APPLICATION OF DIGITAL FORENSICS IN DIGITAL LIBRARIES

Dr B. R. Doraswamy Naick
Assistant Professor in LIS
JNT University Kakinada-Andhra Pradesh, India

Neelima Bachalla
M.Sc. Forensic Science
Bundelkhand University, Uttar Pradesh, India

ABSTRACT

The University Libraries have the potential to encourage digital libraries in e-learning, the imperativeness of training and knowledge for effective functionality of Digital Libraries in Academic Institutions. The digital content includes unique and irresponsible intellectual, cultural and scientific materials without action these e-materials are at greatest risk of loss which should be secured from misuse and theft. Digital Forensics prevents and identifies the problems in Digital Libraries like access to e-resources through a variety of Legal principles, license agreements, exceptions under national Copyright law. This paper briefly discusses to explore the librarians towards the identification of Digital Publications and websites especially misuse and copy of e-resources (e-material like e-papers, e-magazines, e-books, etc) using Digital Forensic applications in Digital Libraries.

Key words: Academic Institutions, digital libraries, Digital Forensics, Copyright law.


http://www.iaeme.com/IJLIS/issues.asp?JType=IJLIS&VType=5&IType=2

INTRODUCTION

A Digital Library is the computer network technology, database technology and multimedia technology. Digital Libraries are principally comprises of magnetic and optical disks and tapes containing digital files. Universities Library are acquiring an increasing amount of digital material/ handheld media. Digital collections are at multiple levels of representation like description, interpretation and use. There is a substantial body of information within the data structures of computer systems that can often be discovered or recovered. Along with new opportunities, institutions also face a variety of technical difficulties as they process digital data, including: file system discrepancies between storage environments, media format obsolescence, operating system incompatibilities, and hardware risks. Digital or even electronic media, copyright holders, content producers, or other financially or artistically interested parties had business and
legal objections to copying technologies. The advent of personal computers has made it convenient for users to convert media (which may or may not be copyrighted) originally in a physical/analog form or a broadcast form into a universal, digital form (ripping). This combined with the internet and popular file sharing tools, has made unauthorized distribution of copies of copyrighted digital media (digital piracy) are identified by Digital Forensics. As per law for user rights and access to information, websites emerging challenges posed at the intersection of technology, society, and law for fair use.

SECURITY AND IDENTIFICATION
Digital library Security is constantly evolving and is a complex technical area. Security is the protection of Computing systems and the data that they store or access. Digital Library includes Computer Security with Software Security, Network Security, Internet Security, Access Control and OPAC (Online Public Access Catalog). The acquisition of digital materials by students, Lecturers, Professors, and libraries has resulted in the need to incorporate new tools and methods into curatorial practices. The e-materials are increasingly used to move born-digital materials from removable media into more sustainable preservation environments.

Basic needs of the library are
- Infrastructure and CCTV cameras.
- Use of Biometrics.
- Use of RFID for management of Books, RFID tags replace of both the EM security strips and Barcode.
- Awareness to the students by conducting seminars for newly joined students in all courses in the University.
- Some students or University staff willingly do the duplication or deleting or editing of e-material.

Backup Procedures
- Backup to CD-RW, DVD-RAM, or external hard drives.
- Full backup – copies all files.
- Differential backup – copies all files that have changed since the last full backup.
- Incremental backup – copies all files that have changed since either the last full backup or the last incremental backup.
- Restoration – is the process of retrieving data from a backup.
- Need Backup Software that provides these options.

Controlling Access
- Physical - Cables, locks, Badge, key, or card to give you physical access to the computer room or a locked terminal.
- Known - Password, pin code, mother’s maiden name, Signature, job role
- Biometrics - Application of technology to authenticate a person’s identity by verifying a personal characteristic.
- Identification of e-material and deletion of any material in Digital Libraries with the help of Digital Forensics.
- Clear, user-friendly documentation
- Modular, cross-platform software tools
- Software and guidance for collecting born-digital materials remotely at a donor's facility or residence.
- An easily navigable graphical user interface, an application programming interface (API) for integration with existing software platforms, and command line tools that support batch processing.
The elements are designed to build capacity and ensure the sustainability of digital acquisition education activities. Knowledge of faculty and personnel security software's will be distributed under an open source license. The tools are distributed and integrated into working collections and repositories.

DIGITAL FORENSICS
Digital/ Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.

Two fundamental needs and opportunities for Universities and Institutions:

1. (1) Integrating digital forensics tools and methods into the workflows and collection management environments of Libraries and (2) Supporting properly mediated public access to forensically acquired data.

Digital Forensic analysis is an important aspect identification and investigation of many different kinds of crime like copyright of e-material, duplicating, theft in the central library. E-library system characteristics, organizational context and individual characteristics are identifies based on Digital Forensics.

Data triage functions to automate repetitive or technically challenging tasks during both appraisal and reprocessing after ingest (e.g., high-quality file type identification, flagging and redaction of private and sensitive data, and general reports on drive contents).


Hardware: A) Acquisition System – Can be older PC or laptop that has been “put out to pasture”. B) Administrative system – Case files, logs, reports, evidence inventory. C) Analysis system – High end system capable of processing a lot of data quickly. D) Hard drives, CD & DVD, Duplicators, Write blockers. E) Cables, connectors, etc.


Digital Forensics includes:

- Evidence might be required for a wide range of computer crimes and misuse of e-resources.
- Multiple methods of
- Discovering data on computer system
- Recovering deleted, encrypted, or damaged file information
- Monitoring live activity
- Detecting violations of corporate policy.
- Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity.
- Restore files and/or e-mail messages that have been deleted.
- Examine data and log files on computers and network servers.
- Specialist must have extensive knowledge of hardware, software, networks and law.

Digital Forensic Analysis involves determining significance, reconstructing data fragments of data and drawing some conclusions based on the evidence collected. May require the use of tools, and test may also be done more than once to support the crime theory. Technical knowledge required to do undertake an effective analysis process.
RESULTS
Digital Libraries are securing E-resources from misusing and whenever fraud done by the individuals identified by the Digital Forensic Applications. In the University Library from all the departments including students, staff of different departments and Library Staff were 100%. Percentage of individuals were identified who were misusing the e-resources from Digital Library, Percentage of theft (E-books) and Students who were not aware to they are misusing the e-resources in Digital library. Total individuals who are using Digital libraries were 100% and Identified percentage was mentioned in Table No. 1.

Table 1 Identification of Fraud/ Misuse of E-resources in Digital Library:

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Year and Percentage</th>
<th>Type of Identification by using Digital Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2013</td>
<td>2014</td>
</tr>
<tr>
<td>1.</td>
<td>16%</td>
<td>10%</td>
</tr>
<tr>
<td>2.</td>
<td>10%</td>
<td>7%</td>
</tr>
<tr>
<td>3.</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>33%</td>
<td>22%</td>
</tr>
</tbody>
</table>

ADVANTAGES
Digital Libraries can enhance legibility and easy access. Security in Digital library allows the University to carry out its mission by: Enabling people to carry out their education, and research. Supporting critical Digital library process. Protecting sensitive information in Digital Libraries. Digital e-resources are Secure by Secure Data Exchange (Identification, Authentication, Verification, and Non-Repudiation). Duplicators are identified with the help of Biometrics and misuse of computer data to determine potential legal evidence by using Forensic tools. Digital Forensic Analysis involves identification, Search and seizure, Preservation, Examination/Analysis, extraction, Documentation and interpretation of computer data to determine potential legal evidence and Reporting to report evidence in the court and accused will be punished. To secure the digital e-resources and following steps will prevent crime regarding e-materials: Data Backup (Encrypt, Secure transfer of backup media, Periodic recovery) Security Issues like Data hiding, Image hiding, Improper destruction of sensitive data, Weak authentication tools (Created, Accessed, Modified date), Boot password, Password cracking. Privacy Issues Computer Forensic investigation reveals like Passwords, Encryption keys, Images.
CONCLUSION
Digital Libraries require safeguarding and awareness towards security systems by using various technologies. The most important role of Digital library is to maintain the quality and security of E-resources (e-material like e-papers, e-magazines, e-books etc). Digital Libraries have to consider Security Systems – Forensic applications to protect from loss, theft, Duplication and fraud by staff. Digital Forensic applications in Digital libraries provide benefits that may improve our lives in such a way by increasing security, efficiency and flexibility. Digital Forensics plays a key role in providing information like Identification, Authentication, Verification and Privacy. Misuse and Fraud are identified by Digital Forensic Analysis; to develop and improve their functions and services in Digital Library. this paper presents Digital e-resource security Identification by digital Forensic Analysis which improves e-resources usage in Digital Libraries and Universities.

REFERENCES

AUTHORS DETAILS

Dr. B. R. Doraswamy Naick

is currently working as Assistant Professor (Selection Grade) in Head of the Central Library in JNTUK Kakinada. He completed his M.Phil on -2004.He did his Ph.D on Sri Venkateswara University Tirupati 2012.He has more than 12 years of professional experience in Library & Information science. He was joined in 2006 in the JNTU services as an Assistant professor in library and information science. Previously He worked as Asst Librarian in more than 3 years in Sri Venkateswara University Library, Tirupati. He has been presented and participated in more than 40 National and International conferences workshops and Seminars. And also 30 and above papers Published in Different Conference Proceedings.6 Papers Published in National journals and 7 papers published in International Journals. He was introduced Library Automation, and Established Digital Library, NPTEL Videos and E-Resources in Central Library at JNTUK Kakinada. He is elected as a Teaching Association Executive member of social sciences & Humanities Departments in JNTUK in The year 2010-12. He win as a Joint Secretary JNTUK Teaching Association 2014-16. Again he elected as a Teaching Association Executive member of social sciences & Humanities Departments in JNTUK in The year 2016-18. He also introduced the Ph.D in Library and Information Science in JNTUK. first time. in the year 2013. About 6 Research Scholars doing Research under his guidance. and acting as Internal Guide of other 5 Research scholars. He is a member of Different National and International Bodies. and his Areas of Interest are user’s studies, information seeking behaviour, ICT applications in Academic Libraries, Networking of Libraries and IPR Issues. Now he is taking a whole Responsibility to Develop a University Library as world class Library.

Ms. Neelima Bachalla

M.Sc. (Forensic Science), PGDCA. She has qualified UGC NET. She worked for One year as a Trainee in Andhra Pradesh Forensic Science Laboratory (APFSL), Hyderabad. She has participated and presented National and International conferences, workshops and Seminars and also presented many Papers.