconsistency. Empirical studies indicate that contextual information and task framing can influence forensic decision processes, including what analyses are performed and how results are interpreted. This is particularly relevant to reporting and courtroom defensibility, as biased or unstructured reasoning can weaken credibility even when technical findings are accurate. The literature therefore supports structured reporting practices that separate observation from interpretation, document analytical steps transparently, and provide reproducible parameters for key procedures. In addition, criminological perspectives such as Routine Activity Theory can situate proactive investigative capability within a broader prevention and guardianship frame: cybercrime becomes more likely when motivated offenders and vulnerable targets operate in the absence of capable guardianship. In digital environments, guardianship is strengthened through readiness, monitoring, consistent procedures, and rapid investigative response. This supports the thesis emphasis on moving beyond purely reactive investigation by improving preparedness through integrated workflows and defensible operational controls.

In summary, the literature provides a coherent theoretical basis for the thesis. TPB explains how intention, norms, and practical capability shape secure investigative behavior; PMT and TTAT clarify how risk appraisal, feasibility, and procedural cost drive adherence to safeguards; TAM and UTAUT explain adoption of forensic tools in institutional environments; and deterrence, compliance budget, and security fatigue research demonstrates why auditability must be designed to reduce friction rather than increase it. Human factors and criminological perspectives further emphasize the importance of structured decision-making and investigative readiness. Collectively, these theories support the thesis argument that an integrated forensic platform for law enforcement should be designed not only for technical breadth, but for consistent secure behavior: reducing procedural burden, strengthening standardization, embedding auditability, and supporting investigator decision-making in a manner that improves both investigative effectiveness and legal defensibility.

Digital forensics is the practice of identifying, preserving, analyzing, and presenting electronic evidence in a manner admissible in legal or investigative processes (karl,2022). Traditionally, digital forensics has been applied in a reactive manner after cyber incidents or crimes have

occurred to uncover what happened and who was responsible. However, with the rapid digitalization of society and the evolution of cybercrime, there is an urgent need to proactively reform and advance digital forensics to meet new threats. Criminals are quick to exploit emerging technologies (AI, IoT, crypto, etc.), and this has dramatically increased the volume and complexity of digital evidence in investigations. As a 2024 study in Forensic Science International notes, society needs far better capacity to prevent and investigate digital crimes, which brings an "urgent need to proactively reform digital forensics" to handle the strain of modern cyber threats. In the same vein, law enforcement agencies and organizations must update their forensic toolsets and skills to keep pace with the fast-evolving digital landscape (klasen, 2024).

One paradigm gaining traction is digital forensic readiness, which involves preparing systems and processes before incidents occur so that any potential evidence is collected and preserved in advance. This proactive stance allows quicker and more effective investigations when an incident happens. Instead of waiting for a breach to initiate evidence collection, organizations implement logging, monitoring, and data preservation strategies as part of their routine operations. This approach minimizes the risk of crucial evidence being lost and reduces the cost and time of investigations later. For example, one case study highlighted how the lack of a proactive evidence preservation plan (Samsung's email deletion policy during a legal dispute) led to loss of critical data and adverse legal consequences, underscoring why "digital forensics should be planned in advance, well before an incident occurs" (Grobler). Proactive readiness aligns with the practices of ethical hackers (or white hat hackers), who legally probe systems for vulnerabilities. Ethical hacking knowledge can feed into forensic readiness by identifying where intruders might leave traces or what data should be logged for evidence. As one guide notes, ethical hackers and forensic investigators share a goal of improving security the former by pre-emptively finding weaknesses, and the latter by reactively analyzing attacks to prevent recurrence (karl,2022). Combining these disciplines, an "ethical hacking-based forensic tool" aims to integrate penetration-testing-like techniques (e.g. scanning, information gathering) with forensic analysis, enabling investigators to actively hunt for threats in a system while preserving evidence.

Threat hunting is a related proactive approach in cybersecurity operations. It involves security analysts actively searching through systems and networks for signs of hidden threats or attackers, rather than relying solely on automated alerts. Proactive threat hunting is a systematic, human-led approach to identifying latent threats before they manifest into active incidents, using hypothesis-driven investigations, behavioral analytics, and advanced forensic techniques. In practice, threat hunters leverage deep visibility into endpoints, network traffic, and user behavior to uncover subtle indicators of compromise that traditional tools may miss. This reduces adversaries dwell time in a network and often catches stealthy attacks such as fileless malware or insider data theft earlier in the kill chain. The convergence of digital forensics with threat hunting means that forensic tools today are not only used for after-the-fact analysis, but also for continuous monitoring and investigation in live environments. For instance, memory forensics might be employed on running systems to detect malware hiding only in RAM, and filesystem artifacts might be periodically

examined for signs of persistence mechanisms before any security breach is formally declared. This proactive use of forensic techniques is crucial in modern cybersecurity, as it enhances visibility and readiness beyond what reactive measures can achieve (deepwatch).

CASE STUDIES

GOOGLE : GRR RAPID RESPONSE

Background

GRR Rapid Response was developed to address the operational challenge of conducting digital forensics and incident response across large numbers of endpoints in enterprise environments. Traditional approaches such as manual collection, physical access to devices, and investigator-specific scripts often introduce delays, inconsistencies, and limited scalability when an incident affects many systems. GRR was designed as a centralized framework that supports remote, structured, and repeatable evidence acquisition, enabling responders to collect prioritized artifacts quickly while maintaining procedural consistency across investigations. This approach reflects a broader trend in modern DFIR: moving from ad-hoc evidence collection toward standardized, centrally managed workflows that can be executed reliably across diverse endpoint populations (Boutnaru, 2025).

Key Functionalities

GRR operates as a remote live-forensics framework built around a lightweight endpoint agent and a centralized server with an investigator interface. Functionally, it enables remote artifact collection and targeted file retrieval, collects system information and relevant endpoint state, and supports structured, repeatable "flows" so that the same evidence acquisition steps can be executed consistently across different machines. By centralizing orchestration, it reduces investigator dependence on ad-hoc scripts and supports parallel acquisition across many endpoints exactly the kind of workflow consistency your thesis emphasizes through standardized intake, integrity preservation, and court-defensible handling (Metz, 2024).

Ethical issues

The ethical risks are tightly linked to GRR's strength: remote visibility and collection power can become invasive without strong governance. Because investigators can pull artifacts remotely, there is a proportional challenge collecting more data than necessary can expose personal or irrelevant information and create privacy harms. Additionally, because remote collection is a powerful administrative capability, it raises insider-misuse risk unless access is strictly role-based, approvals are enforced, and every action is logged. Finally, because evidence is collected live and remotely, forensic defensibility can be questioned if integrity controls (hashing, logging, repeatable procedures) are weak, making chain-of-custody and authenticity harder to defend in legal or disciplinary proceedings an issue that matches your thesis focus on audit logs and standardized reporting.

Possible reasons for success

GRR tends to succeed when organizations already have mature endpoint management, a clear authorization model for incident response collection, and trained investigators who scope acquisitions tightly to case needs. Standardized "flows" also improve success because they reduce human error and prevent every analyst from improvising evidence handling differently, improving repeatability and accountability. However, GRR can fail (or deliver weaker outcomes) when endpoint deployment is incomplete, agents are unstable on diverse systems, or governance is unclear. Overcollection can trigger employee distrust, internal policy violations, or legal challenges, while weak training can lead to inconsistent or poorly documented collection decisions. In these cases, the tool's technical capability may exist, but the organization fails to realize its value because process, policy, and oversight are missing.

Impact on business

GRR improves investigation speed and scale, allowing incident responders to collect evidence across hundreds (or more) endpoints without waiting for physical device access. This reduces time-to-triage and time-to-containment, improves consistency across cases, and strengthens the reliability of investigative outcomes because acquisition becomes repeatable rather than analyst-dependent. In business terms, that translates into reduced downtime, lower incident-response labor cost, faster decision-making, and improved defensibility of internal findings.

Implications for Nepal Police tool design

This case study highlights that Nepal Police would benefit most from a forensic platform that supports rapid, remote, and standardized evidence collection across many endpoints, while still preserving legal defensibility. The tool should therefore implement a controlled "remote acquisition" capability (where permitted), with strict role-based authorization, explicit case assignment, and supervisor approval gates for high-impact actions (e.g., live memory capture, file retrieval). To prevent misuse and strengthen accountability, every action must generate tamper-evident audit logs and maintain a complete chain-of-custody record linked to a case ID and evidence ID. Operationally, GRR also implies the need for scalable deployment and reliability controls agent integrity verification, secure communications, and offline/low-bandwidth handling because Nepal has heterogeneous police infrastructure. Finally, the design must embed privacy-by-design mechanisms (minimization defaults, purpose limitation, and access transparency) so that investigative power does not create unethical surveillance practices.

PINDROP AUDIO FRAUD DETECTION AND CALLER VERIFICATION

Background

Pindrop emerged from the need to improve fraud detection and identity verification in contact-center environments where fraud attempts are frequent and manual verification processes are both slow and inconsistent. Traditional human-led caller authentication is vulnerable to social engineering and may vary widely depending on agent experience, workload, and adherence to policy. The core objective of Pindrop's approach is to transform audio interactions into structured risk signals that can support consistent decision-making at scale. This reflects a broader shift toward automated, data-driven verification models in environments where high volume makes purely manual methods unreliable and costly (Scott, 2023).

Key Functionalities

Pindrop's system analyzes call audio and interaction patterns to support fraud detection and caller verification. It extracts measurable features from voice and call characteristics and correlates them to generate risk assessments. The platform is commonly described as using techniques such as "toneprinting" and "phoneprinting," which capture behavioral and device/line-related signals associated with a call. These features can be used to flag anomalies, support authentication decisions, and provide consistent fraud scoring across many agents and locations. Operationally,

this allows organizations to embed automated verification into call workflows and reduce reliance on subjective judgments alone (Pindrop, 2025).

Ethical Issue

Audio-based verification introduces significant privacy and consent concerns because voice data can be sensitive and potentially identifying. Ethical deployment requires transparency about data use, minimization of unnecessary collection, and strong security controls for storage and access. Another key issue is fairness: model performance may vary based on accent, speech impairment, noise conditions, or line quality, leading to unequal treatment or higher false-positive rates for certain user groups. Misclassification harms are also ethically important; a legitimate caller incorrectly flagged as fraudulent may be denied service or subjected to excessive friction, which can undermine trust and create reputational risk.

Possible reasons for success

Success is more likely when the system is integrated into operations with clear policies, continuous model monitoring, and periodic updates to address evolving fraud tactics. Calibration and human review pathways are important to prevent over-reliance on automated scores. Failure can occur if models drift and are not maintained, if integration is poor and agents do not use the outputs consistently, or if false-positive rates produce unacceptable customer experience impacts. Governance failures such as weak consent practices, insecure retention, or inadequate compliance controls can also lead to legal and reputational consequences that reduce long-term viability.

Impact on Business

When effectively deployed, audio fraud detection can reduce fraud losses, improve authentication speed, and standardize decisions across agents. This can lower operational costs, shorten call durations, and improve overall efficiency. However, the business impact is sensitive to accuracy and fairness: high false positives can increase friction, reduce customer satisfaction, and raise volume of complaints. Therefore, sustainable value depends on balancing security benefits with user experience, transparency, and compliance requirements (Pindrop, 2024).

Implications for Nepal Police tool design

This case study indicates that audio forensics in Nepal Police should move beyond basic file metadata and include evidence-grade voice and call analysis features that support fraud, threat calls, impersonation, and social-engineering investigations. The tool design should include a structured audio workflow: automated extraction of metadata, signal preprocessing, and analytic modules such as spectrogram inspection, noise/room fingerprinting, DTMF decoding, and spoofing indicators (e.g., compression artifacts, replay signatures, synthetic voice cues). Because voice biometrics can be sensitive and error-prone, the tool should present results as probabilistic indicators with confidence levels, not absolute identity claims, and must encourage corroboration (device logs, telecom records, witness statements). To be court-ready, every derived artifact (features, extracted segments, decoded tones) should be hash-linked to the original audio, with reproducible parameters and an interpretable explanation section in the report. Overall, Pindrop implies that Nepal Police's integrated tool should treat audio as a first-class evidence type with standardized procedures, transparency, and safeguards against over-reliance on automated "match" outcomes.

META: DEEPFAKE DETECTION CHALLENGE (DFDC)

Background

The Deepfake Detection Challenge was launched to address the rapid growth of synthetic and manipulated media and the difficulty of detecting such content consistently at scale. Manual visual inspection is unreliable, particularly as manipulation techniques improve and as content spreads rapidly through digital platforms. DFDC was designed to provide a standardized dataset and evaluation framework that enables researchers and developers to test and compare detection approaches under common conditions. This initiative reflects a broader need for benchmark-driven progress in media forensics, where reproducibility and measurable performance are necessary for practical deployment (Meta, 2020).

Key Functionalities

DFDC provides a large corpus of manipulated and authentic media paired with ground-truth labels and evaluation methods. This enables supervised learning approaches for detection and supports comparative benchmarking across different models. The standardized format and metrics promote consistent measurement of detection performance and encourage development of scalable,

automated detection pipelines. In practice, DFDC-style benchmarking helps teams identify strengths and weaknesses of detection approaches under controlled conditions and supports iterative improvement of algorithms (Meta, 2020).

Ethical Issues

Deepfake detection research presents dual-use concerns: the same datasets and evaluation insights that improve detection can indirectly inform adversaries about how to evade detection. Consent and identity rights are also important, as synthetic media research raises concerns about the use of personal likeness and the normalization of manipulation tools. Another ethical issue is the impact of detection errors. False positives can incorrectly label genuine content as manipulated, harming individuals and restricting legitimate expression, while false negatives can allow harmful misinformation or impersonation to spread. Transparency is also ethically complex, as disclosure of detection methods can improve accountability but may increase evasion risk.

Possible reasons for success

DFDC is likely to be successful as a research benchmark when it produces evaluation conditions that represent real-world variation and when it enables comparable results across models. It can fail in practical translation if detection methods overfit to benchmark artifacts and do not generalize to new manipulation techniques, different compression conditions, or adversarial optimized deepfakes. Additionally, because manipulation techniques evolve rapidly, detection systems require continuous updating; static benchmark performance may not reflect operational effectiveness over time. Over-reliance on automated detection without contextual analysis and human review can also lead to policy and moderation errors.

Impact on Business

Improved deepfake detection can protect platform credibility, reduce harms from misinformation and impersonation, and support more consistent enforcement decisions. It may also reduce long-term operational burden by enabling scalable screening and prioritization for human review. However, detection errors can create reputational and legal risks, particularly where incorrect labeling affects public figures or sensitive content. Consequently, the overall business impact depends on the reliability of detection under real-world conditions and the presence of governance measures that manage false positives, appeals, and transparency obligations.

Implications for Nepal Police tool design

This case study shows that Nepal Police need a multimedia verification capability that is methodologically rigorous, not just tool-driven, because deepfake detection is adversarial and evolves quickly. The integrated tool should therefore adopt a design that separates evidence preservation (original file hashing, provenance capture, metadata extraction) from analysis and decision support (forgery indicators, model outputs), ensuring that automated detection never replaces forensic reasoning. DFDC implies the value of benchmarking and continuous evaluation: the tool should include a validation framework where detection modules are tested against known manipulated/authentic samples, with documented performance, limitations, and conditions under which accuracy drops (compression, low light, re-encoding, partial faces). Ethically and legally, the tool must implement strict policies to avoid misuse no public labeling without verification, controlled access to sensitive media, and clear reporting language that frames outputs as "indicators of manipulation" rather than definitive proof. Finally, DFDC suggests the tool should be modular and updateable, allowing Nepal Police to plug in improved detectors over time while keeping evidence handling, logging, and court-reporting consistent.

INTEGRATION

Integration in this research denotes the engineering of a single, defensible investigative environment that unifies disk, image, and audio analysis under one case-management and evidence-governance layer. Rather than treating each forensic capability as an independent script or isolated utility, the proposed system integrates them as coordinated modules that follow shared rules for evidence intake, integrity verification, storage, logging, and reporting. This integrated approach is intended to reduce tool switching overhead, minimize handling errors, and strengthen legal defensibility by making every step traceable and repeatable within a standardized workflow.

At the entry point, all evidence objects disk images, extracted files, standalone images, and audio recordings are processed through a standardized intake pipeline. The intake process assigns a unique Case ID and Evidence ID, captures collection metadata (source, collector identity, acquisition method, and timestamps where available), and computes cryptographic hashes to establish an integrity baseline. The same intake routine performs preliminary validation (file type detection, size checks, and safe storage location assignment) and writes a tamper-evident audit event, ensuring that every evidence type starts with the same chain-of-custody controls and documentation quality.

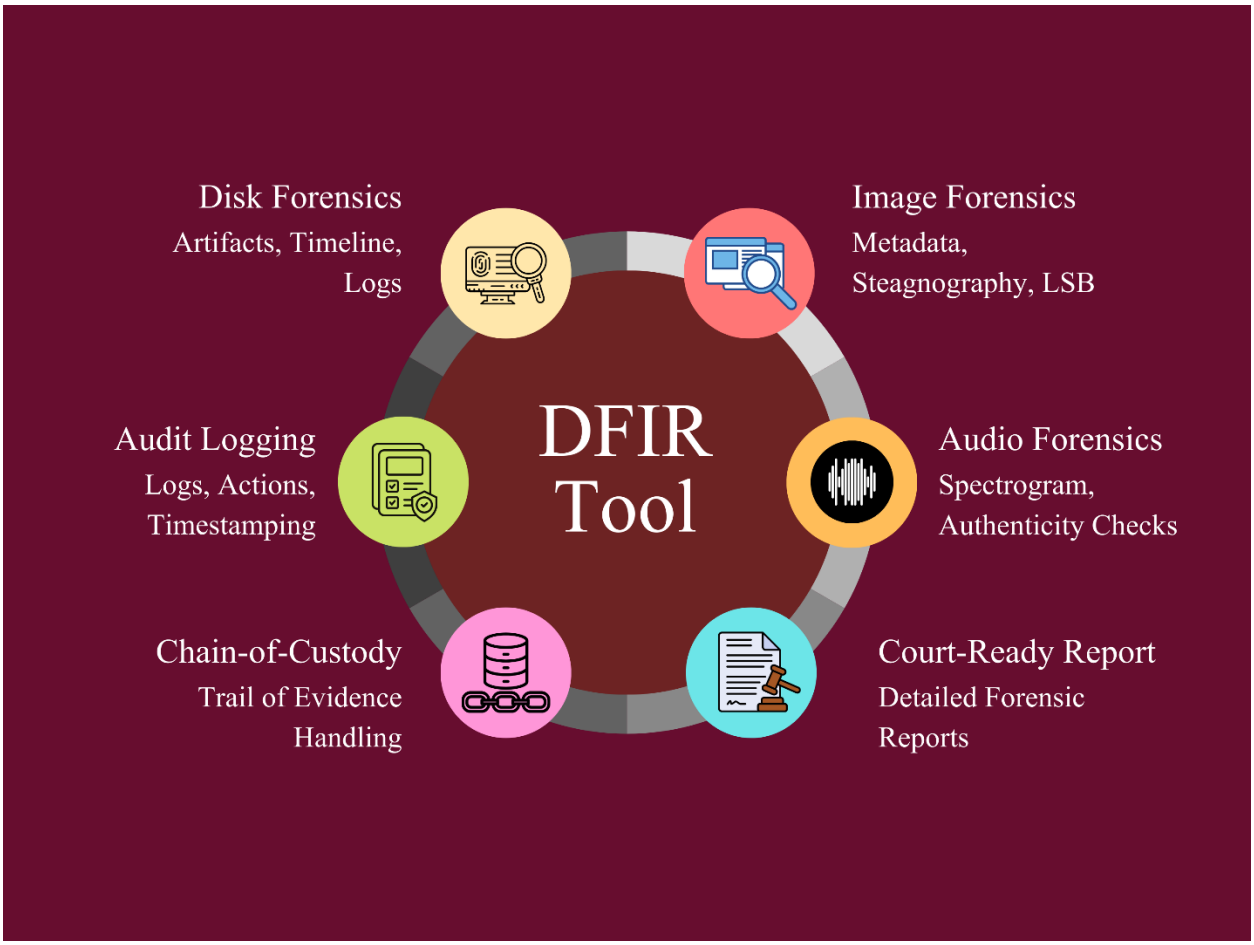


Figure 16: workflow of evidence intake and module routing

Once ingested, an orchestration layer classifies evidence and routes it to the appropriate analysis module while preserving a single investigative flow. The orchestration layer acts as the control plane: it triggers module pipelines, tracks execution status, manages dependencies, and enforces policy such as role-based permissions, approval gates for sensitive actions, and whether a module runs in fully automated or analyst-guided mode. This design allows the platform to remain modular while still behaving as one tool from the investigator's perspective, and it supports incremental expansion as additional forensic capabilities are introduced.

The disk forensics module is integrated primarily as a triage-and-artifact-extraction pipeline. It focuses on consistent recovery of high-value artifacts such as file traces, embedded objects, suspicious strings, and metadata indicators that support incident reconstruction. Where command-line utilities and forensic techniques are applied (e.g., strings analysis, file carving or embedded object identification, and metadata inspection), their outputs are captured and normalized into structured artifact records. Each record retains provenance fields such as method name, parameters, timestamps, and evidence linkage, which allows outputs to be reviewed, reproduced, and cited in a report without depending on informal investigator notes.

The image forensics module integrates both authenticity and concealment checks into the same workflow case. Metadata extraction and header inspection are performed first to recover timestamps, device or software traces, and geolocation tags where present. The module then applies forensic checks aligned with practical investigative needs, including pixel-level inspection methods (such as LSB/MSB analysis for steganography indicators), histogram or channel-based consistency checks, and extraction attempts using steganography utilities when justified by prior indicators. Where OCR is relevant (e.g., screenshots or photographed documents), text extraction is handled as an additional artifact type and stored with the same provenance and integrity tracking as other findings.

The audio forensics module is integrated as a sequence of signal-driven analyses that produce both analyst-friendly outputs (e.g., spectrograms) and machine-readable findings (e.g., detected tone sequences, decoded payloads, and anomaly markers). It supports decoding and covert-channel checks relevant to cyber investigations, such as DTMF detection, SSTV decoding, and Morse/T9 decoding, alongside steganography indicators including phase-based anomalies. Authenticity-oriented routines such as silence-gap analysis, splicing indicators, and background-noise consistency checks are recorded as structured findings so that an investigator can justify why a recording is likely authentic, suspicious, or requires deeper specialist examination.

A central integration mechanism results in normalization and correlation. Each module emits findings into a unified evidence store using a common data model (artifact class, source evidence reference, analysis timestamp, method, and summary). This enables cross-evidence queries such as building a consolidated case timeline by merging disk log timestamps, image metadata times, and audio anomaly markers; identifying contradictions (for example, an image creation time that does not align with disk activity); and clustering indicators of compromise across evidence types. By normalizing outputs, the platform supports consistent filtering, searching, and correlation regardless of which forensic module produced the finding.

Integration also extends to governance controls required when ethical hacking–inspired capabilities are introduced. Proactive actions used for hypothesis validation (for example, limited reconnaissance within an authorized scope or controlled validation of a suspected entry point) are treated as privileged workflows rather than default analysis steps. In the proposed design, these workflows require explicit authorization gates, role-based access control, and mandatory logging of actions, targets, and outcomes. This preserves the investigative value of adversarial reasoning while reducing the risk of misuse, mission creep, or privacy overreach, and it ensures that any proactive step remains auditable and defensible in oversight and legal review.

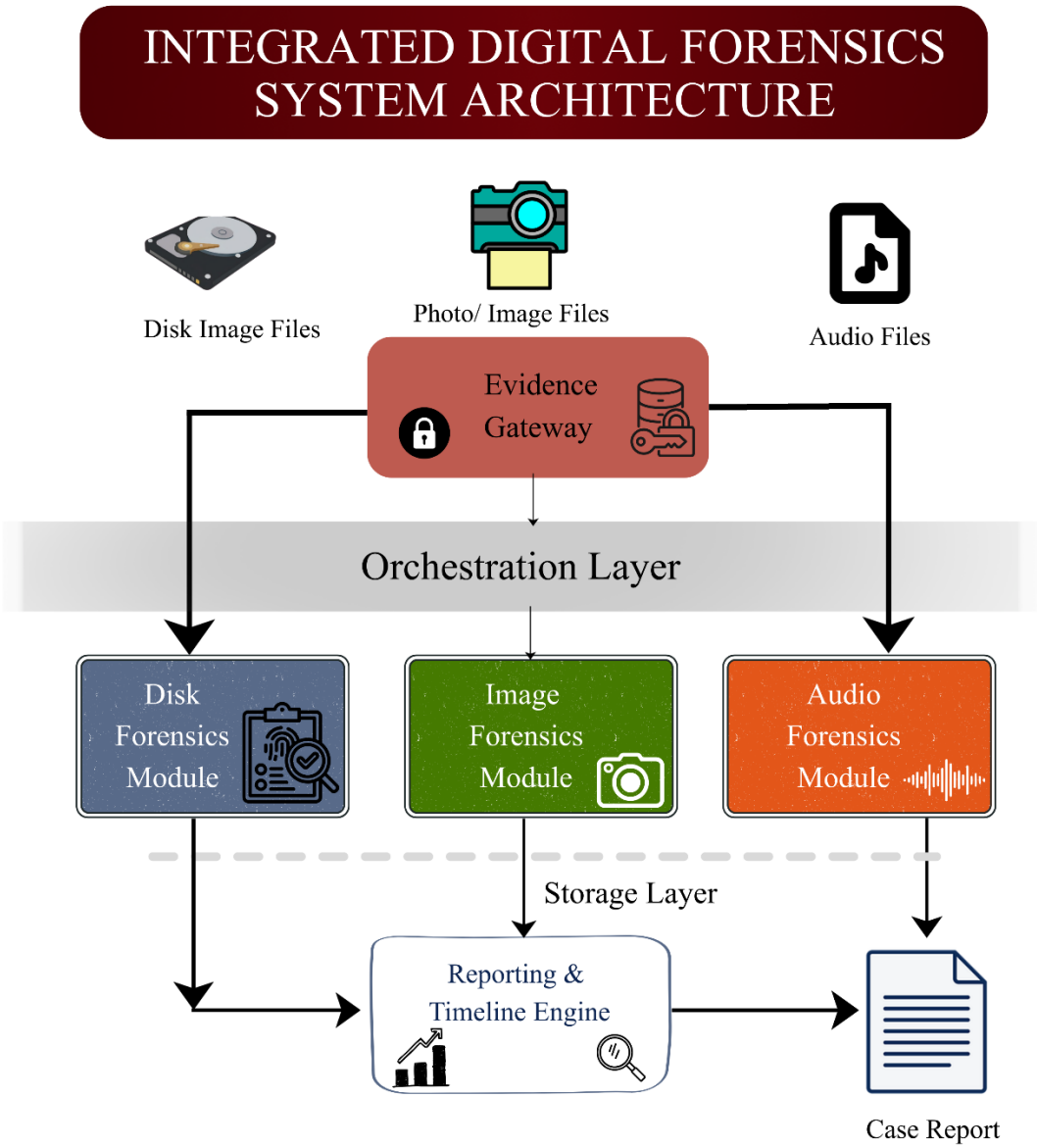


Figure 17: End-to-end integrated reporting and audit-ready pipeline.

Finally, all modules converge in a single reporting pipeline that generates standardized, court-ready documentation. Reports include evidence identifiers and hash values, a chronological activity log of analyst and system actions, the methods and parameters used for each analysis, key findings with provenance, and correlation views such as a consolidated timeline or indicator summary. Because reporting draws directly from the normalized evidence store and audit log, it reduces omission risk and supports repeatability. Overall, the integration approach operationalizes a unified workflow that improves consistency, traceability, and investigative efficiency across disk, image, and audio evidence in Nepal Police cybercrime investigations.

FINDINGS

How can a digital forensic tool integrate controlled ethical hacking features to improve evidence analysis and investigation efficiency in Nepal Police cyber cases?

The findings indicate that investigation efficiency is maximized when ethical hacking capabilities are not treated as standalone "offensive tools," but are operationalized as bounded, hypothesis-driven procedures within a unified digital forensic environment. In practice, the most consequential improvement emerges from integrating proactive validation steps such as limited, authorized enumeration of relevant services, verification of suspected attack paths, or controlled confirmation of persistence mechanisms directly into the same workflow used for evidence intake, analysis, and reporting. This integration reduces fragmentation, eliminates repeated manual documentation across tools, and ensures that every investigative action produces outputs that are traceable, reviewable, and legally defensible.

A further finding is that efficiency gains are strongly associated with standardization at the earliest stage of the process. When evidence is consistently registered using unique identifiers, accompanied by systematic metadata capture, and protected through cryptographic integrity verification, subsequent analysis becomes both faster and more reliable. This early standardization reduces the likelihood of procedural errors, supports repeatability across investigators and cases, and creates a stable foundation for automation. As a result, routine forensic tasks artifact extraction, indicator scanning, and timeline reconstruction can be performed with greater speed and lower variance, while maintaining the documentation quality expected in judicial settings.

The findings also show that the practical value of integration increases when analytic results are normalized into structured artifacts rather than reported as isolated tool outputs. Normalization enables cross-evidence correlation across heterogeneous sources (e.g., disk artifacts, image metadata, and audio anomaly indicators), facilitating a consolidated investigative narrative. This improves interpretability and reduces the cognitive and time burden of manually linking outputs from multiple tools. In effect, the integrated platform supports a shift from "artifact collection" toward "evidence-based reconstruction," enabling investigators to establish event sequences, validate hypotheses, and detect inconsistencies that may indicate anti-forensic manipulation.

Finally, the study suggests that the most academically defensible contribution of controlled ethical hacking in this context is its role in strengthening investigative reasoning rather than increasing technical aggression. When proactive steps are narrowly scoped and executed to test clearly stated hypotheses, they function as an extension of forensic analysis improving the completeness of evidence acquisition, reducing uncertainty, and supporting more timely decision-making. Thus,

the principal finding is that controlled ethical hacking enhances efficiency and evidential quality when embedded in an end-to-end forensic workflow that prioritizes standardization, automation, correlation, and defensible reporting.

What safeguards are required to ensure ethical, legal, and accountable use of ethical hacking features within a law enforcement forensic tool?

The findings demonstrate that the introduction of ethical hacking capabilities substantially increases ethical and legal risk due to their dual-use nature. Consequently, safeguards must be treated as system-enforced constraints rather than optional guidelines. The most critical safeguard is explicit authorization coupled with enforceable scope control. Proactive actions should be permitted only when there is a clearly documented legal basis and a defined operational boundary specifying the approved targets, permitted techniques, and time conditions. From an accountability standpoint, safeguards are strongest when the platform technically prevents actions outside this boundary rather than relying solely on user discretion.

A second major safeguard is rigorous access governance through role-based controls and the principle of least privilege. High-risk capabilities should be restricted to designated roles, and sensitive actions should require stronger control mechanisms such as supervisory approval or multi-party authorization for particularly intrusive procedures. This reduces the likelihood of misuse, minimizes mission creep, and ensures that advanced capabilities are deployed only when necessary and proportionate to investigative objectives. Importantly, such governance also supports institutional accountability by clarifying responsibility and enabling oversight.

A third safeguard finding is that accountability requires comprehensive, tamper-evident auditability across the entire evidence lifecycle. Every action evidence registration, analysis execution, parameter selection, and proactive validation should generate a time-stamped record that links the operator, method, target, and outcome. Audit trails should be protected against alteration and designed to support after-action review and courtroom scrutiny. This is essential because the defensibility of digital evidence often depends as much on demonstrable process integrity as on the technical discovery itself.

The findings further emphasize privacy-by-design as a necessary constraint in law-enforcement cyber investigation systems. Data minimization should be implemented so that collection and analysis are limited to what is relevant to the investigative hypothesis. Access should be tightly controlled, sensitive information should be protected through encryption and controlled disclosure pathways, and retention should be governed by lawful purpose and defined time limits. These measures reduce the risk of disproportionate intrusion into personal data and strengthen public trust by demonstrating that capability is balanced by restraint.

LIMITATIONS

One of the primary limitations of this project was the operational complexity of delivering a unified, court-ready forensic workflow in a resource-constrained law enforcement environment. Unlike mature digital forensic laboratories in well-resourced jurisdictions, Nepal Police cyber investigation units often operate with limited budgets, heterogeneous device ecosystems, uneven technical skill distribution, and fragmented tooling. These conditions make it difficult to design a single platform that remains usable for investigators with varying proficiency while also meeting strict evidentiary expectations. Even when an integrated workflow is defined, practical constraints such as limited hardware for acquisition/analysis, inconsistent access to updated toolchains, and reliance on manual steps for documentation can reduce consistency and slow investigations. As a result, certain advanced capabilities (e.g., handling strong encryption, anti-forensic artifacts, and sophisticated malware traces) may remain only partially achievable for non-specialist users, requiring escalation to highly trained personnel and limiting the uniform effectiveness of the proposed framework across all case types.

Another significant limitation was the restricted scope of validation and measurement, since the study emphasized framework design and feasibility rather than full operational deployment and longitudinal testing within active investigations. Because the project did not include sustained field implementation across multiple real cases, it could not robustly quantify improvements such as reduced turnaround time, increased evidence recovery rates, improved chain-of-custody compliance, or higher prosecution success rates. Additionally, realistic constraints such as investigator workload, courtroom scrutiny, and cross-unit coordination were not continuously stress-tested in live settings. This limitation also affects the generalizability of the results: while the framework is tailored for developing-country policing contexts, the real impact may vary depending on institutional policy maturity, availability of trained personnel, infrastructure reliability, and legal readiness for digital evidence handling.

A further limitation involved legal, ethical, and governance constraints associated with integrating proactive (ethical hacking–aligned) capabilities into a forensic workflow. While such capabilities can strengthen investigative readiness, they require strict authorization controls, audit logging, and clear boundaries to prevent misuse, rights violations, or evidentiary contamination. In practice, evolving cybercrime laws, differing interpretations of admissibility standards, and limited institutional oversight capacity can constrain what functions are permissible and how evidence must be collected, stored, and presented. Maintaining privacy compliance especially when dealing with personal devices, communications, or third-party data adds additional restrictions. These constraints may limit the extent to which proactive modules can be used consistently across jurisdictions or cases, and they reinforce the necessity of human supervision, documented approvals, and policy alignment to ensure the framework remains legally defensible.

Finally, the project faced limitations related to automation reliability and investigative “noise”, particularly when standardizing reporting and decision-making across diverse evidence types

(disk, image, audio, and network artifacts). Automated routines can accelerate triage, extraction, and reporting, but they can also generate false positives, incomplete artifact interpretation, or misleading correlations when evidence is degraded, intentionally manipulated, or context dependent. This is especially relevant for multimedia forensics, where compression artifacts, steganography, deepfake-like manipulation, or partial metadata can complicate definitive conclusions. Consequently, the system still depends on investigator judgment for verification, interpretation, and courtroom explanation. The continuous need for manual validation and iterative tuning highlights a broader limitation: automation can improve speed and consistency, but it cannot fully replace expert reasoning in complex forensic reconstruction and legal testimony.

FUTURE WORK AND RECOMMENDATIONS

Future research should prioritize rigorous field validation of the integrated forensic tool in realistic law-enforcement conditions. This includes controlled pilot deployments across multiple policing contexts (urban cyber units and resource-constrained regional posts) to quantify improvements in investigation time, evidence completeness, analyst workload, and report quality. Future work should also establish a structured evaluation framework using standard digital forensics performance measures such as reproducibility of findings, false positive/negative rates for automated detections, and the consistency of conclusions across investigators with different skill levels so that the tool's effectiveness can be demonstrated beyond proof-of-concept implementation.

A second direction is strengthening the tool's capability against contemporary anti-forensic and privacy-preserving techniques. This includes deeper support for encrypted containers and mobile artifacts, robust memory/volatile data acquisition workflows (where legally permissible), and enhanced detection of manipulation in multimedia evidence through advanced authenticity checks. Future work should further develop correlation features such as timeline fusion, cross-evidence entity linking, and case-to-case pattern analysis to support proactive intelligence generation while maintaining strict governance controls. Additionally, expanding interoperability with widely used forensic suites and standard formats would improve practical adoption by enabling seamless import/export of evidence and results across institutional ecosystems.

Finally, future research should advance the governance and legal defensibility of controlled ethical-hacking workflows. This includes designing formal "scope objects" that encode legal authority, target constraints, and permitted techniques; implementing stronger supervisory approval mechanisms for sensitive actions; and producing audit logs that are not only comprehensive but also cryptographically verifiable. Complementary work should examine organizational change factors training, usability, and procedural standardization to ensure the solution remains effective across diverse user profiles and evolves in step with both operational needs and legal requirements.

It is recommended that law-enforcement agencies adopt an end-to-end standard operating procedure for digital evidence handling that is enforced by the tool itself, beginning with structured evidence intake, cryptographic integrity verification, and consistent chain-of-custody documentation. Embedding these controls into default workflows will improve consistency, reduce avoidable errors, and strengthen courtroom defensibility. Agencies should also prioritize modular adoption: initially deploying core evidence management and automated forensic pipelines (disk/image/audio) before enabling privileged ethical-hacking features, thereby reducing operational risk during early rollout and allowing investigators to build confidence in the platform.

For ethical hacking–inspired capabilities, the recommendation is to implement a strict governance model based on explicit authorization, scope limitation, and least-privilege access. Proactive actions should be permitted only as hypothesis-testing procedures within defined legal and operational boundaries, with mandatory justification fields and supervisory approval for high-impact steps. Comprehensive auditability should be treated as non-negotiable: all actions and outputs must be traceable to operator identity, time, evidence object, and method parameters, with protections against log tampering. These measures reduce misuse potential and support oversight, transparency, and public trust.

From a capacity-building perspective, agencies should invest in role-based training and usability refinement to accommodate varied digital literacy levels. Training should focus not only on tool operation but also on evidential reasoning, privacy-by-design principles, and defensible reporting practices. Finally, it is recommended to establish a continuous improvement cycle in which feedback from investigators, prosecutors, and forensic reviewers is used to refine automation rules, update detection signatures, improve reporting templates, and ensure alignment with evolving cybercrime patterns and legal standards.

CONCLUSION

This thesis has shown that strengthening cybercrime investigations in a law-enforcement context requires more than adding additional forensic utilities; it requires an integrated, governance-driven approach that improves both investigative efficiency and evidential defensibility. By conceptualizing a unified toolchain that standardizes evidence intake, preserves integrity through cryptographic verification, and maintains traceable chain-of-custody and audit logs, the study demonstrates how routine digital forensic work can become more consistent, faster, and less dependent on individual investigator experience. The integration of disk, image, and audio forensic capabilities within a single workflow further supports cross-evidence correlation and timeline reconstruction, enabling investigators to move from isolated artifact extraction toward coherent event reconstruction and case-ready reporting.

The thesis also establishes that ethical hacking inspired capabilities can be academically and operationally justified when they are implemented as narrowly scoped, hypothesis-driven investigative procedures rather than general offensive functions. When such proactive actions are embedded within the same forensic governance layer requiring explicit authorization, enforceable scope limitation, least-privilege access, and tamper-evident auditability they can enhance investigative reasoning without compromising legality, ethics, or public trust. Overall, the study concludes that a well-governed, modular, and auditable integrated forensic platform offers a practical pathway for improving cybercrime investigation capability, strengthening evidence integrity, and supporting court-ready outcomes in environments that face fragmented tools, evolving adversary techniques, and resource constraints.

BIBLIOGRAPHY

Sunde, N. (2019) Https://www.sciencedirect.com/science/article/abs/pii/S1047847720300046?via=ihub. Available at: https://www.med.upenn.edu/pmi/events/https-www-sciencedirect-com-science-article-abs-pii-s1047847720300046-via-3dihub (Accessed: 30 December 2026).

Paudel, A. (2025) Pentester Nepal 12th Anniversary CTF Writeup. Available at: https://medium.com/@7077ashwin7/pentester-nepal-12th-anniversary-ctf-writeup-68868278c9b3 (Accessed: 04 February 2026).

Vance, A. and Siponen, M. (2010) (PDF) neutralization: New insights into the problem of Employee Information Systems Security policy violations. Available at: https://www.researchgate.net/publication/279550478_Neutralization_New_Insights_into_the_Problem_of_Employee_Information_Systems_Security_Policy_Violations (Accessed: 10 February 2026).

Best practices for digital evidence collection. Available at: https://www.swgde.org/wp-content/uploads/2025/07/2025-06-30-Best-Practices-for-Digital-Evidence-Collection-18-F-002-2.0.pdf (Accessed: 13 January 2026).

Davis, F.D. (no date) Parsmodir. Available at: https://parsmodir.com/wp-content/uploads/2018/11/TAM-Davis-1989.pdf (Accessed: 1 February 2026).

Hallberg, J. (2017) The theory of planned behavior and information security ..., Journal of Computer Information Systems. Available at: https://sommestad.com/teodor/papers/Sommestad,%20Karlz%C3%A9n,%20Hallberg%20-%202019%20-%20The%20Theory%20of%20Planned%20Behavior%20and%20Information%20Security%20Policy%20Compliance.pdf (Accessed: 10 February 2026).

Liu, F. and Mikko Siponen (2021) (PDF) Protection Motivation Theory in Information Systems Security Research: A review of the past and a road map for the future, Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. Available at: https://www.researchgate.net/publication/351178459_Protection_Motivation_Theory_in_Information_Systems_Security_Research_A_Review_of_the_Past_and_a_Road_Map_for_the_Future (Accessed: 10 January 2026).

Dang, H. (2006, August). NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

Swgde.org. (n.d.). swgde.org | 520: Web server is returning an unknown error. https://www.swgde.org/documents/published-complete-listing/18-f-002-best-practices-for-digital-evidence-collection/

Gong, C. (2020, December). Detecting fingerprints of audio steganography software. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S2665910720300219

Lu, Y. (2014). Investigating Steganography in Audio Stream for Network Forensic Investigations: Detection & Extraction. Tuwhera Open Repository :. https://openrepository.aut.ac.nz/server/api/core/bitstreams/fbe702cf-c337-4600-b7d1-c349557a0e30/content

Five case studies with digital evidence in corporate investigations. (2025, March 3). Control Risks | Global Risk Consultancy. https://www.controlrisks.com/our-thinking/insights/five-case-studies-of-interest-to-corporate-investigators

Sarmah, D. K. (2024, January). Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. ResearchGate . https://www.researchgate.net/publication/377628138_Steganography_and_steganalysis_for_digital_image_enhanced_Forensic_analysis_and_recommendations

OneMain financial case study. (2025). Amazon Web Services, Inc. https://aws.amazon.com/solutions/case-studies/onemain-financial-aws-sfn-case-study/

Grobler, M. (n.d.). Digital Forensic Readiness: Are We There Yet? Welcome to University of Warwick. https://warwick.ac.uk/fac/sci/dcs/people/chang-tsun_li/publications/ieee_sp_dfr_are_we_there_yet.pdf

Owa, M. (2023, April 25). Desk research: Definition, types, application, pros & cons. Create Free Online Forms & Surveys in 2 Mins | Formplus. https://www.formpl.us/blog/desk-research-definition-types-application-pros-cons

Karl, T. (2022, September 21). Digital forensics: Think like a hacker. New Horizons. https://www.newhorizons.com/resources/blog/digital-forensics-think-like-a-hacker

Klasen, L. (2024, September). The invisible evidence: Digital forensics as key to solving crimes in the digital age. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0379073824002147

Proactive threat hunting. (2025, September 4). Deepwatch. https://www.deepwatch.com/glossary/proactive-threat-hunting

Olatona, R. Volatility is an essential DFIR tool-here's why, Volatility Is an Essential DFIR Tool-Here's Why. Available at: https://www.boozallen.com/insights/cyber/tech/volatility-is-an-essential-dfir-tool-here-s-why.html (Accessed: 28 December 2026).

Five case studies with digital evidence in corporate investigations (2019) Control Risks. Available at: https://www.controlrisks.com/our-thinking/insights/five-case-studies-of-interest-to-corporate-investigators (Accessed: 06 February 2026).

Acharya, S. (2021) (PDF) security threats and legalities with digitalization in Nepal. Available at: https://www.researchgate.net/publication/358239832_Security_Threats_and_Legalities_with_Digitalization_in_Nepal (Accessed: 10 January 2026).

Nasana. (1970, January 1). Nepal police brings in use digital forensics technology. The Himalayan Times. https://thehimalayantimes.com/kathmandu/nepal-police-brings-in-use-digital-forensics-technology

Malla, A. and Timalsena, B. (2022) A study on cyber crime cases in Nepal. Available at: https://giwmscdnone.gov.np/media/files/22071352423-Final%20A%20Study%20on%20Cyber%20Crime%20Cases%20in%20Nepal,%202022-10_u52gj23.pdf (Accessed: 15 January 2026).

Nepal police brings digital forensic lab in use. (2015, December 10). myRepublica - The New York Times Partner, Latest news of Nepal in English, Latest News Articles. https://myrepublica.nagariknetwork.com/news/nepal-police-brings-digital-forensic-lab-in-use

Chaudhary, Dr.N. (2023) The need for Data Protection Law in Nepal: Securing citizen's rights in the Digital age, Kathmandu School of Law Review. Available at: https://kslreview.org/index.php/kslr/article/view/2225 (Accessed: 13 January 2026).

Government establishing national cyber security centre. (n.d.). GorakhaPatra. https://risingnepaldaily.com/news/40784

Chaudhary, B. (2023) Nepal's Digital Security: Exploring the specialised role of Cyber Security Force, OnlineKhabar English News. Available at: https://english.onlinekhabar.com/nepal-cyber-security-data-protection.html (Accessed: 02 January 2026).

Nepal, O. K. (2025, August 5). Understanding the growth of cybercrime in Nepal. Open Knowledge Nepal. https://oknp.org/blogs/understanding-the-growth-of-cybercrime-in-nepal

Medhacorplaw. (2025, November 8). Cybercrime lawyers Nepal: Medha law and partners. MedhaCorpLaw. https://medhacorplaw.com/cybercrime-lawyers-nepal-medha-law-and-partners/

Chaurasia, D. (2023) Nepal Digital Forensics Market (2025-2031): Revenue & Analysis, Nepal Digital Forensics Market (2025-2031) | Revenue & Analysis. Available at: https://www.6wresearch.com/industry-report/nepal-digital-forensics-market (Accessed: 05 January 2026).

(n.d.). GRR Rapid Response - Live forensics, at scale. https://www.grr-response.com/

Nepal police brings in use digital forensics technology. (n.d.). https://www.newsabhiyan.com.np/. https://www.newsabhiyan.com.np/news-details.php?nid=16969

Sigdel, S. (2023) Government eyes on internet monitoring, The Annapurna Express. Available at: https://theannapurnaexpress.com/story/45435/ (Accessed: 10 February 2026)

What is GRR? — GRR documentation. (n.d.). GRR on GitHub — GRR documentation. https://grr-doc.readthedocs.io/en/v3.2.1/what-is-grr.html

Boutnaru, S. (2025) The windows forensic journey — GRR (google rapid response) | by Shlomi Boutnaru, ph.d. | medium. Available at: https://medium.com/@boutnaru/the-windows-forensic-journey-grr-google-rapid-response-66c946aa8fbe (Accessed: 10 February 2026).

What is GRR? — GRR documentation. (n.d.). GRR on GitHub — GRR documentation. https://grr-doc.readthedocs.io/en/latest/what-is-grr.html

Collin. (n.d.). Google rapid response (GRR). The Brain Dump!. https://itscollin.github.io/articles/howtogrr.html

Sindhuja. (2021, December 19). Google rapid response tool for remote live forensics. Security Investigation - Be the first to investigate. https://www.socinvestigation.com/google-rapid-response-tool-for-remote-live-forensics/

Google rapid response - Build process. (2022, December 13). TechAnarchy. https://www.techanarchy.net/google-rapid-response-build-process/

Carry out investigations remotely using containerized GRR. (n.d.). JYVSECTEC. https://jyvsectec.fi/en/2020/05/carry-out-investigations-remotely-using-containerized-grr/

Metz, J. (2024) Life of a GRR message. Available at: https://osdfir.blogspot.com/2024/01/life-of-grr-message_23.html (Accessed: 14 January 2026).

Scott, R. (2023, April 25). Introducing Pindrop: The ultimate fraud detection solution. CX Today. https://www.cxtoday.com/contact-center/introducing-pindrop-ultimate-fraud-detection-solution/

Pindrop anti-fraud & authentication solutions. (2025, March 3). Cybersecurity Excellence Awards. https://cybersecurity-excellence-awards.com/candidates/pindrop-anti-fraud-authentication-solutions-2025/

Stewart, A. (2025, June 23). Best voice AI for fraud detection workflows: 2025 e-Commerce security guide. Best AI Receptionist Service - 24/7 Phone Support from $29 | Dialzara. https://dialzara.com/blog/ai-voice-tools-for-fraud-detection-in-e-commerce

Sharma, S. (2024) Pindrop claims to detect AI audio deepfakes with 99% accuracy | venturebeat. Available at: https://venturebeat.com/ai/pindrop-claims-to-detect-ai-audio-deepfakes-with-99-accuracy (Accessed: 28 December 2026).

Schwartz, E.H. (2024) Pindrop launches real-time audio Deepfake Detection Tool Pindrop Pulse, Voicebot.ai. Available at: https://voicebot.ai/2024/02/21/pindrop-launches-real-time-audio-deepfake-detection-tool-pindrop-pulse/ (Accessed: 10 January 2026).

Pindrop. (2024, August 15). Pindrop launches pulse inspect: A cutting-edge solution to combat Deepfakes and the spread of misinformation. PR Newswire: press release distribution, targeting, monitoring and marketing | PR Newswire. https://www.prnewswire.com/news-releases/pindrop-launches-pulse-inspect-a-cutting-edge-solution-to-combat-deepfakes-and-the-spread-of-misinformation-302222695.html

Cliff S. (2018, March 26). ShopDirect set to use AI to detect fraud on phone calls. ComputerWeekly.com. https://www.computerweekly.com/news/252437556/ShopDirect-set-to-use-AI-to-detect-fraud-on-phone-calls

PR Newswire. (2024, February 20). Pindrop launches revolutionary audio Deepfake detection solution to bring trust back to remote communication. AiThority. https://aithority.com/technology/pindrop-launches-revolutionary-audio-deepfake-detection-solution-to-bring-trust-back-to-remote-communication/

ATLANTA (2026) Pindrop now powers nice CXone and CX AI platform with real-time fraud and Deepfake Defense, The Hamilton Spectator. Available at: https://www.thespec.com/globenewswire/pindrop-now-powers-nice-cxone-and-cx-ai-platform-with-real-time-fraud-and-deepfake/article_bfceda20-f268-5453-992e-667b77a4b3c6.html (Accessed: 10 February 2026).

CanvasBusinessModel. (2024, December 19). How does Pindrop company work? Business Model Canvas Templates. https://canvasbusinessmodel.com/blogs/how-it-works/pindrop-how-it-works

Hersey, F. (2022, July 22). Shrinking commands, ageing voices and microphones everywhere: Pindrop's future for voice biometrics. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/202207/shrinking-commands-ageing-voices-and-microphones-everywhere-pindrops-future-for-voice-biometrics

Deepfake detection using metadata. (n.d.). Meegle - Free Visual Workflow & Project Management Tool. https://www.meegle.com/en_us/topics/deepfake-detection/deepfake-detection-using-metadata

Deepfake detection using deep feature stacking and meta-learning. (n.d.). PMC Home. https://pmc.ncbi.nlm.nih.gov/articles/PMC11636820/

Client challenge. (2025, June 4). Scribd to the world's documents. https://www.scribd.com/document/913146417/MEViT-Generalization-of-Deepfake-Detection-With-Meta-Learning-EfficientNet-Vision-Transformer

Burt, C. (2026, February 4). Deepfakes detection increasingly vital to law enforcement, fraud defense alike. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/202602/deepfakes-detection-increasingly-vital-to-law-enforcement-fraud-defense-alike

Zotov, S. and Dremliuga, R. (2020) Survey on reinforcement learning based efficient routing in SDN. Available at: https://dl.acm.org/doi/fullHtml/10.1145/3426020.3426072 (Accessed: 07 January 2026).

Adaptive meta-learning for robust Deepfake detection: A multi-agent framework to data drift and model generalization. (n.d.). arXiv.org e-Print archive. https://arxiv.org/html/2411.08148v1

Mingabire. (2021, June 17). Detecting the models behind Deepfakes. Meta Newsroom. https://about.fb.com/news/2021/06/detecting-the-models-behind-deepfakes/

Laurenson, T. (2017) Research portal. Available at: https://ourarchive.otago.ac.nz/esploro/outputs/doctoral/Automated-Digital-Forensic-Triage-Rapid-Detection/9926479486701891 (Accessed: 19 January 2026).

Froklage, P. (2025, May 14). Digital forensics tools: The ultimate guide (2024). Magnet Forensics. https://www.magnetforensics.com/blog/digital-forensics-tools-the-ultimate-guide-2024/

Fox, N. (2023) How to use volatility for memory forensics and analysis, Varonis. Available at: https://www.varonis.com/blog/how-to-use-volatility (Accessed: 15 January 2026).

(2023) Volatility. what is volatility? | by Career Technology Cyber Security India Pvt. ltd. | medium. Available at: https://medium.com/@careertechnologymiraroad/volatility-978e32316616 (Accessed: 28 December 2026).

Hacktivities (2021) Forensics — memory analysis with volatility | by hacktivities | infosec write-ups. Available at: https://infosecwriteups.com/forensics-memory-analysis-with-volatility-6f2b9e859765 (Accessed: 10 February 2026)

Understand audio data. (2025, July 23). GeeksforGeeks. https://www.geeksforgeeks.org/nlp/understand-audio-data/

Introduction to audio analysis – Mira. (n.d.). https://doc.flux.audio/mira/Introduction_Analysis.html

Shaking the cobwebs CTF part one – Audio analysis. (2024, January 21). The eDiscovery Channel. https://ediscoverychannel.com/2024/01/22/shaking-the-cobwebs-ctf-part-one-audio-analysis/

Poudel, S. (2022) Help.me file to Audio Spectrogram : CTF Learn | by subeshpoudel | medium. Available at: https://medium.com/@subeshpoudel20/help-me-file-to-audio-spectrogram-ctf-learn-ecb7ab6d0235 (Accessed: 10 February 2026).

Ekira (2025) Audio Steganography CTF WRITEUP. steganography is the practice of hiding… | by Ekira M. | Medium. Available at: https://ekira.medium.com/audio-steganography-ctf-writeup-f9703923abed (Accessed: 10 February 2026).

OSIRIS Lab & CTFd LLC. (n.d.). Metadata. CTF Handbook. https://ctf101.org/forensics/what-is-metadata/

Khan, S. A. (2025, August 22). How to find hidden messages in JPEGs: A beginner's guide to CTF steganography challenges from KUET's cyber security seminar. Blog | Hidden Investigations - Cybersecurity Research & Vulnerability Disclosure. https://hiddeninvestigations.net/blog/how-to-find-hidden-messages-in-jpegs-a-beginners-guide-to-ctf-steganography-challenges-from-kuets-cyber-security-seminar

Client challenge. (n.d.). Client Challenge. https://www.slideshare.net/slideshow/image-png-forensic-analysis/69352209

Hard disk analysis methodology. (n.d.). About Me | jigsaw@jigsaw. https://zach-wong.gitbook.io/easy-reads/forensics-ctf-methodology/hard-disk-analysis-methodology

Mahaloz. (n.d.). Introduction to image analysis. Getting Started - CTF Wiki EN. Retrieved February 10, 2026, from https://ctf-wiki.mahaloz.re/misc/picture/introduction/

Kelcy66. (2019, May 16). The embedded world – Embedded system and hacking tutorial. https://embeddedworld.home.blog/2019/05/16/hacking-walkthrough-ctf-challenge/

FourOctets (2018) CTF tidbits: Part 1 — steganography | by fouroctets | medium. Available at: https://medium.com/@FourOctets/ctf-tidbits-part-1-steganography-ea76cc526b40 (Accessed: 10 February 2026).

APPENDIX

Github Link

https://github.com/ashwin7077/Digital-Forensic-Automation-Tool

Project Plan

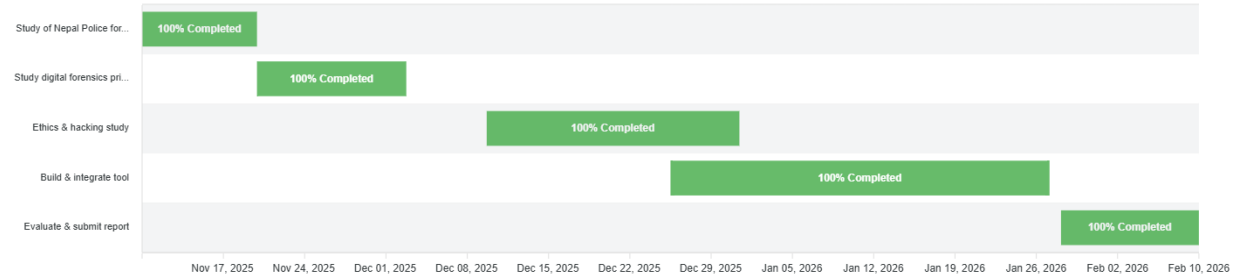


Figure 18: Project Plan

Swot Analysis

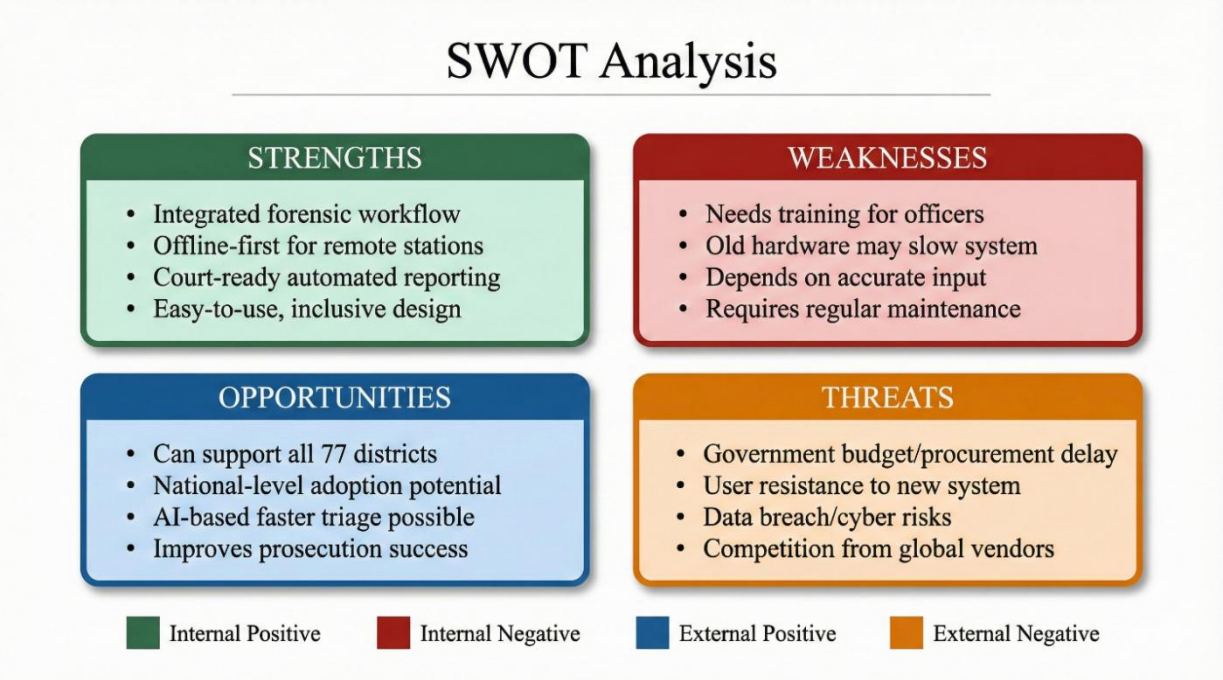


Figure 19: Swot Analysis

Risk Log

Risk Log

Id	Risk Name	Occurrence	Impact	Plan B / Mitigation
R1	Scope creep (too many feature)	High	High	Define MVP early; prioritize core disk/image/audio workflows; keep advanced features optional; freeze features before final weeks.
R2	Limited time	Medium	High	Use weekly milestones; write report alongside development; allocate final period for testing + report only.
R3	Tool integration failure	Medium	High	Build common input/output format from start; test integration after each major feature; keep modules loosely coupled.
R4	Inaccurate or unreliable forensic results	Medium	High	Validate with known test datasets; cross-check outputs with trusted tools; add unit tests and repeatability checks.
R5	Evidence integrity issues	Low	High	Implement hash verification at ingestion and export; maintain audit logs; prevent overwriting originals; keep immuttable case folder structure.
R6	Lack of suitable datasets for evaluation	Medium	High	Use public forensic datasets + synthetic samples; generate controlled test files for stego/splicing/DTMF cases.
R7	Ethical/legal misunderstanding of "ethical hacking" features	Medium	High	Add scope boundaries in design; document authorization requirement; restrict high-risk functions; maintain.
R8	Performance issues on limited hardware	Medium	Medium	Optimize by processing in stages; limit heavy analysis to selected evidence; provide progress indicators and timeouts.
R9	Dependency/installation problems	Medium	Medium	Use requirements file; containrize or provide setup script; document versions and fallback tools.

Figure 20: Risk Log

Ethical Form

Risk Research Ethics Approval

Project Information

Project Ref	4
Full Name	Aswin Paudel
Faculty	Faculty of
Department	School of
Supervisor	Manoj Shrestha
Module Code	ST6047CEM
EFAAF Number	EFAAF
Project Title	Design and Implementation of an Ethical Hacking-Based Digital Forensic Tool for Proactive Cyber Threat Investigation and Evidence Analysis in Nepal Police Operations
Date(s)	Date(s)
Created	Created

Project Summary

This research focuses on designing and implementing a Python-based automated digital forensic analysis tool for Nepal Police operations, capable of processing image, audio, and memory (RAM) evidence with full chain of custody documentation. The tool employs multiple forensic techniques including steganography detection, metadata extraction , image decomposition analysis, audio spectral analysis (spectrogram, DTMF, SSTV, Morse code), and volatile memory forensics using Volatility framework for malware detection, process analysis, and credential extraction. All evidence undergoes cryptographic hash verification before and after analysis to maintain integrity, with automated generation of comprehensive forensic reports. The modular architecture ensures reproducibility, scalability, and compliance with forensic standards while addressing Nepal's specific cybercrime investigation requirements under the Electronic Transactions Act 2063. This tool will enhance Nepal Police's digital forensic capabilities by automating complex analysis workflows, reducing investigation time, and ensuring legally admissible evidence handling for court proceedings.

Names of Co-Investigators and their organisational affiliation(place of study /employer)	None
Is this project externally funded?	No
Are you required to use a Professional Code of Ethical Practice appropriate to your discipline?	No
Have you read the Code?	No

Project Details

What are the aims and objectives of the project?	Aim: To design and implement an ethical hacking-based digital forensic tool for proactive cyber threat investigation and evidence analysis in Nepal Police operations. Objectives: 1. To learn and understand digital forensic principles, evidence preservation techniques, chain of custody protocols, and cryptographic hash verification methods for maintaining evidence integrity in cybercrime investigations. 2. To learn and understand various forensic analysis techniques including steganography detection, metadata extraction, audio spectral analysis, and volatile memory forensics applicable to image, audio, and RAM evidence types. 3. To learn and understand Nepal's cybercrime legal framework, including the Electronic Transactions Act 2063, ethical hacking guidelines, and admissibility requirements for digital evidence in law enforcement operations. 4. To develop a modular Python-based automated digital forensic tool with integrated analysis capabilities for multiple evidence types, automated hash verification, and comprehensive report generation functionality tailored for Nepal Police requirements. 5. To create a comprehensive thesis report documenting the tool's design, implementation, testing, validation, and practical applicability for enhancing Nepal Police cybercrime investigation capabilities, and submit for academic evaluation.
Explain your research design	It's a hybrid approach using both secondary and primary research.
Outline the principal methods you will use	Secondary Research: Literature review, analysis of existing forensic tools, study of Nepal's cyber-

	crime legal framework, examination of digital forensic standards and best practices Primary Research: Tool development in Python, controlled testing with synthetic evidence, performance evaluation and validation, hash verification testing, automated report generation
Are you proposing to use a validated scale or published research method / tool?	No
Does your research seek to understand, identify, analyse and/or report on information on terrorism or from terrorist organisations, require access to terrorist groups or those convicted of terrorist offences or relate to terrorism policies in other international jurisdictions?	No
Does your research seek to understand, identify, analyse and/or report on information for other activities considered illegal in the UK and/or in the country you are researching in?	No
Are you dealing with Secondary Data? (e.g. sourcing info from websites, historical documents)	Yes
Is this data publicly available?	Yes
Could an individual be identified from the data? e.g. identifiable datasets where the data has not been anonymised or there is risk of re-identifying an individual	No
Are you dealing with Primary Data involving people? (e.g. interviews,questionnaires, observations)	No

Are you dealing with personal data?	No
Please specify what personal data you will be collecting.	
Are you dealing with sensitive data (special category data)?	No
Will the Personal or Sensitive data be shared with a third party?	No
Will the Personal or Sensitive data be shared outside of the European Economic Area(EEA)?	No
Is the project solely desk based? (e.g. involving no laboratory, workshop or offcampus work or other activities which pose significant risks to researchers or participants)	Yes
Will the data collection, recruitment materials or any other project documents be in any language other than English?	No
Are there any other ethical issues or risks of harm raised by the study that have notbeen covered by previous questions?	No

DBS (Disclosure & Barring Service) formerly CRB (Criminal Records Bureau)

Question	Yes	No
Does the study require DBS (Disclosure & Barring Service) checks?		×
If YES, Please give details of the level of check, serial number, date obtained andexpiry date (if applicable)		
If NO, does the study involve direct contact by any member of the research team with children or young people under 18 years of age?		×
If NO, does the study involve direct contact by any member of the research team with adults who have learning difficulties, brain injury, dementia,degenerative neurological disorders?	×	×
If NO, does the study involve direct contact by any member of the research team with adults who are frail or physically disabled?		×
If NO, does the study involve direct contact by any member of the research team with adults who are living in residential care, social care, nursing homes, re - ablement centres, hospitals or hospices ?		×
If NO, does the study involve direct contact by any member of the research team with adults who are in prison, remanded on bail or in custody?		×
If you have answered YES to any of the questions above please explain the nature of that contact and what you will be doing		

External Ethics Review

Question	Yes	No
Will this study be submitted for ethical review to an external organisation ? (e.g.Another University, Social Care, National Health Service, Ministry of Defence, Police Service and Probation Office)		×
If YES, name of external organisation		
Will this study be reviewed using the IRAS system?		×
Has this study previously been reviewed by an external organisation?		

Confidentiality, security and retention of research data

Question		Yes	No
What data are you collecting / using / recording?	Publicly available datasets, open-source synthetic forensic images, sample audio files with embedded data, simulated RAM dumps from controlled environments, benchmark datasets for steganography and malware analysis, test cases from digital forensic research repositories		
Are there any reasons why you cannot guarantee the full security and confidentiality of any personal or confidential data collected for the study?			×
Please provide an explanation			
Is there a significant possibility that any of your participants, and associated persons, could be directly or indirectly identified in the outputs or findings from this study?			
Please provide an explanation			
Is there a significant possibility that a specific organisation or agency or participants could have confidential information identified, as a result of the way you write up the results of the study?			
Please provide an explanation			
Will any members of the research team retain any personal of confidential data at the end of the project, other than in fully anonymised form?			×
Please provide an explanation			
Will you or any member of the team intend to make use of any confidential information, knowledge, trade secrets obtained for any other purpose than the research project ?			×
Please give an explanation			
Have you taken necessary precautions for secure data management, in accordance with data protection and CU Policy		×	
Specify location (physical and electronic) where data will be stored			
Will you be responsible for destroying the data after study completion?			×
If NO, who will be responsible for this?	Data destruction is not required as the research exclusively utilizes publicly available synthetic datasets and open-source forensic test samples that are maintained in public repositories for academic and research purposes. No sensitive, personal, or confidential data is collected or processed during this study.		
Please explain how any identifiable and anonymous data will be destroyed			
Planned disposal date			

Participant Information and Informed Consent

Question	Yes	No
Will all the participants be fully informed BEFORE the project begins why the study is being conducted and what their participation will involve ?		
Please explain why		
Will every participant be asked to give written consent to participating in the study, before it begins ?		
If NO, please explain how you will get consent from your participants.If not written consent, explain how you will record consent		
Will all participants be fully informed about what data will be collected, and what will be done with this data during and after the study ?		
If NO, please specify		
Please explain what recordings (audio, visual or both) will be made and how you will gain consent for recording participants		
Will all participants understand that they have the right not to take part at any time, and/or withdraw themselves and their data from the study if they wish?		
If NO, please explain why		
Will every participant understand that there will be no reasons required or repercussions if they withdraw or remove their data from the study?		
If NO, please explain why		
Does the study involve deceiving, or covert observation of, participants?		
Will you debrief them at the earliest possible opportunity?		
If NO to debrief them, please explain why this is necessary		

Risk of harm, potential harm and disclosure of harm

Question	Yes	No
Is there any significant risk that the study may lead to physical harm to participants or researchers ?		
If you have answered Yes, please explain how you will take steps to reduce or address those risks. If you have answered No, explain why you believe this is the case		
Is there any risk that your study may lead or result in harm to the reputation of the University Group, its researchers or the organisations involved in the study?		
If you have answered Yes, please explain how you will take steps to reduce or address those risks. If you have answered No, explain why you believe this is the case		
Is there a risk that the study will lead to participants to disclose evidence of previous criminal offences, or their intention to commit criminal offences?		
If you have answered Yes, please explain how you will take steps to reduce or address those risks. If you have answered No, explain why you believe this is the case		
Is there a risk that the study will lead participants to disclose evidence that children or vulnerable adults are being harmed, or at risk or harm?		
If you have answered Yes, please explain how you will take steps to reduce or address those risks. If you have answered No, explain why you believe this is the case		
Is there a risk that the study will lead participants to disclose evidence of serious risk of other types of harm ?		
If you have answered Yes, please explain how you will take steps to reduce or address those risks. If you have answered No, explain why you believe this is the case		
Will participants be made aware of the circumstances in which disclosure has implications for confidentiality?		

Payments to participants

Question	Yes	No
Do you intend to offer participants cash payments or any kind of inducements, or reward for taking part in your study ?		
If YES, please explain what kind of payment you will be offering(e.g.prize draw or store vouchers)		
Is there any possibility that such payments or inducements will cause participants to consent to risks that they might not otherwise find acceptable ?		
If YES, please explain)		
Is there any possibility that the prospect of payment or inducements will influence the data provided by participants in any way ?		
If YES, please explain)		
Will you inform participants that accepting payments or inducements does not affect their right to withdraw from the study at any time ?		

Capacity to give valid consent

Question	Yes	No
Do you propose to recruit any participants?		X
Do you propose to recruit any participants who are children or young people under 18 years of age?		
Do you propose to recruit any participants who are adults who have learning difficulties, mental health conditions, brain injury, advanced dementia, degenerative neurological disorders ?		X
Do you propose to recruit any participants who are adults who are physically disabled and cannot provide written and/or verbal consent		X
Do you propose to recruit any participants who are with adults who are living in residential care, social care, nursing homes, reablement centres, hospitals or hospices ?		X
Do you propose to recruit any participants who are with adults who are in prison, remanded on bail or in custody?		X
If you have answered YES to any of the questions above please explain overcome any challenges to gaining valid consent		
Do you propose to recruit any participants with possible communication difficulties, including difficulties arising from limited use of knowledge of the English language ?		
If YES, please explain how you will overcome any challenges to gaining valid consent		
Do you propose to recruit participants who may not be able to fully understand the nature of the study, the foreseen implications or cannot provide consent?		
If YES, please explain how you will overcome any challenges to gaining valid consent		

Recruiting Participants

Question		Yes	No
Who are the participants?			
How are participants being recruited? Please provide details on all methods of recruitment you intend to use			
Do you foresee any conflict of interest?			
Please explain how will this conflict of interest be addressed			

Online and Internet Research

Question		Yes	No
Will any part of your project involve collecting data via the internet or social media?		×	
If YES, please explain how you will obtain permission to collect data by these means	All data will be collected from publicly available online repositories, open-source forensic databases, and research datasets that are freely accessible without requiring specific permissions.		
Will this require consent to access?			×
If NO, please explain how you will get permission/ consent' to collect this information?			
Will you be collecting data using an online questionnaire/ survey tool? (e.g. BoS, Filemaker)?			×
If YES, please explain which software and how you are ensuring appropriate data security			
Is there a possibility that the study will encourage children under 18 to access inappropriate websites, or correspond with people who pose risk of harm ?			×
If YES, please explain further			
Will the study incur any other risks that arise specifically from the use of electronic media ?			×
If YES, please explain further			

Information gathered from human participants

Question	Yes	No
Primary		
Does your project involve primary data collection from human participants via questionnaires, focus groups, interviews, psychological tests, photography/videography etc.?		×
If YES, Please detail the information to be collected and methods that will be used.		
Is there the possibility of physical or psychological harm to the researcher(s) or the participants?		×
If YES, please explain the possible harm and action taken to reduce/remove the risk		
Are any specific exclusions needed to prevent possible harm to participants (e.g. excluding people with known mental health problems)?		×
If YES, please explain exclusions needed and how these will be carried out		
Are any of the questionnaires or other tests being used in the research diagnostic for specific clinical conditions?		×
If YES, Please explain how you will take steps to reduce or address these risks		