Alexander CA, et al., J Forensic Leg Investig Sci 2025, 11: 106
DOI: 10.24966/FLIS-733X/100106

HSOA Journal of Forensic, Legal & Investigative Sciences

Research Article

Computer Crime Evidence Collection

Cheryl Ann Alexander[1]* and Lidong Wang[2]

[1]*Institute for IT Innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA*

Abstract

Electronic evidence in cyber forensics can be any digital data that is useful to investigate cybercrimes, including logs, metadata, files, emails, and internet history. Computer crime evidence or digital evidence collection is important, and it has been utilized in investigating crimes. This paper deals with planning computer crime evidence collection. It includes crime evidence collection (approaches, actions, and steps), modeling methods for digital forensics, image forensics, forensic evidence collection using fingerprinting, data collection and rig derivation, digital forensic artifacts and artifact cataloging, anti-forensic types and techniques, cross-border electronic evidence, and cross-border criminal investigations. It is necessary for forensic methods and tools to keep up with new forms of digital evidence and cyberattacks.

Keywords: Digital forensics; Crime evidence; Forensic evidence; Image forensics; Fingerprinting; Anti-forensic types; Cross-border electronic evidence; Cross-border criminal investigations

Introduction

Digital forensics refers to using scientifically derived and proven approaches to preserving, collecting, validating, identifying, analyzing, interpreting, documenting, and presenting digital evidence derived from digital sources to facilitate or further the reconstruction of criminal events or help to anticipate unauthorized actions shown to be disruptive to planned operations [1]. The significance of video in the courtroom and its influence as evidence for the jury was discussed. Video evidence has been very compelling for a jury to convict a criminal. A smartphone (possibly containing Internet searches, video, images, and email) has been an important device to be analyzed forensically [2].

***Corresponding author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA. E-mail: cannalexander68@gmail.com

Citation: Alexander CA, Wang L (2025) Planning Computer Crime Evidence Collection. J Forensic Leg Investig Sci 11: 106.

Received: May 20, 2025; **Accepted:** June 02, 2025; **Published:** June 05, 2025

A hashing algorithm is utilized to validate the integrity of forensic evidence. SHA-1 and SHA-2 are widely used hash functions. SHA-1 and SHA-2 were combined along with the utilization of SALT (a cryptography concept) to compute collision-resistant hash values [3]. Guaranteeing data integrity and authenticity is crucial. It is necessary for forensic methods and tools to keep up with new forms of digital evidence and cyberattacks.

How a panel of expert practitioners viewed evidence acquisitions within the cloud environment was explored. Digital forensic investigators should expand digital forensic practice tools and expertise, and include a cloud computing environment. Cloud forensics is a relatively new area of digital forensic practices [4]. Cyber forensics skills are required for a cyber forensics investigator, including legal expertise, an appreciation for confidentiality, knowledge of computer science, computer programming, continuous learning, linguistic ability, and communication skills [5].

Crime Evidence Collection: Approaches, Actions, and Steps

Electronic evidence in cyber forensics can be any digital data that is useful to investigate cybercrimes, including logs, metadata, files, emails, and Internet history. Linked with computers, networks, mobile devices, and the cloud, this evidence plays a key role in detecting illegal activities. The primary processes involved in digital evidence collection are data collection, examination, analysis, and reporting. Two types of data are collected: persistent data (stored on a non-volatile storage device such as a local hard drive and CDs) and volatile data (such as memory and registers). One of the major challenges in digital evidence collection is that evidence may not be at the crime scene but distributed across data centers (on the cloud) in various locations. As for evidence acquisition, detailed information must be recorded and preserved. Suitable steps are taken to copy and transfer evidence to the investigator's system. At least steps to derive evidence from the cybercrime scene include capturing or recording data, storing the data, and making an exact copy of the CD or disk containing the data to protect the original from loss, damage, or destruction [6].

An investigating team that conducts digital forensic (DF) examinations requires two fundamental and linked components: 1) a digital evidence strategy (DES) with the outline of an effective investigative method, and 2) deploying it with suitable techniques and tools. When performing a DF examination, the investigative team needs to consider the relationship between the DES and its tools. A DES is an essential part of a DF examination. DF tools are an important part of the DF investigative process. A DES must include the definition of the conduct with a maximum coverage of all the available inquiry-related data [7].

Digital forensic tools and techniques have been used by law enforcement organizations to investigate crimes. The open-source DF tool is a cost-saving choice. DF tools assist DF analysts in identifying, collecting, preserving, and examining digital evidence. The tools can

be grouped into software forensics, computer forensics, memory forensics, and mobile device forensics. There are three phases involving the use of forensic tools: 1) preservation—focusing on creating an image from the digital media while preserving the chain of custody; 2) collection—extracting data or information from the digital media or created image; and 3) examination and analysis— an in-depth evaluation of the collected data, recovery of deleted or hidden data from the digital media, and data validation. Digital evidence needs to be authentic and represent an accurate and true representation of the original data. Reliability and integrity are critical in digital forensics [8].

Modeling Methods for Digital Forensics

Digital forensics (DF) uses computer science to investigate digital crime. Intention recognition can be utilized to detect a cybercriminal's intentions and even to predict the cybercriminal's further behaviors. It is important for modeling methods developed for DF to foster judicial confidence. A logic-based method utilizes a formal language such as logic to represent knowledge and reasoning. Deep learning offers robust pattern recognition capabilities. Table 1 [9] shows the advantages and disadvantages of modeling methods.

Methods	Advantages	Disadvantages
Logic-based methods	• Ability to learn new knowledge from examples • Good prediction capability • Ability to deduct & infer based on logical rules • Compact knowledge representation • Understandable & explainable by humans	• Manually introducing new rules • Limitation in handling uncertainty • Difficulty in integrating with other models • Rigid when rules are used • Not scalable, expensive in computation
Classical machine learning	• Learning from data • Handling data noises • Handling uncertainty as it leverages probability • Handling partial observability • Minimal human intervention	• Not explainable • Requirement for manually encoding features & parameters • Not scalable though better than a logic-based method
Deep Learning	• Extracting insights & learning from data • No requirement for feature engineering • Handling noises • Handling uncertainty • Handling partial observability • Handling multimodal & complicated data	• Possible overfitting • Not explainable • Catastrophic forgetting • Requirement for much data for training • Need for much computational power • Difficulty in learning new classes

Table 1: Advantages and disadvantages of modeling methods.

Image Forensics

Images are frequently utilized as authentication proof for cybercrimes in a court of law. Tampering means removing or adding significant characteristics from an image without leaving any apparent trace. An automatic image forensic tool was designed and developed to identify tampered images. The algorithm and control flow diagram of the image forensic tool is illustrated in Figure 1. Image forensics has been defined as the process of the identification, acquisition, analysis, and reporting of digital evidence associated with images that can be legally accepted by a court of law [10].

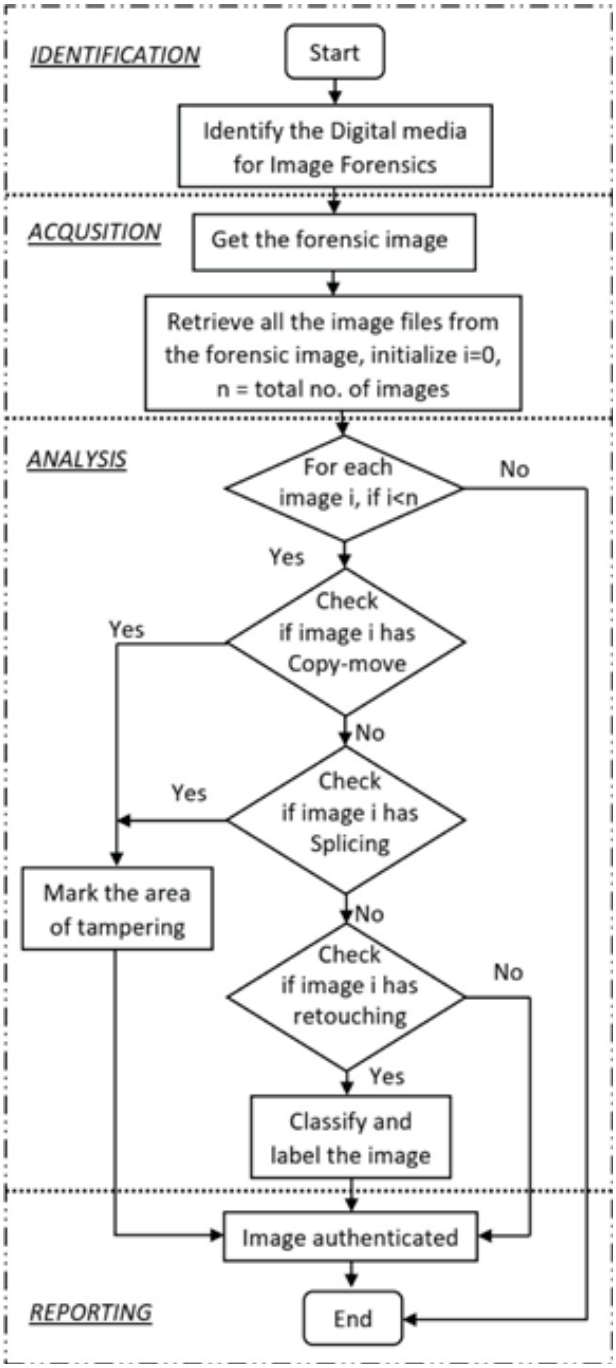

Figure 1: The algorithm and control flow diagram of a developed image forensic tool [10].

Forensic Evidence Collection Using Fingerprinting

Fingerprints have been utilized for forensic investigation. A secure protocol for collecting the device fingerprint was developed to help network forensic investigation and non-repudiation was achieved.

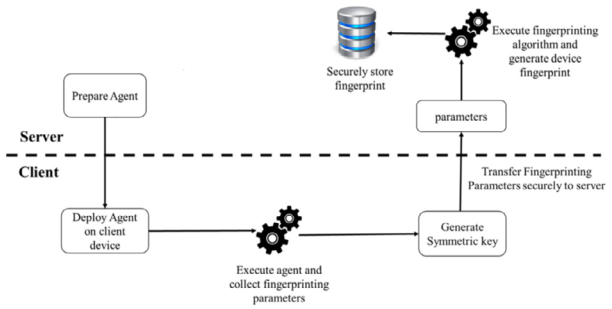

Figure 2: A proposed protocol framework for collecting forensic evidence using fingerprinting [11].

The fingerprinting technology utilizes a hash tree and generates legal evidence. The proposed protocol framework for collecting forensic evidence using fingerprinting is shown in Figure 2. After a client agrees, an agent executes on a client machine and gathers the needed fingerprinting parameters. The parameters are then transmitted to the server securely. The server performs the fingerprinting algorithm and generates the unique fingerprint. The fingerprint is finally stored on the server for a verification when a forensic investigation is needed [11].

Data Collection and Rig Derivation

There are limitations to traditional investigation methods and approaches, such as gait analysis and face recognition. A method based on anthropometric person-specific digital skeletons (so-called rigs) was presented, which was researched in the research project called COMBI. The method was used to present computer-aided opportunities for the recognition of perpetrators. Figure 3 shows the recording and assessment approaches in the COMBI, which includes the following steps: 1) study design and data collection, 2) generating a metric 3D reference model, 3) predicting person-specific rigs through OpenPose—an AI framework for predicting various joints of the human body, 4) generating person-specific 3D rigs, and 5) rig assignment in the metric 3D reference model. Data is captured at various stations in the first step. Rigs are derived from the captured data using AI and manual procedures. It is possible to compare and assign the rigs of known identities with the rigs of unknown identities after including 3D spatial information and integrating all the information into a metric 3D reference model [12].

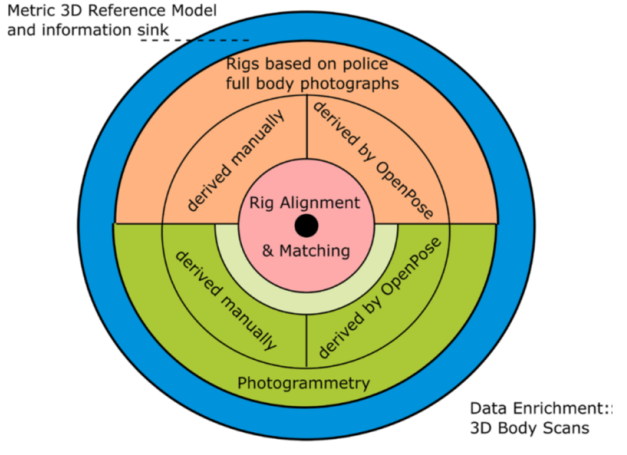

Figure 3: Representation of the data collection, rig derivation, and approaches utilized in the COMBI [12].

Digital Forensic Artifacts and Artifact Cataloging

Digital forensic practitioners often collect data in an ad hoc manner; therefore, results are frequently unverified, unstructured, and even incomplete. An approach to cataloging crowdsourced knowledge of digital forensic artifacts in an easily searchable and well-structured method was presented to help extract information efficiently and improve the reliability and availability of the artifact interpretation. An artifact catalog can provide a framework to organize and share knowledge about digital atomic artifacts. A practitioner can use the artifact catalog to look for artifacts. Figure 4 shows the structured composition of an entry in the artifact catalog [13].

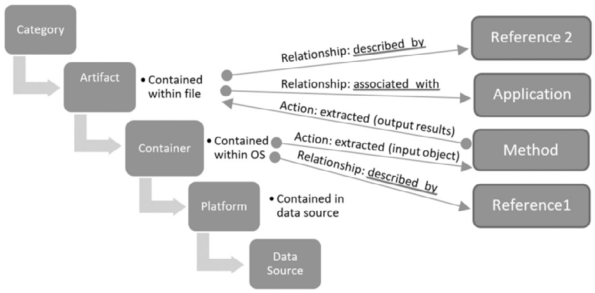

Figure 4: An artifact's structured composition within nested containers [13].

Anti-forensic types	Techniques	Description
Data hiding	Forging Timestamps	Modifying file timestamps (leading to the reconstruction of events on the misleading timeline)
	Hiding by Mounting	Hiding data within a directory by mounting a newly created (or existing) file system/directory onto it
Attacking forensic tools	Opening Sparse File	An empty file with a very big logical size finally overflows the disk capacity & makes a tool crash
Trail obfuscation	Opening Compression Bomb	Substantially compressed files expand to tremendously large sizes after decompression, resulting in forensic tool crash
	Modifying Magic Number	Changing magic numbers of the file system to stop forensic tools from identifying & analyzing the file system under investigation
Artefact wiping	Secure- Deletion	Overwriting deleted information with random data makes recovery impossible
	Hiding using Encryption	Hiding data in a cipher leads to CPU overhead, management costs, & legal bindings related to decryption
	Hiding in Slack Space	Hiding data in idle space
	Hiding in Reserved Locations	Hiding data in reserved spaces file system data structures without disturbing the file system's working
	Hiding using Steganography	Hiding data in a carrier file without corrupting its contents & disturbing its working
	Hiding in HPA/DCO	Hiding data in the host protected area (HPA)/device configure overlay (DCO)

Table 2: Anti-forensic types and techniques.

Anti-forensic Types and Techniques

Whether computer forensic tools (CFTs) can obtain complete and credible digital evidence from digital crime scenes with file system anti-forensic (AF) attacks has been investigated, indicating that evidence obtained by CFTs was not complete and even not credible when there were AF attacks such as data hiding, secure-deletion, forging timestamps, and modifying magic numbers. Practitioners should not completely count on CFTs for evidence collection from a digital crime scene where there are AF attacks. Table 2 [14] shows the types of AF attacks on file systems and specific techniques.

Cross-border Electronic Evidence and Cross-border Criminal Investigations

Legal remedies for removing barriers to gathering cross-border electronic evidence were proposed to fight against cybercrime and other crimes. An online survey (available for completion from April 11, 2017 to September 26, 2017) was conducted and survey participants were from public prosecutors, judges, investigation judges, ministries of justice, law enforcement, and other institutions in the European Union (EU). Almost all participants (97%) thought that they needed to upgrade their knowledge of digital investigation. Most of the participants (68%) felt that they needed training regarding the technical and legal issues associated with gathering cross-border e-evidence. The lack of knowledge and skills in digital forensic and cybercrime investigations and the requirements for further training to upgrade their expertise are shown in Figure 5 [15].

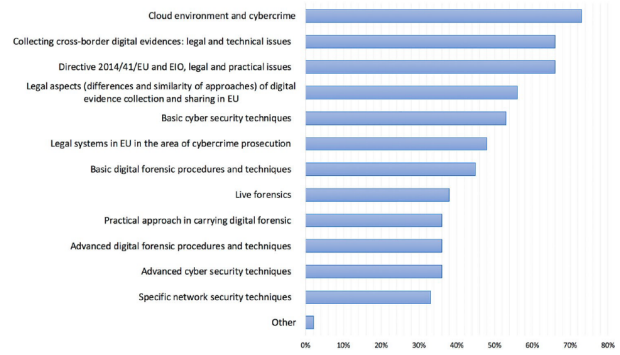

Figure 5: Themes on additional training among legal practitioners based on a survey [15].

Cross-border criminal investigations are very complicated owing to the heterogeneity of legal frameworks. The challenges were identified, and the efficacy of cooperation protocols was studied. A digital evidence management system (DEMS) helps digital forensic investigations. Several features of a DEMS have been identified. The relationship between the challenges of cross-border criminal investigations and the features of the DEMS is summarized in Table 3 [16].

Conclusion

Digital evidence collection has been utilized in investigating crimes. The evidence can be computer systems, storage devices (e.g., hard disks and USB flash drives), or electronic documents such as images, chat logs, and emails. Modeling methods (such as logic-based methods and deep learning) for digital forensics have their advantages and disadvantages. Hybrid methods are more powerful in many situations. Data integrity and authenticity are crucial for crime evidence collection.

Challenges	Evidence collection	Reporting tools	Chain of custody assurance	Use of standards	Regulation compliance
Data location & individuals' control over their own data					X
Timely collection & sharing of evidence	X				
Lack of harmonization in admissibility rules of criminal evidence & prosecution		X	X	X	
Lack of compatibility between protocols regarding data definition & categorization				X	
Direct cooperation with service providers & opportunity equality					X
Incompatibility conflicts between jurisdictions (maybe violating procedural laws & rights)				X	X
Lack of automatic mechanisms for efficient collecting & reporting requests	X		X		
Auditability of data collection procedures		X		X	X
Lack of resources (equipment & law enforcement training) & judicial authorities (aiding direct cooperation between jurisdictions)				X	X
Data retention issues	X		X		X

Table 3: Relationship between the challenges of cross-border criminal investigations and the features of the DEMS.

Evidence obtained by CFTs was not complete and even not credible when there were AF attacks. Practitioners should not completely count on CFTs for evidence collection from a digital crime scene where there are AF attacks. Cross-border criminal investigations are very complicated owing to the heterogeneity of legal frameworks. A digital evidence management system (DEMS) helps digital forensic investigations. It is necessary for forensic methods and tools to keep up with new forms of digital evidence and cyber-attacks.

Acknowledgement

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Declaration of the Use of AI Tools

The authors declare that they did not use AI tools in writing this paper.

Conflict of Interest

The authors would like to announce that there is no conflict of interest.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

1. Pilski M (2022) Methods to acquisition digital evidence for computer forensics. Stud Inform Syst Inf Technol 26: 73-84.
2. Onwuachi-Willig A (2021) The trauma of awakening to racism: did the tragic killing of George Floyd result in cultural trauma for whites? Houst Law Rev 58: 817.
3. Pradeep KC, Soman R, Honnavalli P (2020) Validity of forensic evidence using hash function. In: 2020 5th International Conference on Communication and Electronics Systems (ICCES), IEEE, 823-826.
4. Barrett D (2020) Cloud based evidence acquisitions in digital forensic education. Inf Syst Educ J 18: 46-56.
5. Hayes D (2020) A practical guide to digital forensics investigations (2nd ed.).
6. Khashashneh T, Al-Billeh T, Al-Hammouri A, Belghit R (2023) The importance of digital technology in extracting electronic evidence: how can digital technology be used at crime scenes? Pak J Criminol 15.
7. Horsman G (2024) The importance of digital evidence strategies. Wiley Interdiscip Rev Forensic Sci 6: e1507.
8. Ismail I, Ariffin KAZ (2024) Open source tools for digital forensic investigation: capability, reliability, transparency and legal requirements. KSII Trans Internet Inf Syst (TIIS) 18: 2692-2716.
9. Kassa YW, James JI, Belay EG (2024) Cybercrime intention recognition: a systematic literature review. Information 15: 263.
10. Pawar D, Gajpal M (2021) Image forensic tool (IFT): image retrieval, tampering detection, and classification. Int J Digit Crime Forensics (IJDCF) 13: 1-15.
11. Patil RY, Devane SR (2022) Network forensic investigation protocol to identify true origin of cyber crime. J King Saud Univ Comput Inf Sci 34: 2031-2044.
12. Becker S, Heuschkel M, Richter S, Labudde D (2022) COMBI: artificial intelligence for computer-based forensic analysis of persons. KI-Künstl Intell 36: 171-180.
13. Casey E, Nguyen L, Mates J, Lalliss S (2022) Crowdsourcing forensics: creating a curated catalog of digital forensic artifacts. J Forensic Sci 67: 1846-1857.
14. Bhat WA, AlZahrani A, Wani MA (2021) Can computer forensic tools be trusted in digital investigations? Sci Justice 61: 198-203.
15. Jerman Blažič B, Klobučar T (2020) Investigating crime in an interconnected society: will the new and updated EU judicial environment remove the barriers to justice? Int Rev Law Comput Technol 34: 87-107.
16. 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.

HERALD

Advances In Industrial Biotechnology | ISSN: 2639-5665

Advances In Microbiology Research | ISSN: 2689-694X

Archives Of Surgery And Surgical Education | ISSN: 2689-3126

Archives Of Urology

Archives Of Zoological Studies | ISSN: 2640-7779

Current Trends Medical And Biological Engineering

International Journal Of Case Reports And Therapeutic Studies | ISSN: 2689-310X

Journal Of Addiction & Addictive Disorders | ISSN: 2578-7276

Journal Of Agronomy & Agricultural Science | ISSN: 2689-8292

Journal Of AIDS Clinical Research & STDs | ISSN: 2572-7370

Journal Of Alcoholism Drug Abuse & Substance Dependence | ISSN: 2572-9594

Journal Of Allergy Disorders & Therapy | ISSN: 2470-749X

Journal Of Alternative Complementary & Integrative Medicine | ISSN: 2470-7562

Journal Of Alzheimers & Neurodegenerative Diseases | ISSN: 2572-9608

Journal Of Anesthesia & Clinical Care | ISSN: 2378-8879

Journal Of Angiology & Vascular Surgery | ISSN: 2572-7397

Journal Of Animal Research & Veterinary Science | ISSN: 2639-3751

Journal Of Aquaculture & Fisheries | ISSN: 2576-5523

Journal Of Atmospheric & Earth Sciences | ISSN: 2689-8780

Journal Of Biotech Research & Biochemistry

Journal Of Brain & Neuroscience Research

Journal Of Cancer Biology & Treatment | ISSN: 2470-7546

Journal Of Cardiology Study & Research | ISSN: 2640-768X

Journal Of Cell Biology & Cell Metabolism | ISSN: 2381-1943

Journal Of Clinical Dermatology & Therapy | ISSN: 2378-8771

Journal Of Clinical Immunology & Immunotherapy | ISSN: 2378-8844

Journal Of Clinical Studies & Medical Case Reports | ISSN: 2378-8801

Journal Of Community Medicine & Public Health Care | ISSN: 2381-1978

Journal Of Cytology & Tissue Biology | ISSN: 2378-9107

Journal Of Dairy Research & Technology | ISSN: 2688-9315

Journal Of Dentistry Oral Health & Cosmesis | ISSN: 2473-6783

Journal Of Diabetes & Metabolic Disorders | ISSN: 2381-201X

Journal Of Emergency Medicine Trauma & Surgical Care | ISSN: 2378-8798

Journal Of Environmental Science Current Research | ISSN: 2643-5020

Journal Of Food Science & Nutrition | ISSN: 2470-1076

Journal Of Forensic Legal & Investigative Sciences | ISSN: 2473-733X

Journal Of Gastroenterology & Hepatology Research | ISSN: 2574-2566

Journal Of Genetics & Genomic Sciences | ISSN: 2574-2485

Journal Of Gerontology & Geriatric Medicine | ISSN: 2381-8662

Journal Of Hematology Blood Transfusion & Disorders | ISSN: 2572-2999

Journal Of Hospice & Palliative Medical Care

Journal Of Human Endocrinology | ISSN: 2572-9640

Journal Of Infectious & Non Infectious Diseases | ISSN: 2381-8654

Journal Of Internal Medicine & Primary Healthcare | ISSN: 2574-2493

Journal Of Light & Laser Current Trends

Journal Of Medicine Study & Research | ISSN: 2639-5657

Journal Of Modern Chemical Sciences

Journal Of Nanotechnology Nanomedicine & Nanobiotechnology | ISSN: 2381-2044

Journal Of Neonatology & Clinical Pediatrics | ISSN: 2378-878X

Journal Of Nephrology & Renal Therapy | ISSN: 2473-7313

Journal Of Non Invasive Vascular Investigation | ISSN: 2572-7400

Journal Of Nuclear Medicine Radiology & Radiation Therapy | ISSN: 2572-7419

Journal Of Obesity & Weight Loss | ISSN: 2473-7372

Journal Of Ophthalmology & Clinical Research | ISSN: 2378-8887

Journal Of Orthopedic Research & Physiotherapy | ISSN: 2381-2052

Journal Of Otolaryngology Head & Neck Surgery | ISSN: 2573-010X

Journal Of Pathology Clinical & Medical Research

Journal Of Pharmacology Pharmaceutics & Pharmacovigilance | ISSN: 2639-5649

Journal Of Physical Medicine Rehabilitation & Disabilities | ISSN: 2381-8670

Journal Of Plant Science Current Research | ISSN: 2639-3743

Journal Of Practical & Professional Nursing | ISSN: 2639-5681

Journal Of Protein Research & Bioinformatics

Journal Of Psychiatry Depression & Anxiety | ISSN: 2573-0150

Journal Of Pulmonary Medicine & Respiratory Research | ISSN: 2573-0177

Journal Of Reproductive Medicine Gynaecology & Obstetrics | ISSN: 2574-2574

Journal Of Stem Cells Research Development & Therapy | ISSN: 2381-2060

Journal Of Surgery Current Trends & Innovations | ISSN: 2578-7284

Journal Of Toxicology Current Research | ISSN: 2639-3735

Journal Of Translational Science And Research

Journal Of Vaccines Research & Vaccination | ISSN: 2573-0193

Journal Of Virology & Antivirals

Sports Medicine And Injury Care Journal | ISSN: 2689-8829

Trends In Anatomy & Physiology | ISSN: 2640-7752