Scholar Insight Journal
https://scholarinsightjournal.com/
Volume.3, Issue.1 (March-2025)

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X

Shariah Analysis of Qanun-E-Shahadat Order and Application of Classical Qarīna Doctrines On Electronic-Evidence

Dr. Hafsa Abbasi
Lecturer, Shariah, Allama Iqbal Open University Islamabad. This article is based on my post-doctoral project from IRI Islamabad hafsa.abbasi@aiou.edu.pk

Abstract

The advent of digital technology has transformed the evidentiary landscape, presenting unique challenges for legal systems grounded in classical doctrines. This article undertakes a Shariah-based analysis of Pakistan's Qanun-e-Shahadat Order (QSO), 1984, with particular focus on its treatment of electronic evidence. It examines how traditional Islamic principles of proof, especially the classical doctrine of *Qarīna* (presumptions and inferential evidence), can inform the admissibility, credibility, and weight of electronic records such as emails, digital contracts, and forensic data. By juxtaposing the QSO provisions with classical *qarīna* concepts, the study identifies convergences and gaps, highlighting areas where contemporary judicial practice may benefit from Shariah-guided reasoning. The article also discusses methodological challenges in interpreting electronic evidence under both statutory and Shariah frameworks, emphasizing principles such as certainty (*yaqin*), corroboration, and avoidance of unjust assumptions. Through case law analysis and doctrinal comparison, it proposes a harmonized approach that respects the integrity of Islamic evidentiary standards while addressing the technical complexities of digital proof. The findings underscore the potential for classical *qarīna* doctrines to enrich modern evidentiary evaluation, ensuring justice, reliability, and fairness in the digital age.

Keywords: Qanun-e-Shahadat Order, Shariah, electronic evidence, Qarīna, Islamic jurisprudence.

Introduction: The evidentiary challenge of the digital age

Pakistan's Qanun-e-Shahadat Order, 1984 (QSO) declares an ambition to consolidate the law of evidence "in conformity with the injunctions of Islam as laid down in the Holy Quran and Sunnah," while also functioning as a modern statute for courts operating inside a complex state. At the same time, modern litigation increasingly turns on "evidence that has become available because of modern devices or techniques"—a phrase used directly by QSO Article

164. The contemporary question is not merely whether electronic evidence (WhatsApp messages, emails, cloud logs, CCTV, biometric access logs, location data, transaction records) is "admissible," but whether Pakistan's evidentiary regime can absorb digital material in a way that is both procedurally fair and normatively coherent with Islamic jurisprudential ideals of truth-seeking (iẓhār al-ḥaqq), justice (ʿadl), and avoidance of wrongful attribution (ihtiyāṭ in uqubāt).

Classical Islamic law is sometimes portrayed as rigidly tied to oral testimony and oath; yet historical scholarship shows a more complicated institutional reality in which circumstantial indicators (qarāʾin) and "clues through indications" (al-amārāt al-dālla wa-shawāhid al-aḥwāl) played a recognized role, sometimes formally and sometimes through parallel institutions such as maẓālim. Hossein Modarressi, discussing early Islamic adjudication, highlights a core distinction: ordinary courts were expected to rely mainly on oral testimony, confession, and oath, while maẓālim authorities could look for "obscure and concealed" evidence and use tools "not available to judges," including reliance on circumstantial indicators. The lesson for modern electronic evidence is immediate: digital traces are often not the kind of "direct oral testimony" that classical procedural theory privileged, yet they may function as powerful qarīna—sometimes stronger than memory-based witness narration—if courts learn how to evaluate provenance, integrity, and the risk of fabrication.

This article offers a Shariah-oriented analysis of the QSO's doctrinal structure and proposes a framework for applying classical qarīna reasoning to electronic evidence under Article 164, while remaining faithful to the statute's broader architecture for relevancy, oral proof, documentary proof, presumptions, and burden of proof.

1. QSO as an "Islamized" statute of proof: what the text actually commits to

Any Shariah analysis must begin with what the QSO actually enacts rather than what lawyers assume it means. The QSO defines "evidence" as both (i) statements made by witnesses (oral evidence) and (ii) documents produced for inspection (documentary evidence). It defines "document" broadly as "any matter expressed or described upon any substance," intended to record that matter, and gives examples that include printed or photographed material. In doctrinal terms, this definition supplies an interpretive bridge: electronic records are routinely "expressed" upon a medium (storage chips, servers, drives), and often appear in court as printed screenshots, logs, images, or certified extracts—thus naturally entering the QSO's documentary universe even if the statute was drafted before smartphones.

At the same time, QSO provides a strong model of directness for oral evidence: if a fact is seen, the witness must say he saw it; if heard, he must say he heard it; and so forth. This is

one reason why electronic material creates tension: a witness may not "see" the underlying event, yet may see a screen output or print-out. Here, Shariah-informed reasoning becomes relevant because classical jurists distinguished between (a) the *source* of knowledge, (b) the *certainty* of knowledge, and (c) the *legal weight* assigned to various forms of proof—especially when the proof is not "testimony" in the strict sense.

QSO Article 164 is the statute's explicit portal for technical modernity: "In such cases as the Court may consider appropriate, the Court may allow to be produced any evidence that may have become available because of modern devices or techniques." The text is deliberately open-textured—"may," "appropriate," and "modern devices or techniques." That openness is not a weakness; it is a delegation of discretion to the judge to admit modern forms of proof where the standard categories (oral testimony, classic documents) would otherwise struggle to capture relevant truth. In Islamic legal theory, discretion in evidence-evaluation is not foreign; rather, its legitimacy depends on disciplined use—ensuring that discretionary reception of qarāʾin does not collapse due process or create pathways for injustice.

2. Classical qarīna and the institutional memory of maẓālim

Modarressi's historical account is important because it corrects a simplistic narrative that "Islamic law rejects circumstantial evidence." Author notes that ordinary courts "acted strictly on the basis of oral testimony including voluntary confession and oath, and were not supposed to use any other evidence." Yet he also emphasizes that maẓālim courts would examine cases in context and consider internal and external indications, including circumstantial evidence, precisely because the system could not always function with oral proof alone. This is more than history: it is a jurisprudential idea about *institutional competence*. Some forums operate with stricter procedural constraints; others exist to remedy injustice when strict proof cannot be produced, especially where wrongdoing is concealed.

That distinction maps surprisingly well onto modern electronic evidence. Digital wrongdoing often involves concealment, replication, remote deletion, impersonation, and manipulation of logs—meaning that insisting on "two upright eyewitnesses who saw the event" can make justice impossible in many modern disputes (cyber-fraud, harassment, online threats, coordinated deception, digital financial crimes). Modarressi reports sources where officials responsible for maẓālim "look for clues through indications and circumstantial evidence … means that are not available to judges." In a contemporary court system, the analog of those "means" is not intimidation; it is lawful investigative technique: forensic imaging, metadata extraction, audit logs, network traces, device correlation, and chain-of-custody documentation—tools that help a judge responsibly treat a digital trace as a reliable qarīna rather than a mere allegation.

Modarressi also records two "exceptions" discussed by jurists within ordinary legal theory: (1) allowing a judge to act on personal knowledge (ʿilm al-qāḍī) understood conventionally as knowledge from direct witnessing, and (2) the position of several jurists—especially Ibn al-Qayyim—who argued that limiting proof to testimony and oaths wastes rights, emboldens wrongdoers, and makes the Sharīʿa appear nonfunctional. Whatever one's school position, the second strand is conceptually aligned with a controlled embrace of digital qarāʾin: it frames evidence rules as instruments for realizing justice, not barriers that systematically protect sophisticated deception.

3. Electronic Evidence as Qarīna: the "Logic of Inference" and the problem of reliability

A key misunderstanding in digital litigation is treating "electronic evidence" as one thing. Modern evidence in digital form ranges from human-authored content (messages, documents) to software-generated records (system logs, access events, transaction counters), to hybrid records where human input is processed by software logic. This matters because the Shariah-logic of qarīna is fundamentally inferential: a qarīna does not "testify," but it points, supports, corroborates, or undermines a narrative—like footprints, possession, timing, opportunity, pattern, or inconsistent conduct. The QSO already recognizes inferential relevance widely: facts forming part of the same transaction, facts showing motive or conduct, facts explaining other facts, and facts that make the existence of a fact in issue "highly probable or improbable." These relevancy gateways are structurally compatible with qarīna reasoning.

But inference must be disciplined by reliability assessment. The Stephen Mason, in his book, *Electronic Evidence* stresses that electronic evidence has distinctive characteristics: dependence on machinery and software, speed of change, volume and replication, and the central role of metadata. It also highlights authenticity issues: in digital contexts, proving authenticity is often about demonstrating identity and integrity (wholeness, soundness, unaltered state), and sometimes shifting attention from an "original document" to the integrity of the record-keeping system. In Shariah terms, this is not alien: classical jurists used concepts of ẓann (probabilistic belief) versus yaqīn (certainty), and developed procedural safeguards to prevent punishment on doubtful proof. A modern Islamic-legal sensibility would therefore ask: what level of confidence does a given digital artifact generate, and is the level adequate for the legal consequence sought (civil liability, discretionary taʿzīr, or the highest criminal thresholds)?

The authenticity challenges may include claims of alteration, manipulation, damage, identity disputes (who authored a message), and attacks on the reliability of the generating

program. In a Shariah-informed qarīna approach, the court would not treat these as mere technical quibbles; they are precisely the "hidden defects" that can turn a seemingly strong indicator into a misleading sign. Thus, a controlled system of digital qarīna requires attention to: provenance (where the data came from), continuity of custody (who handled it), integrity controls (hashing, secure preservation), and contextual corroboration (does it match other traces).

4. Article 164 as a gateway: harmonizing modern devices with classical evidentiary ethics

Article 164 gives Pakistani judge's discretion to "allow to be produced any evidence" made available by modern devices or techniques. A Shariah-analysis should treat this not as a purely procedural clause, but as a *moral-legal delegation* to use new means to reach justice, while staying inside the ethical constraints of truthful proof and fair process.

Three points are critical.

First, Article 164 allows modern evidence to be produced, but questions of relevancy, authenticity, primary/secondary proof, and evaluation remain governed by the statute's general principles. So, admitting a WhatsApp screenshot under Article 164 does not mean the court must accept it as true; it only means the court may consider it as an evidentiary item within the case.

Second, Article 164 should be read alongside the QSO's robust relevancy structure. The QSO already allows facts that support or rebut an inference, explain conduct, establish identity, fix time and place, or show motive and preparation. These categories naturally absorb digital traces: location records can fix place; metadata can fix time; login logs can establish identity-linked access; message timing can show preparation or subsequent conduct.

Third, Article 164 can be conceptualized as the statutory "space" where qarīna may be formally operationalized. Classical doctrine, as Modarressi reports, often treated circumstantial evidence as outside strict ordinary adjudication, yet practically essential, and sometimes institutionally routed through maẓālim or through juristic arguments (e.g., Ibn al-Qayyim) urging broader consideration of indicators to prevent rights being lost. Article 164 functions like a modern legislative acknowledgment of that need: it permits courts to consider new forms of indicia, without pretending they are identical to eyewitness testimony.

5. A proposed Shariah-consistent method for digital Qarīna

To apply classical qarīna doctrines responsibly to electronic evidence under QSO, courts and lawyers need a method that is (a) principled, (b) technically literate, and (c) sensitive to different burdens/standards in different kinds of cases. The following method is implied by the combined reading of QSO's structure and modern electronic evidence scholarship:

1. Classify the digital item: human-authored content, machine-generated log, or hybrid output.
2. Identify the claim the item supports: identity, time, place, authorship, intention, conduct, transaction, or system state.
3. Establish provenance and custody: how collected, by whom, and whether continuity is credible.
4. Test integrity: whether alteration is plausible; consider metadata, system controls, and preservation method.
5. Corroborate with other qarāʾin: convergence of independent traces strengthens inference; inconsistency weakens it.
6. Match evidentiary strength to legal consequence: higher consequences require stronger, less contestable indicators, echoing classical caution where doubt blocks severe outcomes.

6. Making Article 164 workable: linking "modern devices" to the QSO's proof-structure

A common mistake in Pakistani practice is to treat Article 164 as if it is a self-contained "digital evidence law." It is not. Article 164 is better understood as a gate-opening clause that permits courts to receive new categories of proof, while leaving questions of *how* to prove, *how much* to prove, and *how to evaluate* evidence to the rest of the QSO.

This is not only a technical reading; it is Shariah-coherent. Modarressi shows that where strict courtroom proof rules relied heavily on oral testimony and oath, other institutions (like maẓālim) and some juristic viewpoints made room for wider consideration of "indications and circumstantial evidence." Article 164 resembles a legislative acknowledgment of the same need: not every modern wrong can be proven through classical testimonial forms, yet justice still demands that courts consider the best available indicia—provided those indicia are screened for reliability.

To operationalize Article 164, judges routinely anchor digital material in four clusters of QSO doctrine:

- Relevancy and inference (Articles 18–29): the QSO already admits facts that explain a transaction, show conduct, establish identity, fix time/place, or make a fact in issue more probable.
- Documentary proof (Articles 72–77): the QSO sets a default preference for primary evidence but allows secondary evidence in defined circumstances, including where copies are made by "microfilming or other modern devices" due to volume/bulk.
- Presumptions (e.g., Articles 90–92, 98–100, 129): the QSO contains presumptions for certified copies, documents kept under law from proper custody, and even telegraphic messages (with an important limitation about authorship).
- Expert support (Articles 59–60, plus related rules): expert opinion is explicitly relevant, and so are the "grounds" of that opinion—this is crucial for digital forensic testimony.

In a Shariah-informed approach, these clusters become the doctrinal machinery through which electronic evidence can be treated as qarīna (an indicator) with controlled weight, rather than as an uncontrolled substitute for testimony.

7. Primary/secondary evidence in the digital context: a Shariah-friendly reading

The QSO's documentary proof provisions turn on the primary/secondary distinction. Primary evidence is "the document itself produced for inspection." Secondary evidence includes certified copies, mechanical copies ensuring accuracy, copies compared with originals, and even oral accounts by someone who has seen the document.

Digital material complicates "the document itself." Is "the document" the phone? the file? the server log? the screenshot? a printout? The *Electronic Evidence* text explains why this is hard: digital data is dependent on machinery and software, can be replicated perfectly, and is frequently understood through metadata rather than visible "content" alone. In practice, a screenshot may be a *representation* of data, but it can also be easy to manipulate, so the best evidentiary posture is often to treat the screenshot as secondary unless it is backed by better provenance (export logs, device acquisition, hash verification, or platform records).

Importantly, the QSO itself already anticipates modern copying: Article 76(d) explicitly allows secondary evidence where, due to volume/bulk, copies are made by "microfilming or other modern devices." That phrase can be read as a legislative acceptance that modern record systems may not be produced physically in court as "the original," and that accurate mechanical reproduction can be a legitimate path to proof. A Shariah-consistent inference is that the law aims at truthful reproduction rather than fetishizing a physical "original"—the

ethical priority is avoiding tazwīr (falsification) and preventing rights from being wasted due to impractical procedural demands.

8. Presumptions and digital evidence: lessons from "telegraph messages"

The QSO's presumption provisions show how Pakistani law can accept mediated communication without abandoning caution.

Article 98 (telegraphic messages) allows the court to presume that a message delivered corresponds to the message handed in for transmission, but the court shall not presume who delivered it for transmission. This structure is extremely instructive for electronic evidence:

- Courts may accept that a platform reliably transmits/stores messages in normal operation (a limited technical presumption).
- Courts should be cautious about attributing authorship/agency solely from the existence of a message (no automatic presumption of "who typed it").

This mirrors the Shariah logic of qarīna: a sign may establish that "something happened" in a system, but it may not conclusively establish "who did it" unless strengthened by corroboration (device possession, account control, login records, SIM ownership, location evidence, admissions, conduct, or forensic linkage).

The QSO also contains strong presumptions about certified copies and about documents required by law to be kept if produced from "proper custody." As digital governance expands, many crucial electronic records are in fact "documents directed by law to be kept" (for example, official registries, regulated logs, licensed telecom records, etc.), and Article 92 provides a presumption of genuineness when those are produced from proper custody. This, too, can be framed as Shariah-consistent: official recordkeeping (ḥifẓ al-ḥuqūq) is a public interest (maṣlaḥa) function, but presumptions must remain rebuttable when credible doubt arises.

9. Authentication as modern tazkiyah: "uprightness" becomes "integrity"

Classical Islamic procedure placed heavy emphasis on witness credibility and uprightness (ʿadālah), often tested through tazkiyah procedures (validation of witnesses). Modarressi notes how testimonial processes could become burdensome and delay justice, with extensive scrutiny of witness wording and reliability. In the electronic evidence environment, the moral equivalent of tazkiyah is not moral character checking; it is integrity checking—of the data, the device, and the collection method.

The *Electronic Evidence* text devotes extensive attention to authentication: the need to show that a digital object is what it is claimed to be, and that it has not been tampered with. It also flags how electronic evidence can be challenged (alteration, wrong file/version, metadata stripping, provenance gaps) and why preservation method matters. If Pakistani courts view electronic evidence through the qarīna lens, authentication becomes the condition for the qarīna to be weighty rather than deceptive.

A Shariah-oriented courtroom practice can therefore treat the following as modern "tazkiyah" elements for digital exhibits:

- Provenance narrative: who obtained it, from where, and under what authority.
- Preservation narrative: how it was preserved, copied, and secured against later change.
- Technical grounding: metadata, timestamps, hash values, system logs, export methods, and whether the data could plausibly have been altered without traces.
- Corroborative ecology: whether other facts (conduct, opportunity, transaction chains) align with the digital artifact.

This approach also answers a key Shariah concern: electronic evidence should not become a tool for *qذف*-like wrongful accusation or reputational harm based on easy fabrication. Instead, courts should require that digital artifacts reach a threshold of integrity before being treated as strong indicia.

10. Expert opinion and forensic method: embedding "ilm" into the QSO

The QSO explicitly recognizes expert opinion as relevant (Article 59) and makes supporting/inconsistent facts relevant when expert opinion is relevant (Article 60). It also recognizes that the *grounds* of an opinion are relevant (Article 65), including experiments. These provisions are vital for digital evidence because electronic proof often cannot be responsibly evaluated without explaining technical grounds: acquisition method, metadata interpretation, log meanings, software behavior, and whether alternative hypotheses exist.

The *Electronic Evidence* text reinforces that reliability assumptions about computers/software are complex; it discusses the presumption that computers are reliable and how such a presumption can be challenged, and it highlights the need to examine critically any suggestion of malfunction and its relevance to the specific record. Translating this into a Shariah-coherent doctrine: the judge is not asked to "believe the machine" as if it were a

morally accountable witness; the judge is asked to evaluate a trace produced by machinery through expert explanation and adversarial testing, then assign weight as a qarīna.

In practical Pakistani terms, Article 59 + Article 65 can support a court practice where:

- Forensic experts explain not only conclusions ("this screenshot is edited") but also methods and grounds ("hash mismatch," "metadata inconsistent," "compression artifacts," "log discontinuity," "export tool limitations").
- Opposing parties test those grounds through cross-examination and competing expertise, ensuring the process remains just rather than technocratic.

11. Burden of proof and "facts especially within knowledge": digital control matters

Electronic evidence disputes often pivot on control: who had the device, who controlled the account, who had passwords, who could access cloud backups, who could delete logs. The QSO contains a powerful doctrinal tool here: Article 122 shifts the burden for any fact "especially within the knowledge" of a person onto that person. This can be decisive in modern cases.

Examples (illustrative, not exhaustive):

- If a party claims a WhatsApp account was hacked, the details of account security, device custody, SIM control, and password practices may be "especially within" that party's knowledge.
- If an employer relies on access logs from its own system, the employer is best placed to explain system design, log retention, admin access, and audit policies (again, facts within special knowledge).

This aligns with classical Shariah instincts about allocating evidentiary responsibilities to the party best positioned to clarify the truth, and it reduces the risk that sophisticated actors exploit complexity to create unanswerable doubt.

12. Applied examples: using classical qarīna logic with modern electronic artifacts

To make the theory concrete, consider how a court could treat common electronic exhibits as qarāʾin, using the QSO structure and electronic evidence best practices.

Example A: WhatsApp screenshot alleging threats

A screenshot by itself is a weak qarīna because it is easy to fabricate and may lack metadata context. Under Article 164, the court may allow it to be produced, but then evaluate it under the QSO's general rules. Strengthening steps (each adds corroborative qarāʾin):

- Produce the phone for inspection or forensic extraction (moving toward primary evidence).
- Show chat export and message IDs/metadata, if available, and preserve device image with integrity controls.
- Corroborate timing with call detail records, location, or conduct evidence relevant under Articles 19–22.
- Address authorship cautiously (telegraph analogy): don't presume the sender solely from the message; link to device/account control through additional indicators.

Example B: CCTV footage of an incident

Video is often treated as strong because it "shows" events, but digital video is still subject to authenticity issues (editing, missing segments, transcoding). A Shariah-aligned court would treat it as strong qarīna if integrity is established:

- Provenance: who retrieved the recording, from which DVR/NVR, with what safeguards.
- Continuity: who held it before court; gaps increase doubt.
- Technical grounding: timestamps, camera system settings, and whether export/transcoding could alter content.

Under QSO, these integrity facts become relevant both through expert opinion (Articles 59–65) and through the judge's general power to require proper proof before relying on the item.

Example C: Bank/ERP transaction logs (internal business systems)

Digital business records can be decisive but may embed spreadsheet risk, software logic risk, and access-control risk. A qarīna-based method pushes the court to ask: are we seeing a reliable record of an event, or a potentially manipulated output?

- Request system audit logs, role-based access records, and record-generation process descriptions (expert grounds).

- Use Article 122 "special knowledge" to press the controlling organization to explain the system.
- Use corroboration: independent bank statements, emails, delivery records—QSO relevancy articles allow assembling a "web of indicia."

13. Addressing objections: "Isn't this just hearsay?"

In common-law terms, electronic records sometimes resemble hearsay: they are out-of-court statements offered for truth. But the materials you provided highlight a deeper point: some digital outputs are *not* human statements at all; they may be machine-generated logs or system states. Even human-authored messages, when authenticated, can be treated as admissions, conduct evidence, or corroboration under the QSO's relevancy architecture.

From a Shariah perspective, the key is not to force digital evidence into "oral testimony" categories; it is to treat it as qarīna and evaluate weight according to reliability. Modarressi's discussion shows that ignoring contextual and circumstantial indicators can cause rights to be wasted, which is itself a serious injustice. Therefore, the Shariah-consistent response is not "reject digital traces"; it is "accept them with disciplined safeguards."

14. Proposed court-ready guidelines (Pakistan): a "Qarīna + Integrity" standard under Article 164

Based on QSO doctrine and the electronic evidence literature you attached, Pakistani courts could adopt the following practical guidelines (not as new law, but as structured judicial reasoning):

- Step 1: Admit for consideration, not for truth. Use Article 164 to allow production, and then decide probative value separately.
- Step 2: Require a provenance statement from the producing party (how obtained, when, from what source).
- Step 3: Prefer better forms of "primary" access where feasible (device, certified system export), and treat screenshots/printouts as weaker secondary evidence unless corroborated.
- Step 4: Treat authorship as a separate issue (telegraph rule): don't presume who created/sent merely because the message exists.
- Step 5: Encourage expert grounding when integrity is contested (Articles 59–65), and require disclosure of the "grounds" (methods, tools, limitations).

- Step 6: Use corroboration explicitly through the QSO relevancy provisions (Articles 19–24), building a converging set of qarāʾin.
- Step 7: Allocate burdens sensibly using Article 120 (facts needed for admissibility) and Article 122 (facts within special knowledge), especially where the resisting party controls relevant technical details.

Conclusion: reconciling Article 164 with Sharīʿa goals of justice

The QSO already contains the tools needed to handle electronic evidence ethically and coherently: an explicit modern-devices gateway (Article 164), broad relevancy doctrines supporting inference, structured documentary proof rules, rebuttable presumptions, expert opinion provisions, and burden-allocation rules for facts within special knowledge. Classical Islamic institutions and juristic debates—captured in Modarressi's account of maẓālim and of arguments for using circumstantial evidence—show that incorporating strong indicators is not a betrayal of Islamic legal values but can be necessary to prevent rights from being lost and to prevent sophisticated wrongdoing from hiding behind procedural formalisms.

At the same time, electronic evidence must be treated with the Shariah caution appropriate to any powerful but fallible indicator: it should function as qarīna whose weight rises and falls with proven integrity, corroboration, and fair adversarial testing, not as a shortcut that bypasses due process. If you want, I can now (1) format this into a proper academic paper structure (abstract, keywords, headings, footnote-style references), or (2) tailor it specifically to Pakistani litigation practice with a checklist for lawyers and judges.

References

1. Al-'Amrī, Ṣ. b. Muḥammad. (n.d.). *Iqāẓ himam ūlī al-abṣār li'l-iqtiḍā' bi-sayyid al-muhājirīn wa'l-anṣār*. Beirut: Dār al-Ma'rifah li'l-Ṭibā'ah wa'l-Nashr.
2. Al-'Atāsī, M. K. (1985). *Sharḥ Majallat al-aḥkām al-'adliyyah* (Vols. 1–5). Quetta: Maktabah Islāmiyyah.
3. Alfaize, N. A. (2015). *The impact of culture and religion on digital forensics: The study of the role of digital evidence in the legal process in Saudi Arabia* (Doctoral dissertation, De Montfort University, Leicester).
4. Al-Qurṭubī, A. 'U. Y. b. 'Abd Allāh. (1980). *Al-kāfī fī fiqh ahl al-Madīnah* (Vols. 1–2). Riyadh: Maktabat al-Riyadh al-Ḥadīthah.
5. Al-Rāzī, F. al-D. M. b. 'U. (1420 AH). *Mafātīḥ al-ghayb (al-tafsīr al-kabīr)* (Vols. 1–18). Beirut: Dār Iḥyā' al-Turāth al-'Arabī. Retrieved from www.altafsir.com
6. Al-Sarkhasī, S. al-D. M. b. A. (1998). *Al-mabsūṭ* (Vols. 1–30). Beirut: Dār al-Ma'rifah.

7. Al-Shāfi‘ī, A. Ḥ. Y. b. ‘A. al-K. al-‘Imrānī. (2000). *Al-bayān fī madhhab al-imām al-Shāfi‘ī* (Vols. 1–13). Jeddah: Dār al-Minhāj.
8. Al-Shīrāzī, A. Y. (n.d.). *Al-muhadhdhab fī fiqh al-imām al-Shāfi‘ī* (Vols. 1–3). Beirut: Dār al-Kitāb al-‘Ilmiyyah.
9. Al-Zuḥaylī, W. (1985). *Al-fiqh al-islāmī wa adillatuh* (Vols. 1–10). Damascus: Dār al-Fikr.
10. Badā’i‘ al-Ṣanā’i‘ fī tartīb al-sharā’i‘. (1998). Al-Kāsānī, ‘A. al-D. A. B. b. M. (2nd ed., Vols. 1–7). Beirut: Dār al-Kutub al-‘Ilmiyyah.
11. Davidson, A. (2009). *The law of electronic commerce*. New Delhi: Cambridge University Press.
12. Daniel, L., & Daniel, L. (2012). *Digital forensics for legal professionals: Understanding digital evidence from warrant to courtroom*. Waltham, MA: Elsevier.
13. Delaney, H., & Francis, B. (2015). Is your use of electronic signatures protecting your interests? *Governance Directions, 67*(8), 479–482.
14. Duranti, L., Rogers, C., & Sheppard, A. (2010). Electronic records and the law of evidence in Canada: The uniform electronic evidence act twelve years later. *Archivaria, 70*, 95–124.
15. Favro, P. J. (2007). A new frontier in electronic discovery: Preserving and obtaining metadata. *Boston University Journal of Science & Technology Law, 13*(1), 1–25. https://ssrn.com/abstract=2255160
16. Finkelstein, S. M., & Storch, E. R. (2010). Admissibility of electronically stored information: It’s still the same old story. *Journal of the American Academy of Matrimonial Lawyers, 23*, 45–72.
17. Fredesvinda, I. (2007). The admissibility of electronic evidence in court: Fighting against high-tech crime. *Journal of Digital Forensic Practice, 1*(4), 285–289. https://doi.org/10.1080/15567280701418049
18. Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital evidence and the U.S. criminal justice system*. Santa Monica, CA: RAND Corporation.
19. Haneef, S. S. S. (2006). Modern means of proof: Legal basis for its accommodation in Islamic law. *Arab Law Quarterly, 20*(4), 334–364.
20. Ingram, J. L. (2015). *Criminal evidence* (12th ed.). Waltham, MA: Anderson Publishing.
21. Ibn ‘Ābidīn, M. A. b. ‘U. (1992). *Radd al-muḥtār ‘alā al-durr al-mukhtār* (Vols. 1–6). Beirut: Dār al-Fikr.
22. Ibn Nujaīm, Z. al-D. b. I. (n.d.). *Al-baḥr al-rā’iq sharḥ Kanz al-daqā’iq* (Vols. 1–8). Beirut: Dār al-Kitāb al-Islāmī.
23. Ibn Qayyim al-Jawziyyah, M. b. A. B. (1953). *Al-ṭuruq al-ḥukmiyyah fī al-siyāsah al-shar‘iyyah*. Cairo: Dār al-Madanī.

24. Ibn Rushd, M. b. A. (2004). *Bidāyat al-mujtahid wa nihāyat al-muqtaṣid* (Vols. 1–4). Cairo: Dār al-Ḥadīth.
25. Ibn Taymiyyah, T. al-D. A. b. ‘A. (1995). *Majmū‘ al-fatāwā* (Vols. 1–35). Madinah: Majma‘ al-Malik Fahd.
26. Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Columbia Law Review, 105*, 279–318.
27. Keane, A., & McKeown, P. (2014). *The modern law of evidence*. Oxford: Oxford University Press.
28. Mālik b. Anas. (2004). *Al-Muwaṭṭa’* (Vols. 1–6). Abu Dhabi: Mu’assasat Zāyid b. Sulṭān.
29. Muslim b. al-Ḥajjāj. (n.d.). *Ṣaḥīḥ Muslim*. Beirut: Dār Iḥyā’ al-Turāth al-‘Arabī.
30. Seng, D. K. B. (1997). Computer output as evidence. *Singapore Journal of Legal Studies*, 159–166.