

Research Instruments and Analytic Dataset

Supplementary methodological materials

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

Bunder Sebail Alshammari^{1,*} and Khaled Nasser Alfraidi¹

¹*Department of Arabic Language, College of Arts and Letters, University of Ha'il, Ha'il, Saudi Arabia*

*Corresponding author: ban.alshammari@uoh.edu.sa

This document consolidates the study's three research instruments and its complete analytic dataset in a single reference. The corpus comprises twelve authenticated judgments (Cases A–L) from Eastern Province judicial circuits, 1432–1435 AH (2011–2014), adjudicated under the Anti-Cyber Crime Law. The design is qualitative and information-rich: reported frequencies are descriptive characterisations of a small purposive corpus, not inferential population estimates. All identifiers are anonymised; no party-identifying details are stored.

Contents. The materials are organised as: the case-selection rubric (Instrument 1); the forensic-pragmatic coding scheme (Instrument 2); the judicial-uptake scale (Instrument 3); a variable dictionary; the twelve-case master dataset; a worked application of the Multidimensional Discourse Integration Model (MDIM); the segment-level inter-coder reliability record and Cohen's κ computation; and descriptive strategy, uptake, and co-occurrence distributions.

Machine-readable file	Contents
<code>..._instrument_and_data.xlsx</code>	Eleven-sheet workbook (instruments, dictionary, data, statistics).
<code>cybercrime_corpus_master.sav</code>	SPSS: 12 cases $\times$ 11 coded variables (value-labelled).
<code>intercoder_reliability.sav</code>	SPSS: 50 coded segments $\times$ two coders.

The uploaded `intercoder_reliability_1.sav` is byte-for-byte identical to `intercoder_reliability.sav` and is treated here as a single file.

1 Instrument 1 — Case selection and inclusion rubric

Screening reduced the forty-seven cybercrime judgments in the source volume to nineteen cases with explicit defendant responses to digital evidence, and then to the twelve analytic cases that satisfied every criterion below.

Criterion	Requirement	Verification
Legal basis	Adjudicated under the Anti-Cyber Crime Law (Royal Decree M/17).	Yes / No
Technical trace	Evidence involves an IP address, MAC address, or account log.	Yes / No
Defence type	Defendant explicitly invokes shared infrastructure (Wi-Fi, household PC, shared account).	Yes / No
Discursive data	Judgment includes verbatim or detailed paraphrased speech of the defendant.	Yes / No
Judicial logic	Judge explicitly discusses doubt (shubha), intent (niyya), or evidence weight.	Yes / No

2 Instrument 2 — Forensic-pragmatic coding scheme

Five defence strategies structure the coding of every extracted segment. Arabic linguistic triggers are illustrative diagnostic cues, not exhaustive lists.

#	Code	Strategy	Operational definition	Arabic triggers (examples)	Decision rule	Jurisprudential hinge
1	CAT-DEN	Categorical denial	Complete rejection of the act and of authorship.	<i>lam af'al (I did not do); ma li 'alaqa (I have no connection).</i>	Dominant move denies the act itself rather than the trace-to-actor inference.	Sufficiency and decisiveness of proof
2	SAB-TRANS	Shared-access blame transfer	Concedes the trace location but names other users with access.	<i>al-shabaka mushtaraka (shared network); ahl al-bayt (family members).</i>	Defendant admits the environmental link yet foregrounds alternative users.	shubha (legal doubt)
3	EVID-DISP	Evidential displacement	Attacks the trace-to-actor inference itself.	<i>al-taqrir la yuthbit (the report does not prove [me]); mujarrad ittisal (merely a connection).</i>	Central move contests the granularity or reach of the technical report.	Threshold of decisive proof
4	MOR-REL	Moral-religious credibility work	Uses piety and character to bolster truth-claims.	<i>Wallahi (by God); akhsha Allah (I fear God); laysa min khuluqi (not my character).</i>	Moral-religious positioning is the salient support for the denial.	niyya and credibility
5	ALT-CAUS	Alternative-causation narrative	Proposes a specific external event such as hacking or framing.	<i>ikhтираq (hacking); talfiq (framing / fabrication).</i>	Defence advances a positive alternative causal story.	Alternative causation, shubha, intent

Assignment procedure. One *primary* strategy is assigned per case by three ordered rules: (1) frequency within the defendant's response; (2) explicitness of judicial evaluation; (3) argumentative centrality to the final ruling. Secondary strategies are recorded when present. **Reliability.** Two coders independently coded 50 extracted segments; Cohen's $\kappa = 0.92$ (almost perfect, Landis & Koch 1977); disagreements were adjudicated by a third reviewer.

3 Instrument 3 — Judicial uptake evaluation scale

Each judgment receives one uptake level recording how the court treated the shared-access denial.

Level	Judicial uptake category	Operational definition
0	Rejection	Judge treats the technical trace as conclusive and dismisses the denial as a bare claim.
1	Procedural recognition	Judge acknowledges shared access but finds it outweighed by other evidence.
2	Mitigation / doubt	Judge admits shubha regarding the specific actor and reduces the ta'zir sentence.
3	Non-conviction	Judge finds the evidence insufficient for individual attribution; dismissal or acquittal.

4 Variable dictionary

cybercrime_corpus_master.sav

Variable	Label	Value codes
case_num	Case number (1–12)	1–12
case_id	Case identifier (A–L)	A–L (string)
year_hijri	Year of judgment (Hijri)	1432–1435
offence_code	Dominant offence context	1=Defamation / posting attribution; 2=Privacy / reputational posting; 3=Online threat / abusive message; 4=Blackmail / coercive communication; 5=Unauthorised access allegation; 6=Technical-report attribution dispute; 7=Account-use attribution dispute; 8=Hacking / framing scenario
trace_code	Technical trace type	1=IP Log (Household); 2=PC Forensic Image; 3=Mobile Device Log; 4=Account Metadata; 5=IP Log (Open Wi-Fi); 6=Social Media Log; 7=Router Admin Log; 8=Forensic Report; 9=Login History; 10=Device Ownership; 11=Account Logs; 12=Remote Access Log
feature_code	Shared-access feature	1=Household router / network; 2=Shared family computer; 3=Communal mobile / device access; 4=Shared account / device access; 5=Open or weakly secured Wi-Fi; 6=IP log without user-level corroboration; 7=Device logs without individual identification; 8=Unknown third-party network exploitation
shared_access	Shared digital infrastructure involved	0=No; 1=Yes
primary_code	Primary defence strategy	1=CAT-DEN (Categorical denial); 2=SAB-TRANS (Shared-access blame transfer); 3=EVID-DISP (Evidential displacement); 4=MOR-REL (Moral-religious credibility work); 5=ALT-CAUS (Alternative-causation narrative)
hinge_code	Islamic legal hinge invoked	1=Shubha (legal doubt); 2=Bayyinah (proof sufficiency); 3=Istishab (presumption); 4=Niyya (intent); 5=Ta'zir discretion; 6=Yaqin (certainty); 7=Tazkiyah (credibility)
uptake_level	Judicial uptake level (0–3)	0=Rejection; 1=Procedural recognition; 2=Mitigation / doubt; 3=Non-conviction
conviction	Conviction recorded	0=No; 1=Yes

intercoder_reliability.sav

Variable	Label	Value codes
segment_id	Coded defence segment ID	S01–S50 (string)
case_id	Case identifier (A–L)	A–L (string)
coderA_code	Coder A (adjudicated) strategy	1=CAT-DEN (Categorical denial); 2=SAB-TRANS (Shared-access blame transfer); 3=EVID-DISP (Evidential displacement); 4=MOR-REL (Moral-religious credibility work); 5=ALT-CAUS (Alternative-causation narrative)
coderB_code	Coder B strategy	1=CAT-DEN (Categorical denial); 2=SAB-TRANS (Shared-access blame transfer); 3=EVID-DISP (Evidential displacement); 4=MOR-REL (Moral-religious credibility work); 5=ALT-CAUS (Alternative-causation narrative)
agreement	Coders agree (1 = yes)	0=No; 1=Yes

5 Master analytic dataset — twelve judgments (Cases A–L)

Case	Yr AH	Yr CE	Offence context	Trace type	Shared-access feature	Primary	Islamic hinge	Uptake	Conv.	Judicial outcome (detail)
A	1433	2012–2013	Defamation / posting attribution	IP Log (Household)	Household router / network	SAB-TRANS	Shubha (legal doubt)	2 — Mitigation / doubt	No	Mitigation / doubt-constrained
B	1432	2011–2012	Defamation / posting attribution	PC Forensic Image	Shared family computer	CAT-DEN	Bayyinah (proof sufficiency)	0 — Rejection	Yes	Conviction (strong corroboration)
C	1432	2011–2012	Privacy / reputational posting	Mobile Device Log	Communal mobile / device access	CAT-DEN	Istishab (presumption)	0 — Rejection	Yes	Conviction (exclusive access; inconclusive denial)
D	1433	2012–2013	Online threat / abusive message	Account Metadata	Shared account / device access	CAT-DEN	Niyya (intent)	0 — Rejection	Yes	Conviction (behavioural / corroborated)
E	1433	2012–2013	Defamation / posting attribution	IP Log (Open Wi-Fi)	Open or weakly secured Wi-Fi	SAB-TRANS	Shubha (legal doubt)	2 — Mitigation / doubt	No	Mitigation (unsecured network)
F	1434	2013	Blackmail / coercive communication	Social Media Log	Shared account / device access	SAB-TRANS	Ta'zir discretion	2 — Mitigation / doubt	No	Mitigation (ta'zir discretion)
G	1434	2013	Unauthorised access allegation	Router Admin Log	Household router / network	SAB-TRANS	Shubha (legal doubt)	3 — Non-conviction	No	Non-conviction (multiple users; doubt-based)
H	1434	2013	Technical-report attribution dispute	Forensic Report	IP log without user-level corroboration	EVID-DISP	Yaqin (certainty)	3 — Non-conviction	No	Non-conviction (trace gap; insufficient detail)
I	1435	2014	Account-use attribution dispute	Login History	Device logs without individual identification	EVID-DISP	Shubha (legal doubt)	2 — Mitigation / doubt	No	Mitigation / non-conviction (granularity)
J	1435	2014	Blackmail / coercive communication	Device Ownership	Shared account / device access	MOR-REL	Tazkiyah (credibility)	0 — Rejection	Yes	Conviction (physical evidence; ambiguity resolved)
K	1435	2014	Privacy / reputational posting	Account Logs	Communal mobile / device access	MOR-REL	Niyya (intent)	2 — Mitigation / doubt	No	Mitigation (character and intent)
L	1435	2014	Hacking / framing scenario	Remote Access Log	Unknown third-party network exploitation	ALT-CAUS	Shubha (legal doubt)	3 — Non-conviction	No	Non-conviction (alternative causation not excluded)

Every case involves shared digital infrastructure (*shared_access*=Yes). “Uptake” gives the level and its label; “Conv.” is whether a conviction was recorded.

6 Multidimensional Discourse Integration Model — worked application to Case G

The MDIM links five analytic layers from technical input to judicial output. Case G (unauthorised-access allegation; router admin log; household network) illustrates the full mapping.

MDIM layer	Case G coding / analytic output
Technical input	IP address identifies the subscriber's DSL line at a specific timestamp.
Forensic-pragmatic layer	Defendant uses SAB-TRANS: "the modem is in the majlis (guest room); many visitors and my brothers have the password."
Evidentiary evaluation	Court notes that the forensic report confirms the source but cannot confirm the MAC address of the specific handset used.
Islamic reasoning layer	Judge invokes al-hudud tudra'u bi-l-shubuhah (punishments are warded off by doubts), applied here to ta'zir.
Output	Non-conviction for the specific charge: the perpetrator cannot be individualised among a group of potential users.

7 Inter-coder reliability — segment-level codings (n = 50)

Coder A is the adjudicated coding. Disagreements (×) occur at S06, S31, and S42; all other segments agree.

Seg	Case	Coder A	Coder B	Agr.	Seg	Case	Coder A	Coder B	Agr.
S01	A	CAT-DEN	CAT-DEN	✓	S26	F	SAB-TRANS	SAB-TRANS	✓
S02	A	CAT-DEN	CAT-DEN	✓	S27	G	SAB-TRANS	SAB-TRANS	✓
S03	A	CAT-DEN	CAT-DEN	✓	S28	G	SAB-TRANS	SAB-TRANS	✓
S04	A	CAT-DEN	CAT-DEN	✓	S29	G	EVID-DISP	EVID-DISP	✓
S05	B	CAT-DEN	CAT-DEN	✓	S30	G	EVID-DISP	EVID-DISP	✓
S06	B	CAT-DEN	SAB-TRANS	×	S31	H	EVID-DISP	CAT-DEN	×
S07	B	CAT-DEN	CAT-DEN	✓	S32	H	EVID-DISP	EVID-DISP	✓
S08	B	CAT-DEN	CAT-DEN	✓	S33	H	EVID-DISP	EVID-DISP	✓
S09	B	CAT-DEN	CAT-DEN	✓	S34	H	EVID-DISP	EVID-DISP	✓
S10	C	CAT-DEN	CAT-DEN	✓	S35	I	EVID-DISP	EVID-DISP	✓
S11	C	CAT-DEN	CAT-DEN	✓	S36	I	EVID-DISP	EVID-DISP	✓
S12	C	CAT-DEN	CAT-DEN	✓	S37	I	EVID-DISP	EVID-DISP	✓
S13	C	CAT-DEN	CAT-DEN	✓	S38	I	MOR-REL	MOR-REL	✓
S14	D	SAB-TRANS	SAB-TRANS	✓	S39	J	MOR-REL	MOR-REL	✓
S15	D	SAB-TRANS	SAB-TRANS	✓	S40	J	MOR-REL	MOR-REL	✓
S16	D	SAB-TRANS	SAB-TRANS	✓	S41	J	MOR-REL	MOR-REL	✓
S17	D	SAB-TRANS	SAB-TRANS	✓	S42	J	MOR-REL	SAB-TRANS	×
S18	E	SAB-TRANS	SAB-TRANS	✓	S43	K	MOR-REL	MOR-REL	✓
S19	E	SAB-TRANS	SAB-TRANS	✓	S44	K	MOR-REL	MOR-REL	✓
S20	E	SAB-TRANS	SAB-TRANS	✓	S45	K	MOR-REL	MOR-REL	✓
S21	E	SAB-TRANS	SAB-TRANS	✓	S46	K	ALT-CAUS	ALT-CAUS	✓
S22	E	SAB-TRANS	SAB-TRANS	✓	S47	L	ALT-CAUS	ALT-CAUS	✓
S23	F	SAB-TRANS	SAB-TRANS	✓	S48	L	ALT-CAUS	ALT-CAUS	✓
S24	F	SAB-TRANS	SAB-TRANS	✓	S49	L	ALT-CAUS	ALT-CAUS	✓
S25	F	SAB-TRANS	SAB-TRANS	✓	S50	L	ALT-CAUS	ALT-CAUS	✓

8 Cohen's κ — inter-coder reliability computation

Confusion matrix (rows = Coder A, columns = Coder B)

A \ B	CAT-DEN	SAB-TRANS	EVID-DISP	MOR-REL	ALT-CAUS	Row
CAT-DEN	12	1	0	0	0	13
SAB-TRANS	0	15	0	0	0	15
EVID-DISP	1	0	8	0	0	9
MOR-REL	0	1	0	7	0	8
ALT-CAUS	0	0	0	0	5	5
Col	13	17	8	7	5	50

Statistics

Quantity	Value
Observed agreement (p_o)	0.9400
Expected agreement (p_e)	0.2308
Cohen's κ	0.9220
Agreements / total	47 / 50
Disagreements	3 (S06, S31, S42)
Interpretation	Almost perfect (Landis & Koch 1977)

$\kappa = (p_o - p_e) / (1 - p_e)$. Marginals: Coder A 13, 15, 9, 8, 5; Coder B 13, 17, 8, 7, 5 across CAT-DEN, SAB-TRANS, EVID-DISP, MOR-REL, ALT-CAUS.

9 Descriptive distributions (N = 12)

Primary defence strategy

Primary defence strategy	Frequency	Share
CAT-DEN (Categorical denial)	3	25.0%
SAB-TRANS (Shared-access blame transfer)	4	33.3%
EVID-DISP (Evidential displacement)	2	16.7%
MOR-REL (Moral-religious credibility work)	2	16.7%
ALT-CAUS (Alternative-causation narrative)	1	8.3%
Total	12	100.0%

Judicial uptake and convictions

Judicial uptake level	Frequency	Share
0 — Rejection	4	33.3%
1 — Procedural recognition	0	0.0%
2 — Mitigation / doubt	5	41.7%
3 — Non-conviction	3	25.0%
Convictions recorded	4	33.3%

Primary × secondary strategy co-occurrence

Primary \ Secondary	CAT-DEN	SAB-TRANS	EVID-DISP	MOR-REL	ALT-CAUS
CAT-DEN (n=3)	–	1	0	1	1
SAB-TRANS (n=4)	2	–	2	1	0
EVID-DISP (n=2)	1	1	–	0	0
MOR-REL (n=2)	1	1	0	–	0
ALT-CAUS (n=1)	0	0	1	0	–

Descriptive counts of secondary strategies observed alongside each primary strategy; diagonal is not applicable. Layered denial is common, so row sums may exceed the primary-strategy frequency.