

Shared-access denial and the individual-attribution gap in Saudi cybercrime judgments

Bunder Alshammari

Ban.Alshammari@uoh.edu.sa

University of Ha'il

Khaled Nasser Alfraidi

University of Ha'il

Article

Keywords: cybercrime adjudication, digital evidence, shared IP address, forensic pragmatics, Islamic legal reasoning, Saudi law

Posted Date: October 16th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10406563/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License. [Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Network-generated evidence is often treated as a gateway to cybercrime attribution, yet a technical trace rarely identifies a human actor without further inferential work. This article examines how defendants and judges negotiate this trace-to-actor gap in Saudi cybercrime judgments involving shared IP addresses, communal devices, family networks, or open wireless access. Drawing on twelve authenticated judgments issued by Eastern Province judicial circuits between 1432 and 1435 AH (2011–2014), the study develops a forensic-pragmatic account of how digital evidence becomes legally meaningful in a Sharia-informed evidentiary environment. The analysis integrates speech-act theory, politeness and facework, relevance theory, digital-evidence scholarship, and Islamic legal concepts of *shubha* (legal doubt), *niyya* (intent), and *ta'zir* discretion. Five recurrent defence strategies are identified: categorical denial, shared-access blame transfer, evidential displacement, moral-religious credibility work, and alternative-causation narrative. The findings show that defendants do not simply deny wrongdoing; they reframe the probative status of the trace by separating network location from individual agency, challenging the granularity of forensic reports, and invoking credibility and intent. Judicial uptake is similarly hybrid: courts treat digital traces as probative indicators but require corroborative reasoning before converting access-point evidence into individual attribution. The article contributes an operational typology of denial strategies in Arabic cybercrime judgments and proposes a multidimensional model for analysing digital attribution disputes across legal cultures. Although the corpus is small and historically bounded, it illuminates a persistent problem in cybercrime adjudication: how courts assign responsibility when technical evidence identifies a route of access more readily than an accountable person.

Introduction

Cybercrime adjudication increasingly depends on network-generated traces: IP logs, account records, device identifiers, timestamps, platform metadata, and forensic reports. These materials can establish that an activity occurred through a particular route of access, but they do not always establish who performed the act. The gap between a technical trace and an accountable human actor is particularly consequential in cases involving household routers, shared mobile devices, communal computers, weakly secured Wi-Fi, or multiple users of the same account. In such cases, the evidentiary question is not only whether the trace is authentic, but whether it is sufficiently individualised to sustain legal attribution.

This article addresses that problem through Saudi cybercrime judgments in which defendants contested attribution by invoking shared digital infrastructure. The paper is not a technical evaluation of network forensics and does not attempt to measure the accuracy of digital-investigative tools. Its contribution lies instead in the legal-discursive space where technical evidence is translated into judicial reasoning. It asks how defendants linguistically construct doubt around trace-based evidence and how judges evaluate those constructions within a legal order that combines statutory cybercrime provisions, codified evidence rules, and Sharia-informed principles of intent, credibility, and doubt.

The study is motivated by a recurring misalignment in cybercrime evidence. A network identifier may indicate a subscriber, a location, an access point, or an account environment, while legal responsibility requires a stronger inference about agency. This misalignment has been widely discussed in digital forensics and technology-law scholarship, including debates over the probative limits of IP-address evidence and the need for layered

corroboration in cyber attribution (Berghel 2017; Casey 2011; Grotto 2020; Ohm 2010). Yet less attention has been paid to how such disputes are linguistically performed and judicially resolved in Arabic, judge-led, Sharia-informed court settings.

Saudi Arabia provides an analytically valuable context for this inquiry. The Anti-Cyber Crime Law, issued by Royal Decree No. M/17 in 2007, criminalises a range of offences involving computers, information networks, privacy violations, defamation, blackmail, and unlawful access (Bureau of Experts at the Council of Ministers 2007). More recently, the Law of Evidence codified the probative status of digital evidence while leaving courts with the task of assessing its validity, context, and evidentiary weight (Bureau of Experts at the Council of Ministers 2022). The historical judgments examined here predate the Law of Evidence but remain relevant because they document early judicial reasoning around a problem that has not disappeared: authentication of a digital trace does not automatically settle identity, intention, or exclusive control.

The article advances three arguments. First, denial in shared-infrastructure cases is not a simple negation but a structured forensic-pragmatic practice. Defendants use denial to redirect the court from the existence of a trace to the uncertainty of individual authorship. Second, judicial uptake depends on whether denial interacts with evidentiary insufficiency, corroborative weakness, or plausible alternative access. Bare denial is rarely decisive; shared-access explanation becomes relevant when it exposes a gap in the prosecution's inference. Third, Saudi judicial reasoning is best understood as hybrid. It evaluates digital forensic indicators through concepts of evidentiary sufficiency while also drawing on Islamic legal categories such as *shubha*, *niyya*, and *ta'zir* discretion.

The article contributes to digital-evidence scholarship, forensic linguistics, and comparative law, and speaks to the broader interdisciplinary readership at the intersection of law, language, and society. For digital-evidence studies, it shows how trace evidence is contested after collection and authentication, at the stage of legal interpretation. For forensic pragmatics, it offers an empirically grounded typology of denial strategies in Arabic cybercrime judgments. For comparative legal scholarship, it demonstrates how a universal evidentiary problem—the trace-to-actor gap—is processed through a locally specific jurisprudential vocabulary.

Legal and evidentiary context

The Saudi Anti-Cyber Crime Law defines cybercrime as conduct involving computers or information networks in violation of statutory provisions. Relevant offence categories include unlawful access, blackmail, privacy infringement, defamation, harm through information-technology devices, and the production or transmission of unlawful digital content (Bureau of Experts at the Council of Ministers 2007). These categories frequently require a court to connect a digital act to an individual user. Where a message, post, threat, or login is traced to a device or network associated with a defendant, attribution becomes the central legal issue.

The subsequent Law of Evidence strengthens the contemporary relevance of this study. It recognises digital evidence as a legally cognisable form of proof and gives it probative value comparable to ordinary documentary evidence, while also preserving the court's evaluative role in determining whether the evidence is sufficiently reliable and relevant to the disputed fact (Bureau of Experts at the Council of Ministers 2022). The Controls of Electronic Evidentiary Procedures further specify modes through which digital evidence may be submitted and assessed (Ministry of Justice 2022). These reforms do not make digital traces self-interpreting. Rather, they

formalise the question that earlier courts were already confronting: when does a digital trace support the legal conclusion that a particular person acted with the required intent?

Saudi criminal adjudication also remains shaped by Islamic legal epistemology. In offences handled through *ta'zir*, courts exercise discretion in light of proof, credibility, public interest, and the circumstances of the act. Concepts such as *shubha* and *niyya* are not ornamental religious references; they structure how doubt and intent are evaluated when evidence is incomplete or inferential. In cybercrime cases, this matters because the digital record may authenticate access while leaving intention or human agency uncertain.

Literature review and conceptual framework

Digital traces and the attribution problem

Digital evidence scholarship distinguishes between the integrity of a record and the attribution of conduct. A log file, IP address, or device timestamp may be authentic in the sense that it accurately records a technical event, yet the event still requires interpretation. Casey (2011) emphasises that digital evidence must be evaluated in relation to source, context, and investigative hypothesis rather than treated as mechanically conclusive. Berghel (2017) and Grotto (2020) similarly argue that cyber attribution is layered and probabilistic; it depends on corroboration across technical, contextual, and behavioural indicators. Work on cross-border digital evidence and cyber attribution likewise emphasises the need to separate technical traceability from legal responsibility (Banks 2021; Bendiek and Schulze 2021; Casino et al. 2022; Rogers 2017), while authorship-attribution scholarship treats attribution as probabilistic and context-dependent (Juola 2008; Koppel et al. 2009).

The same problem appears in legal debates over IP-address evidence. Ohm (2010) famously warns against the assumption that an IP address identifies a person. At most, an IP address may indicate a network endpoint or subscriber relationship during a given time window. The legal inference from endpoint to actor requires additional proof, such as device-level artefacts, credential control, temporal proximity, user admissions, account history, behavioural patterns, or exclusion of alternative users. Without such corroboration, trace evidence may produce suspicion but not decisive authorship.

Forensic pragmatics, denial, and blame management

Forensic linguistics has long shown that legal facts are partly constructed through language. Courtroom discourse does not merely report events; it organises agency, credibility, intention, and blame (Cotterill 2003; Shuy 1993; Solan and Tiersma 2005; Tiersma 2000). In this perspective, denial is an illocutionary and interactional act. It rejects a proposition, but it also proposes an alternative distribution of responsibility; analyses of refusals and other dispreferred responses show how speakers simultaneously reject a proposition and manage the redistribution of accountability (Beebe et al. 1990). Analyses of threatening discourse further show how stance and appraisal cues can organise responsibility, threat, and speaker alignment in legally relevant texts (Gales 2011).

The present study treats denial as a forensic-pragmatic strategy: a patterned communicative move through which a defendant contests the prosecution's account of authorship or intent. Speech-act theory explains the force of categorical denial; politeness and facework explain how accused persons manage moral identity and

social credibility; relevance theory explains how defendants guide judges toward alternative interpretations of the same evidentiary record (Austin 1975; Brown and Levinson 1987; Searle 1969; Sperber and Wilson 1995; Wilson and Sperber 2004). In cybercrime cases, denial often works by transforming a trace into an evidentiary question: the issue becomes not whether the network was used, but whether the defendant was the user.

Islamic evidentiary reasoning and digital doubt

Islamic legal reasoning places strong emphasis on evidentiary certainty, intention, and the avoidance of punishment where legally consequential doubt persists. While the operation of *shubha* differs across offence categories and schools of law, the principle remains important for understanding doubt-sensitive reasoning in Muslim legal traditions (al-Zuhayli 2001; Kamali 2008; Peters 2005). In *ta'zir* matters, judicial discretion allows the court to weigh circumstantial evidence, credibility, harm, intent, and public interest. Broader accounts of Sharia legal theory similarly stress the relationship between evidentiary reasoning, judicial discretion, and institutional practice (Hallaq 2009).

Digital attribution disputes fit naturally into this epistemic structure because they often involve a technically authenticated trace and an uncertain human actor. The trace may prove that an access point was involved, but *shubha* may arise if the court cannot confidently identify the user or infer *niyya*. The question is therefore not whether Islamic law resists digital evidence. Rather, the question is how digital evidence is jurisprudentially evaluated when its probative reach stops short of individualised agency.

The multidimensional discourse integration model

To organise the analysis, this study proposes the Multidimensional Discourse Integration Model (MDIM). The model links five layers: (1) a technical input layer consisting of IP logs, device records, account data, timestamps, and forensic reports; (2) a forensic-pragmatic layer in which defendants deploy denial strategies; (3) an evidentiary-evaluation layer in which courts assess authenticity, corroboration, granularity, and alternative-access plausibility; (4) an Islamic legal reasoning layer involving *shubha*, *niyya*, credibility, and *ta'zir* discretion; and (5) an output layer consisting of judicial uptake, conviction, mitigation, dismissal, non-conviction, or doubt-constrained reasoning.

The MDIM does not claim that discourse determines judicial outcome. Rather, it explains how discourse interacts with evidentiary conditions. A denial becomes legally consequential only when it identifies an evidentiary gap or supplies a plausible alternative account that the court cannot exclude. Conversely, when digital evidence is strongly corroborated, denial may be rejected even if linguistically elaborate. Figure 1 visualises these five layers and their movement from technical input to judicial outcome.

Research questions

RQ1. What forensic-pragmatic strategies do defendants use to deny authorship or contest digital evidence associated with shared IP addresses, communal devices, or shared accounts in Saudi cybercrime judgments?

RQ2. How do these strategies use linguistic and pragmatic resources—including negation, modality, stance, alternative causation, moral positioning, and religious expression—to generate evidentiary doubt?

RQ3. How do Saudi judges evaluate shared-access defences when weighing technical digital forensic indicators against denial, credibility, intent, and Islamic evidentiary reasoning?

RQ4. What transferable analytic lessons can be drawn from a small, historically bounded Saudi corpus without overstating national or temporal generalisability?

Methods

Design

The study uses a qualitative, corpus-based design grounded in forensic pragmatics and legal discourse analysis. The objective is not statistical prevalence estimation but analytic explanation: to identify how defendants construct denial and how courts reason through attribution uncertainty. The design is appropriate because the judgments contain dense legal reasoning, reported defendant speech, forensic references, and outcome-linked judicial evaluation.

Corpus source and access

The empirical corpus consists of twelve authenticated Saudi criminal judgments drawn from the official published volume *Jarā'im Ma'ālūmātiyyah* (Cybercrimes), issued by the Saudi Ministry of Justice. The volume compiles finalised rulings under the Anti-Cyber Crime Law. The volume is held in institutional legal libraries and is not publicly downloadable. It was accessed through an institutional legal library. The study reports only anonymised case descriptions and does not reproduce identifying party details.

Sampling logic and corpus boundaries

The source volume contains forty-seven cybercrime judgments. Initial screening identified nineteen cases involving explicit defendant responses to digital evidence. Twelve judgments were selected for detailed analysis because they met four criteria: (a) adjudication under the Anti-Cyber Crime Law; (b) an explicit denial or defence based on shared digital infrastructure; (c) inclusion of both technical material and defendant response; and (d) judicial reasoning that addressed ambiguity, intent, credibility, or legal doubt. Seven cases were excluded because they lacked articulated denial discourse or because the ruling resolved the matter procedurally without substantive reasoning on attribution.

The sample is intentionally narrow. All cases come from Eastern Province circuits and were issued between 1432 and 1435 AH (2011–2014). These boundaries limit representativeness, but they also create a coherent corpus for analysing early judicial reasoning under the Anti-Cyber Crime Law. The study does not claim to describe all Saudi cybercrime adjudication or current national practice. Instead, it uses information-rich cases to theorise mechanisms of trace-to-actor reasoning that remain relevant under contemporary evidence law. Table 1 summarises the corpus characteristics, shared-access features, primary defence strategies, and outcome-relevant judicial uptake for each judgment.

Table 1
Corpus characteristics and analytic classification of the twelve judgments

Case	Year	Dominant offence context	Shared-access feature	Primary defence strategy	Outcome-relevant judicial uptake
A	1433H / 2012–2013	Defamation / posting attribution	Household router used by family and visitors	Shared-access blame transfer	Shared access treated as producing doubt; outcome constrained by ta'zir reasoning
B	1432H / 2011–2012	Defamation / insulting online statement	Shared family computer	Categorical denial	Denial rejected where additional corroboration supported attribution
C	1432H / 2011–2012	Privacy-related posting	Communal mobile/device access	Categorical denial	Denial contributed to doubt only where actor identity remained inconclusive
D	1433H / 2012–2013	Online threat / abusive message	Account accessed from shared device	Categorical denial	Court required corroboration beyond denial where trace evidence had support
E	1433H / 2012–2013	Defamation through social-media account	Open or weakly secured Wi-Fi	Shared-access blame transfer	Shared access reduced certainty and supported mitigation
F	1434H / 2013	Blackmail / coercive communication	Several users had access to account/device	Shared-access blame transfer	Uncertainty in actor identity considered within ta'zir discretion
G	1434H / 2013	Unauthorised access allegation	Household network and shared device	Shared-access blame transfer	Alternative access accepted as relevant to doubt
H	1434H / 2013	Technical-report attribution dispute	IP log without user-level corroboration	Evidential displacement	Court noted limits of trace-to-actor inference
I	1435H / 2014	Account-use attribution dispute	Device logs did not identify individual user	Evidential displacement	Insufficient individualisation supported mitigation or non-conviction reasoning
J	1435H / 2014	Blackmail / moral-harm allegation	Shared device or account access	Moral-religious credibility work	Religious and moral stance considered only alongside evidentiary ambiguity
K	1435H / 2014	Privacy or reputational harm	Communal access environment	Moral-religious credibility work	Intent and character language aligned with mitigation
L	1435H / 2014	Hacking / framing scenario	Unknown third-party use of network/account	Alternative-causation narrative	Alternative scenario not technically excluded; doubt constrained attribution

Coding and reliability

The judgments were analysed in Arabic. All segments in which defendants denied, displaced, qualified, or recontextualised digital evidence were extracted and coded against a purpose-built coding instrument that operationalised each defence strategy through a core function, diagnostic linguistic cues, a jurisprudential hinge, and decision rules for assignment. Coding began with deductive categories from speech-act theory, forensic pragmatics, and blame-management research, then was refined inductively to capture strategies specific to shared-access digital evidence and Saudi judicial discourse. Each case was assigned one primary defence strategy according to three decision rules: frequency within the defendant's response, explicitness of judicial evaluation, and argumentative centrality to the final ruling. Secondary strategies were also recorded.

Two Arabic-speaking researchers independently coded the full corpus, classifying fifty extracted defence segments into the five strategy categories. Inter-coder reliability was assessed with Cohen's kappa and reached $\kappa = 0.92$, indicating high agreement. Disagreements were resolved through adjudication with a third reviewer. English translations of examples were prepared after coding and checked by a second bilingual reader for functional equivalence rather than literal word-for-word correspondence.

Saturation and analytic stopping criterion

Analytic saturation was assessed through a staged coding log. After each case, the researchers recorded whether a new defence strategy, linguistic trigger, jurisprudential hinge, or judicial uptake pattern had emerged. By the tenth case, no new primary strategy or jurisprudential hinge appeared. Cases K and L repeated and refined existing categories rather than generating new ones. Saturation is therefore defined narrowly as typological stabilisation within the selected information-rich corpus, not as exhaustion of all possible Saudi cybercrime judgments.

Data handling and anonymisation

The study analysed published archival judicial records; no participants were recruited or contacted. All names, national identifiers, addresses, and potentially identifying contextual details were removed or generalised before coding. Source files, coding logs, and anonymised extracts were stored on password-protected institutional devices accessible only to the research team.

Analysis and findings

Across the twelve judgments, defendants used five primary defence strategies to contest trace-based attribution. These strategies are not mutually exclusive; several cases involved layered denial. A strategy is treated as judicially effective only where the judgment shows outcome-linked uptake, such as explicit acceptance of its logic, mitigation, dismissal, non-conviction, or doubt-constrained reasoning. Effectiveness does not mean factual truth, and no statistical inference is made from the small corpus.

Table 2 reports the coding categories, linguistic cues, illustrative examples, jurisprudential hinges, and typical judicial uptake for the five defence strategies. Table 3 then summarises their distribution as primary strategies across the corpus.

Table 2
Defence strategies, linguistic cues, jurisprudential hinges, and judicial uptake

Strategy	Core function	Typical linguistic cues	Illustrative example	Legal hinge	Judicial uptake
Categorical denial	Rejects authorship or involvement outright	I did not write; I did not do this; I have no connection	I did not write this, and I have no connection to it.	Sufficiency and decisiveness of proof	Rejected where corroboration is strong; relevant to doubt only if actor identification remains unresolved
Shared-access blame transfer	Accepts infrastructure link but shifts plausible authorship to others with access	Yes, but; my brothers/relatives/visitors use it; the modem is shared	Yes, it is my internet, but my brothers, relatives, and visitors use the network.	shubha (legal doubt)	Often taken up where shared access undermines individualised attribution
Evidential displacement	Challenges the inference from trace to actor	The report proves the connection, not the user; this may be an error	The report proves the connection, not who used the device.	Threshold of decisive proof	Taken up where the technical report lacks user-level granularity
Moral-religious credibility work	Builds credibility through oath, character, and pious self-presentation	By God; I seek God's forgiveness; this is not my character	By God, this is not my character; I fear God in my actions.	niyya and credibility	Mitigation-aligned only where evidence is already ambiguous
Alternative-causation narrative	Reframes defendant as victim of hacking, framing, or third-party exploitation	My account was hacked; someone used my network to frame me	Someone may have hacked my account or used my network to frame me.	Alternative causation, shubha, intent	Relevant where the alternative scenario is not technically excluded

Table 3
Distribution of primary defence strategies and typical judicial responses

Primary strategy	Frequency	Typical case context	Typical judicial response pattern
Categorical denial	3	Defamation, posting attribution, or threat contexts	Rejected when corroboration is present; contributes to doubt only when actor identification is inconclusive
Shared-access blame transfer	4	Household networks, family computers, open Wi-Fi	Most frequently taken up as generating doubt; may support dismissal, acquittal, or ta'zir mitigation
Evidential displacement	2	Technical-report or log-contestation disputes	Mitigation or non-conviction where trace-to-actor inference remains unresolved
Moral-religious credibility work	2	Blackmail, moral-harm, or reputational contexts	Relevant to mitigation where intent and credibility are evaluated under ta'zir and evidence is ambiguous
Alternative-causation narrative	1	Hacking, framing, or third-party exploitation scenario	Doubt-based reasoning where alternative scenario is not technically excluded

Categorical denial

Categorical denial consists of explicit rejection of authorship or involvement. It appears through direct negation and relational distancing: the defendant states that he did not write, send, post, access, or participate in the disputed act. In speech-act terms, the denial is a direct commissive-resistant act: it refuses the proposition that the accused is the author of the digital event.

In this corpus, categorical denial was the primary strategy in three cases. Its legal value depended heavily on corroboration. Where the court treated the technical evidence as supported by additional circumstances, categorical denial was rejected. Where user identification remained thin, however, denial contributed to doubt. The pattern shows that denial is not persuasive because of its grammatical directness; it becomes relevant when it aligns with evidentiary incompleteness.

Shared-access blame transfer

Shared-access blame transfer was the most frequent primary strategy. It differs from categorical denial because it concedes part of the prosecution's technical narrative while disputing its attributional conclusion. The defendant accepts that the modem, device, or account may be connected to him, but argues that others had access. This produces a concessive structure: "yes, the trace is linked to my environment, but that environment was not exclusively under my control."

This strategy directly targets the trace-to-actor gap. Its persuasive force lies in plausible multiplicity. By invoking family members, relatives, visitors, shared devices, or open Wi-Fi, the defendant transforms a single technical trace into a set of possible human actors. In the judgments, courts were most receptive to this strategy where the forensic record did not exclude alternative users. The resulting doubt did not always produce acquittal, but it often constrained the legal movement from access-point evidence to individual culpability.

Evidential displacement

Evidential displacement challenges the evidentiary object itself. The defendant does not merely say “I did not do it”; he argues that the report proves a different fact from the one alleged. In these cases, the defence separates connection from authorship, authentication from agency, and location from intent. The typical argument is that a forensic report may prove that the relevant connection passed through a network, but not that the accused personally operated the device or authored the communication.

In the two cases where evidential displacement was primary, judicial uptake occurred when the court acknowledged limits in technical granularity. The strategy therefore operates as an epistemic challenge: it asks the court to specify what exactly the digital evidence proves and what remains inferential. This is particularly important in shared-IP cases, where the evidence may be reliable but not sufficiently individualised.

Moral-religious credibility work

Moral-religious credibility work uses oath, pious expression, character claims, and fear-of-God formulations to support denial. In the Saudi judicial setting, such language is not simply decorative. It positions the defendant as a morally accountable speaker whose self-presentation bears on credibility and intent. Nevertheless, the corpus shows that pious appeal was not determinative by itself.

The courts treated moral-religious claims as relevant only when the evidentiary record was already ambiguous. In this sense, pious appeal operates as a credibility supplement, not as a substitute for proof. Its practical effect is strongest under *ta'zir* reasoning, where intent, remorse, character, harm, and uncertainty may influence sanctioning or mitigation.

Alternative-causation narrative

Alternative-causation narrative reframes the defendant as a possible victim of hacking, framing, or third-party exploitation. This strategy is more elaborate than blame transfer because it constructs an alternative story of how the digital trace came to exist. Rather than merely saying that others could have used the network, the defendant presents a causal scenario in which someone exploited the account, device, or connection to implicate him.

Although this strategy was primary in only one case, it is theoretically important. It shows how digital attribution disputes can shift procedural identity: the accused is reconfigured from offender to potential target. Judicial uptake depended on whether the alternative narrative was technically plausible and not excluded by the evidence. The finding aligns with broader cyber-attribution scholarship: alternative explanations matter most when technical evidence lacks sufficient exclusionary power.

Strategy layering and co-occurrence

The strategies often appeared in combination. Defendants paired categorical denial with blame transfer, evidential displacement with shared access, and pious appeal with direct denial. Layering allows defendants to contest attribution at multiple levels: factual authorship, technical sufficiency, moral credibility, and causal explanation. This layered structure helps explain why shared-access defences can be powerful even when no single statement is decisive. Table 4 shows the descriptive co-occurrence patterns among primary and secondary defence strategies.

Table 4
Descriptive co-occurrence matrix of primary and secondary defence strategies

Primary strategy	Categorical denial	Shared-access blame transfer	Evidential displacement	Moral-religious credibility work	Alternative-causation narrative
Categorical denial (n = 3)	–	1	0	1	1
Shared-access blame transfer (n = 4)	2	–	2	1	0
Evidential displacement (n = 2)	1	1	–	0	0
Moral-religious credibility work (n = 2)	1	1	0	–	0
Alternative-causation narrative (n = 1)	0	0	1	0	–
Data availability					
The source judgments analysed in this study are contained in the official published volume Jarā'im Ma'ūmātiyyah (Cybercrimes), issued by the Saudi Ministry of Justice. The volume is not publicly downloadable but may be consulted through institutional legal libraries. The anonymised case-level coded dataset, coding instrument, and segment-level inter-coder reliability dataset generated and analysed during the study are available from the corresponding author on reasonable request. No directly identifying data are included in the shared materials.					

Worked application of the MDIM: Case A

Case A illustrates the MDIM's movement from technical input to judicial outcome. The relevant digital activity was linked to a home router during the material period. The forensic report therefore provided a probative connection between the event and the defendant's household network. It did not, however, establish which person operated the device at the time of the disputed communication.

The defendant's strategy was shared-access blame transfer. He conceded the infrastructure link but introduced non-exclusive access by household members and visitors. Linguistically, this strategy relied on concessive acknowledgement, plural third-party referents, and underspecified agency. The court treated shared access as relevant to *shubha* because the evidence did not decisively bridge the gap between network location and individual user. Case A therefore demonstrates the article's core claim: an authenticated trace can remain probative while its legal force is constrained when it cannot support individualised attribution.

Discussion

From technical trace to legal attribution

The findings support a central distinction in digital-evidence scholarship: proving that a network, device, or account was involved is not equivalent to proving that a particular person acted. In the Saudi judgments analysed here, courts did not treat technical traces as meaningless. They treated them as probative indicators that required interpretation. The decisive issue was whether the evidence could move from environmental connection to individualised authorship.

This distinction has practical consequences. IP-only or access-point evidence is vulnerable where multiple users plausibly share the same infrastructure. Stronger attribution requires corroborative features that narrow the human actor: device-level artefacts, credential use, account history, temporal alignment, content authorship indicators, admissions, witness evidence, or exclusion of alternative users. The study therefore reinforces the importance of forensic granularity and legal caution in cybercrime adjudication.

Why the historical corpus still matters

The 2011–2014 time window is a limitation but also an analytic opportunity. These judgments capture early Saudi judicial engagement with digital attribution under the Anti-Cyber Crime Law. They show how courts reasoned before the contemporary Law of Evidence codified digital evidence more explicitly. The core problem, however, remains current. Digital networks have changed, but shared access, account compromise, device borrowing, household connectivity, and alternative-user explanations continue to complicate attribution.

The article therefore treats the corpus as historical-analytical rather than contemporary-descriptive. It does not claim that these twelve cases represent current Saudi practice. Instead, it argues that they document foundational reasoning patterns around a durable evidentiary issue. This framing makes the manuscript more defensible for international readers because it avoids overgeneralisation while preserving theoretical value.

Comparative implications

A cautious comparative perspective shows that the trace-to-actor gap is not unique to Saudi Arabia. Western adversarial systems also require authentication, reliability, relevance, and corroboration before digital traces can support legal responsibility (Casey 2011; Chaski 2013; Eichensehr 2020). The Saudi corpus differs not in the existence of attribution uncertainty, but in the legal vocabulary through which uncertainty is evaluated. *Shubha*, *niyya*, and *ta'zir* provide explicit doctrinal resources for reasoning about doubt, intent, and discretionary response.

This distinction is important. The study does not exoticise Saudi adjudication or suggest that Islamic legal reasoning is incompatible with digital evidence. Rather, it shows that digital evidence is interpreted through locally available legal concepts. The same technical ambiguity can be processed through different institutional grammars: reliability and cross-examination in one setting; doubt, intent, and discretionary sanctioning in another. Comparative cybercrime scholarship benefits from attention to both shared evidentiary problems and legal-cultural variation.

Implications for investigators, prosecutors, defence lawyers, and judges

For investigators, the findings emphasise the need to move beyond access-point evidence wherever possible. Reports should distinguish clearly between what is technically established and what is inferred. Where a case

depends on a household router or shared device, investigators should seek corroboration that narrows user identity rather than relying on the subscriber relationship alone.

For prosecutors, the study highlights a predictable defence pathway: shared access will be used to generate doubt when attribution is thin. Anticipating this pathway requires presenting evidence that excludes alternative users or links the defendant to the act through additional indicators. For defence practitioners, the findings show that shared-access claims are more legally consequential when supported by plausible context and tied to a specific gap in the forensic report. For judges and legal educators, the typology provides a tool for separating categories of denial: direct denial, alternative-user attribution, evidential challenge, moral credibility work, and alternative causation.

Limitations and future research

The study has four limitations. First, the corpus is small and information-rich rather than statistically representative. Second, the cases are geographically concentrated in Eastern Province circuits. Third, the judgments are historical and do not provide a complete account of contemporary Saudi cybercrime practice. Fourth, published judgments provide limited access to underlying case files, full forensic reports, and courtroom interaction beyond what the judgment records.

Future research should expand the corpus across regions, years, and offence categories; compare Saudi judgments with other Gulf and common-law jurisdictions; and integrate technical digital forensics expertise with discourse analysis. A larger corpus could test whether the five-strategy typology remains stable across more recent cases and whether judicial uptake varies by offence type, evidentiary richness, or type of digital infrastructure.

Conclusion

This article examined how defendants and judges negotiate digital attribution in Saudi cybercrime judgments involving shared digital infrastructure. The analysis shows that defendants mobilise a five-part repertoire—categorical denial, shared-access blame transfer, evidential displacement, moral-religious credibility work, and alternative-causation narrative—to contest the inference from network trace to individual actor. These strategies work by separating technical connection from authorship, challenging the granularity of forensic reports, and activating doubt around agency and intent.

The findings also show that Saudi judicial reasoning is hybrid. Digital traces are treated as probative but not self-sufficient. Courts evaluate them alongside corroboration, plausibility of alternative access, credibility, *niyya*, *shubha*, and *ta'zir* discretion. The study contributes an operational typology for Arabic cybercrime judgments and a multidimensional model for analysing trace-to-actor disputes across legal cultures. Its claims remain bounded by corpus size, region, and historical period, but its theoretical contribution is broader: cybercrime attribution is not completed when a trace is found; it is completed, contested, or constrained through legal reasoning about who the trace can responsibly identify.

Declarations

Competing interests

The authors declare no competing interests.

Author Contribution

B.S.A. conceptualized the study, developed the theoretical framework, designed the methodology, identified and organized the judicial corpus, conducted the primary forensic-pragmatic analysis, and wrote the first draft of the manuscript. K.N.A. contributed to corpus verification, coding validation, inter-coder reliability procedures, legal-context interpretation, and refinement of the analytical categories. B.S.A. and K.N.A. jointly interpreted the findings, developed the discussion and implications, revised the manuscript critically for intellectual content, and approved the final version for submission. Both authors agree to be accountable for all aspects of the work.

Data Availability

The judicial materials analyzed in this study are derived from authenticated Saudi cybercrime judgments held in institutional legal-library and archival collections. Because the source judgments contain legally sensitive material and are subject to access restrictions, the full corpus cannot be deposited in a public repository. However, anonymized coding summaries, analytic tables, and non-identifying case classifications are available from the corresponding author upon reasonable request, subject to institutional approval and applicable legal and ethical restrictions.

References

1. Al-Zuhayli W (2001) *Al-fiqh al-Islāmī wa adillatuh* [Islamic jurisprudence and its proofs], vol 6. Dār al-Fikr, Damascus
2. Austin JL (1975) *How to do things with words*, 2nd edn. Harvard University Press, Cambridge, MA
3. Banks W (2021) Cyber attribution and state responsibility. *Int Law Stud* 97:1039–1072
4. Beebe LM, Takahashi T, Uliss-Weltz R (1990) Pragmatic transfer in ESL refusals. In: Scarcella RC, Andersen ES, Krashen SD (eds) *Developing communicative competence in a second language*. Newbury House, New York, pp 55–73
5. Bendiek A, Schulze M (2021) Attribution: a major challenge for EU cyber sanctions: an analysis of WannaCry, NotPetya. Cloud Hopper, Bundestag Hack and the attack on the OPCW. SWP Research Paper No 11/2021. Stiftung Wissenschaft und Politik, Berlin. <https://doi.org/10.18449/2021RP11>
6. Berghel H (2017) On the problem of (cyber) attribution. *Computer* 50(3):84–89. <https://doi.org/10.1109/MC.2017.74>
7. Brown P, Levinson SC (1987) *Politeness: some universals in language usage*. Cambridge University Press, Cambridge
8. Bureau of Experts at the Council of Ministers (2007) *Anti-Cyber Crime Law* (Royal Decree No M/17). Kingdom of Saudi Arabia, Riyadh

9. Bureau of Experts at the Council of Ministers (2022) Law of Evidence (Royal Decree No M/43). Kingdom of Saudi Arabia, Riyadh
10. Casey E (2011) Digital evidence and computer crime: forensic science, computers, and the internet, 3rd edn. Academic, Waltham, MA
11. Casino F, Pina C, López-Aguilar P, Batista E, Solanas A, Patsakis C (2022) SoK: cross-border criminal investigations and digital evidence. *J Cybersecur* 8(1):tyac014. <https://doi.org/10.1093/cybsec/tyac014>
12. Chaski CE (2013) Best practices and admissibility of forensic author identification. *J Law Policy* 21(2):333–376
13. Cotterill J (2003) Language and power in court: a linguistic analysis of the O. J. Simpson trial. Palgrave Macmillan, Basingstoke. <https://doi.org/10.1057/9780230006010>
14. Eichensehr KE (2020) The law and politics of cyberattack attribution. *UCLA Law Rev* 67(3):520–598
15. Gales T (2011) Identifying interpersonal stance in threatening discourse: an appraisal analysis. *Discourse Stud* 13(1):27–46. <https://doi.org/10.1177/1461445610387735>
16. Grotto A (2020) Deconstructing cyber attribution: a proposed framework and lexicon. *IEEE Secur Priv* 18(1):12–20. <https://doi.org/10.1109/MSEC.2019.2938134>
17. Hallaq WB (2009) *Sharīʿa: theory, practice, transformations*. Cambridge University Press, Cambridge
18. Juola P (2008) Authorship attribution. *Found Trends Inf Retr* 1(3):233–334. <https://doi.org/10.1561/15000000005>
19. Kamali MH (2008) *Shariʿah law: an introduction*. Oneworld, Oxford
20. Koppel M, Schler J, Argamon S (2009) Computational methods in authorship attribution. *J Am Soc Inf Sci Technol* 60(1):9–26. <https://doi.org/10.1002/asi.20961>
21. Ministry of Justice (2022) Controls of electronic evidentiary procedures (Ministerial Decision No 921/1444). Ministry of Justice, Riyadh
22. Ohm P (2010) Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Rev* 57:1701–1777
23. Peters R (2005) *Crime and punishment in Islamic law: theory and practice from the sixteenth to the twenty-first century*. Cambridge University Press, Cambridge
24. Rogers M (2017) Technology and digital forensics. In: McGuire MR, Holt TJ (eds) *The Routledge handbook of technology, crime and justice*. Routledge, London. <https://doi.org/10.4324/9781315743981-24>
25. Searle JR (1969) *Speech acts: an essay in the philosophy of language*. Cambridge University Press, Cambridge
26. Shuy RW (1993) *Language crimes: the use and abuse of language evidence in the courtroom*. Blackwell, Oxford
27. Solan LM, Tiersma PM (2005) *Speaking of crime: the language of criminal justice*. University of Chicago Press, Chicago
28. Sperber D, Wilson D (1995) *Relevance: communication and cognition*, 2nd edn. Blackwell, Oxford
29. Tiersma PM (2000) *Legal language*. University of Chicago Press, Chicago
30. Wilson D, Sperber D (2004) Relevance theory. In: Horn LR, Ward G (eds) *The handbook of pragmatics*. Blackwell, Oxford, pp 607–632. <https://doi.org/10.1002/9780470756959.ch27>

Figures

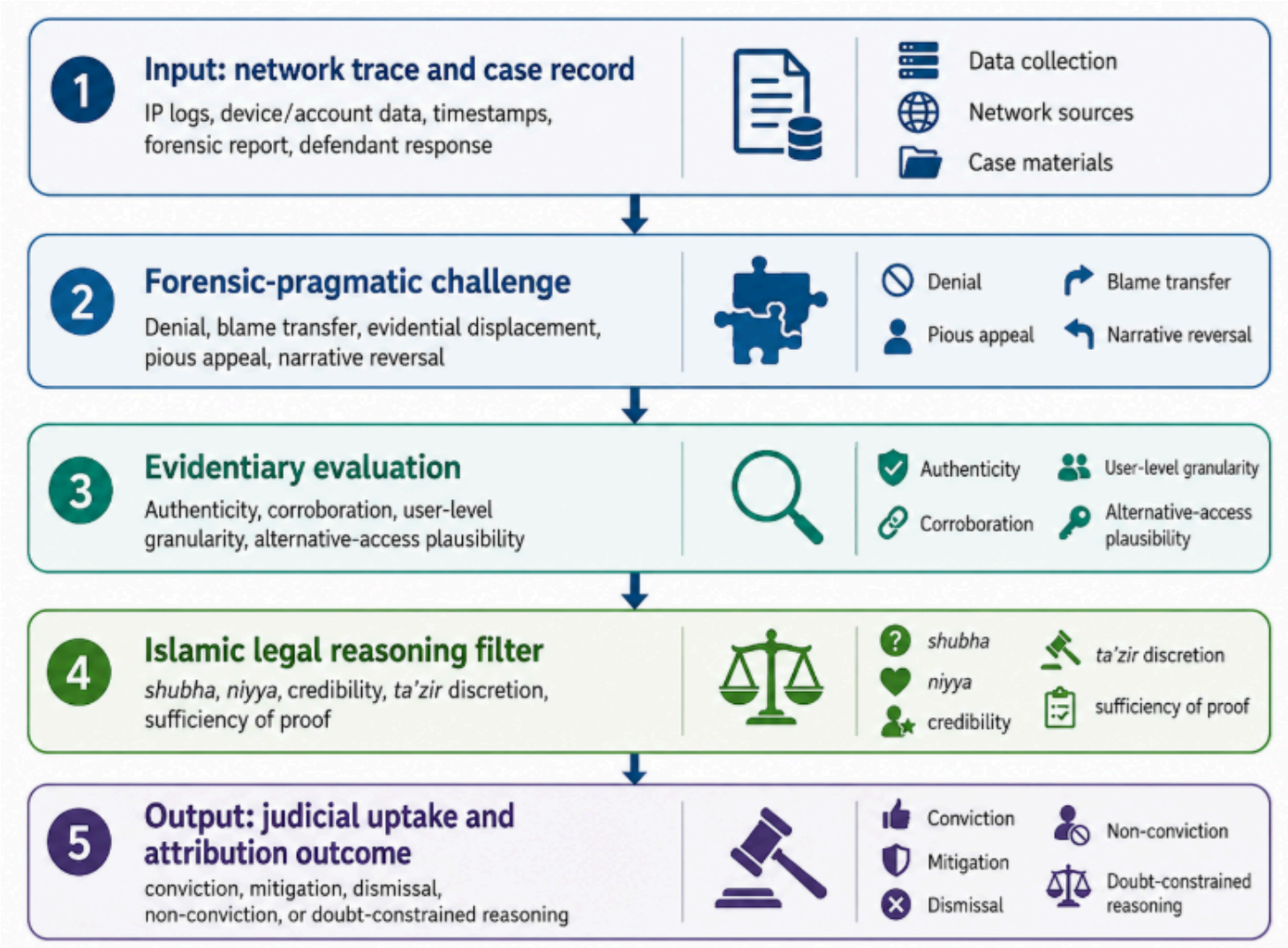


Figure 1

Multidimensional Discourse Integration Model for trace-to-actor attribution in Saudi cybercrime judgments. The model follows five linked stages: (1) technical inputs from network traces and case records; (2) forensic-pragmatic defence strategies; (3) evidentiary evaluation of authenticity, corroboration, user-level granularity, and plausible alternative access; (4) Islamic legal reasoning through *shubha*, *niyya*, credibility, *ta'zir* discretion, and sufficiency of proof; and (5) judicial uptake and attribution outcomes. The figure is an original author-created schematic.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [Cybercrimeinstrumentsanddata.pdf](#)
- [Cybercrimeinstrumentsanddata.tex](#)