Volume 1, Issue 5 December 2015 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi, Urdu all research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

WORKING OF P2P PROTOCOL FOR FORENSIC INVESTIGATION FRAMEWORK

PROF. YUVRAJ NIKAM, MANISHA PRAJAPATI, NARESH BATTULWAR, SWAPNIL SONAWANE & RAHUL AVHAD
Department Computer, Engineering, Savitribai Phule, Pune University, Pune, India

ABSTRACT:
Associate to Peer(P2P) document sharing systems are amongst the best free wellsprings of data on the web. Intentional cooperation and absence of control makes them an exceptionally alluring choice to share information secretly. Be that as it may, a little gathering of individuals exploit the flexibility gave by these systems and offer substance that is restricted by law. Aside from copyrighted substance, there are situations where individuals offer documents identified with Child Pornography which is a criminal offense. Law implementation endeavors to find these o enders by getting a court request for inquiry and seizure of PCs at a suspect area. These seized PCs are forensically inspected utilizing capacity and memory-crime scene investigation instruments. On the other hand, before the court order is issued solid confirmation must be displayed to give motivation to suspicion. Conventional examination in the starting stages may prompt misidentification of the source and guide the examination in a wrong course. Introductory proof accumulation on distributed document sharing systems is a test because of the absence of an essential issue of control and exceptionally dynamic nature of the systems. The objective of this work is to make a working model of an introductory proof accumulation device for criminology in P2P systems. The model depends on the thought that P2P systems could be observed by presenting altered associate hubs onto the system for a sure time period and recording applicable data about hubs that have criminally hostile substance. Logging data sent by a suspicious hub alongside timestamps and one of a kind distinguishing proof data would give an in number, evident starting confirmation. This work presents one such working model in arrangement with the objectives expressed previously.

Keywords: ***Network Forensics, Packet Reordering, P2P Traffic Analysis, Torrent File, P2P network PCAP File***

1. INTRODUCTION

Framework wrongdoing scene examination is a branch of examination of perceiving framework irregularities and breaks from the case of framework bundles. To grasp framework, utilize, a substance level examination of individual development stream must be driven. The behavior and interest sample of any intruder from the information set away in the frameworks as bundles. This activity is entitled as audit framework examination or framework criminology. We can get to lawful data from bundle level examination as a logged off method. The proposed framework lawful examination structure accumulates forensically rich information from the data assembled as packs. In every way that really matters it is to a great degree difficult to separate packs online as it needs unprecedented fast package getting figuring and auxiliary building nearby support of complex sturdy merchandise. The proposed framework wrongdoing scene examination structure for P2P examination accumulates

forensically rich information by realizing disengaged from the net bundle reordering and multiplication count which is interestingly expected to handle seeders, criminals and trackers in a P2P area. Most of the researchers in this field defy the issue of seeing best parts from which most compelling legitimate dada can be assembled. The group examination frameworks, for instance, Wire shark, TCP dump et cetera give some sort of legitimate information to supervisor or master, yet these structures can't make the genuine substance from the packages.

1. LITERATURE SURVEY

2.1 An Improved Approach towards Network Forensic Investigation of HTTP and FTP Protocols

- Manesh T, B Brijith, Mahendra Prathap Singh

System bundle examination and remaking of system sessions are more modern procedures in any system measurable and investigation framework. Here we present an incorporated system which can be utilized for reviewing, reordering also, reproducing the substance of parcels in a system session as a component of legal examination. System investigators ought to have the capacity to watch the put away bundle data when a suspicious movement is accounted for and ought to gather sufficient recreating so as to support confirmations from put away bundle data the unique information/documents/messages sent/got by every client. Consequently, suspicious client exercises can be found by checking the parcels in disconnected from the net. So we require a productive system for reordering bundles and recreating the records or archives to execute criminological examination and to make important confirmation against any system wrongdoing. The proposed system can be utilized for substance level investigation of bundles going through the system in light of HTTP and FTP conventions and reports beguiling system exercises in the undertaking for measurable examination.

2.2 Analyzing Peer-To-Peer Traffic Across Large Networks

-Subhabrata Sen, and Jia Wang, (2009)

The utilization of distributed (P2P) applications is becoming significantly, especially to share vast feature/sound documents and programming. In this paper, we dissect P2P activity by measuring flow level data gathered at numerous outskirt switches over an expansive ISP system, and report our examination of three well known P2P frameworks Fast Track, Gnutella, and Direct-Connect. We describe the P2P traffic saw at a solitary ISP and its effect on the basic system. We watch extremely skewed dissemination in the movement over the system at diverse levels of spatial accumulation (IP, prefix, AS). Each of the three P2P frameworks display critical motion at brief time scale and especially at the IP location level. Still, the portion of P2P movement contributed by every prefix is more steady than the relating circulation of either Web activity or general movement. The high volume and great dependability properties of P2P activity recommends that the P2P workload is a decent contender for being overseen through application-particular layer-3 movement building in an ISP's system.

2.3 Attack Pattern Discovery in Forensic Investigation of Network Attacks

-Ying Zhu (2011)

System assaults on frameworks executed by remote programmers once in a while happen in confinement; when a fruitful or just distinguished assault happens, it is frequently attractive to recreate the setting of this security rupture: every one of the occasions that pave the way to and are identified with the break. We mine the logs of late system traffic information to and these connections of assaults we call them

assault designs. We propose an iterative calculation for finding assault designs; the logs are examined to distinguish rational gatherings of occasions (called air pockets) that are prone to constitute assaults, and through a criticism system, the degrees of conviction that the air pockets are assault cases are engendered to the following cycle so as to renew the quest for air pockets identified with the ones officially found. Our reproductions confirm that the calculation accomplishes precision in finding assault designs. Our assault design revelation has the extra point of interest of being an unsupervised calculation,

e.g., it doesn't oblige from the earlier client denied.

2. EXISTING SYSTEM

Dataset: An information set (or dataset) is an accumulation of information. Most normally an information set relates to the substance of a solitary database table, or a solitary measurable information grid, where each section of the table speaks to a specific variable, and every column compares to a given individual from the information set being referred to. The information set records values for each of the variables, for example, stature and weight of an article, for every individual from the information set. Every quality is known as a datum. The information set may involve information for one or more individuals, comparing to the quantity of columns. The term information set may likewise be utilized all the more freely, to allude to the information in a gathering of firmly related tables, comparing to a specific examination then again occasion. An illustration of this sort is the information sets gathered by space offices performing tests with instruments on board space tests. - Existing framework inconveniences: Large-Scale Hierarchical grouping assignments regularly have a huge number of classes on which the most broadly utilized way to deal with multiclass order one-versus-rest gets to be immovable because of computational complex Inconveniences: Existing routines regularly create an immense arrangement of PHUIs and their mining execution is debased hence. The enormous number of PHUIs structures a testing issue to the mining execution since the more PHUIs the creates, the higher preparing time it devours.

3. PROPOSED SYSTEM

Framework wrongdoing scene examination is a branch of examination of perceiving framework irregularities and breaks from the illustration of framework parcels. To grasp framework, utilize, a substance level examination of individual development stream must be driven. The behavior and interest illustration of any gatecrasher from the information set away in the frameworks as packages. This activity is entitled as audit framework examination or framework criminology. We can get to lawful data from bundle level examination as a logged off method. The proposed framework lawful examination structure accumulates forensically rich information from the data accumulated as groups. In every practical sense it is to a great degree difficult to separate packs online as it needs extraordinary fast bundle getting estimation and basic designing close by sponsorship of complex tough products. The proposed framework wrongdoing scene examination structure for P2P examination assembles forensically rich information by completing separated from the net package reordering and generation estimation which is remarkably expected to handle seeders, criminals and trackers in a P2P area. Most of the researchers in this field stand up to the issue of seeing best parts from which most amazing legitimate dada can be assembled. The group examination frameworks, for instance, Wire shark, TCP dump et cetera give some sort of lawful information to supervisor or pro, yet these structures can't make the genuine substance from the bundles.

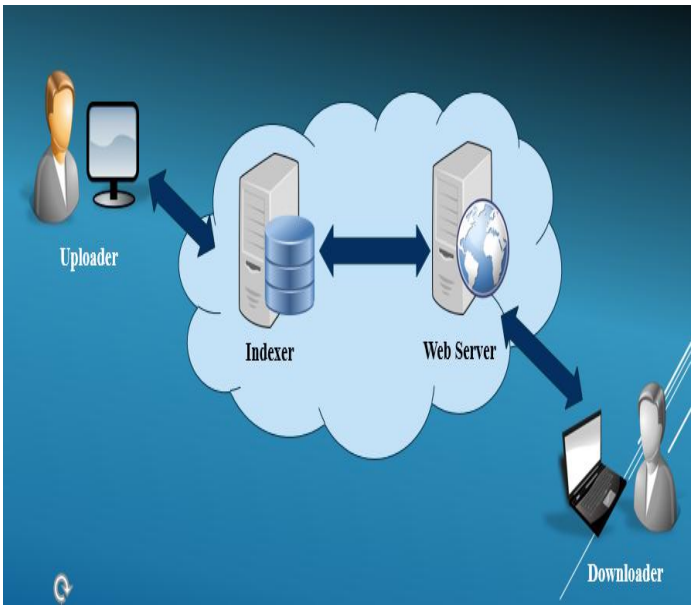
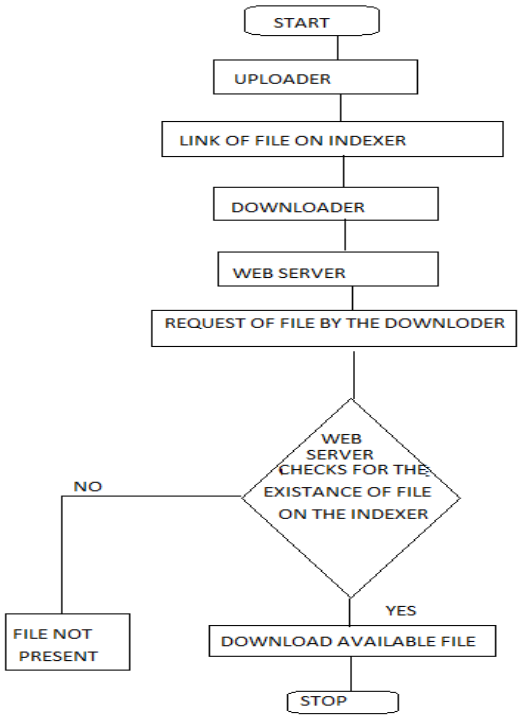


Fig.1 Architecture of P2P Protocol

4. FLOW CHART:



6. FLOW DIAGRAM:

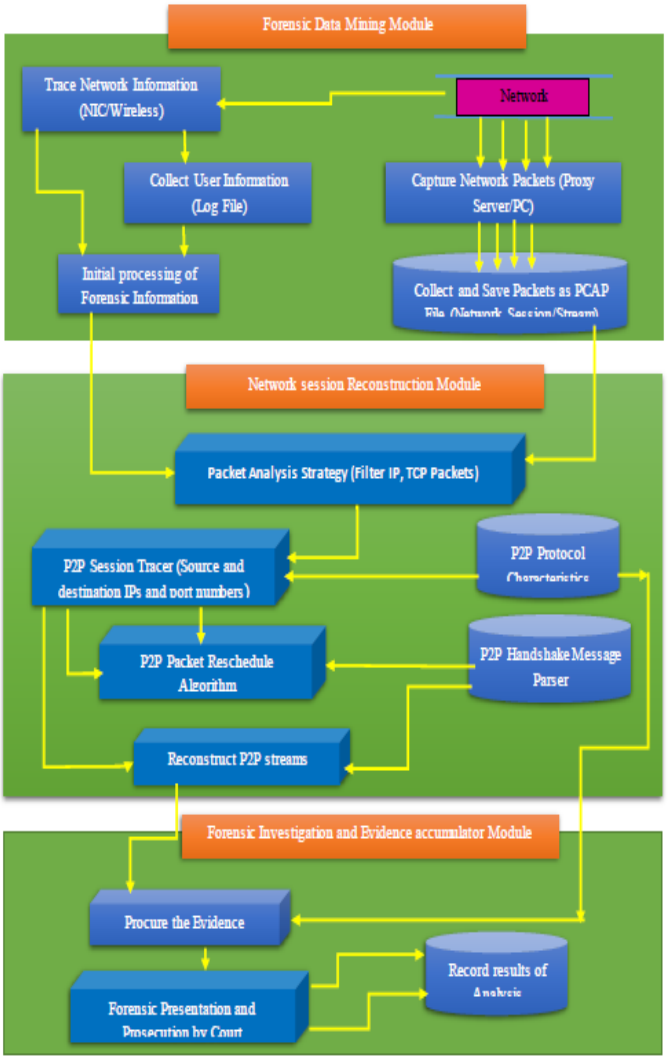


Fig.2 Flow Diagram of P2P Protocol

7. CONCLUSION:

Bit Torrent is the Popular P2P technology deployed across the internet. The protocol has found a niche as a preferred method for the decentralization distribution of large file. It provides data integrity which insures that the data will always be guanine and free from flaws.

Bit Torrent uses Tit for Tat exchange to increase cooperation among peers.

8. REFERENCES:

[1] Subhabrata Sen, and Jia Wang, (2009) "Analyzing Peer-To-Peer Traffic across Large Networks." IEEE/ACM Transactions on Networking, vol 12, pages 219-232, April 2009.

{2] ZHOU Xu, TANG Hui, (2009) DDP: "A Novel P2P Traffic Management and Optimization Protocol. IEEE Proceedings of International Conference on Information" Management, Innovation Management and Industrial Engineering, vol 3, pages 329-332, May 2009.

[3] A Ali, A Tuncay (2010) "Comparison of Bit Torrent traffic characterizations over IPv4 and IPv6." IEEE Proceeding of International Multi Conference on Global Information Technology, 2010.

[4] Y.Q. Wang, M. Qi (2011), "Computer Forensics in Communication Networks," IEEE International Communication Conference on Wireless Mobile and Computing Nov. 2011.

[5] M. Ali (2012), "Digital Forensics Best Practices and Managerial Implications", IEEE Fourth International Conference on Computational Intelligence, Communication Systems and Networks, pp- 196 199, Jul 2012.

[6] Marc Liberatore, Robert Erdely, and Thomas Kerle (2010) "Forensic Investigation of peer-to peer files sharing networks. Proceedings of the DFRWS Annual Digital" Forensics Research Conference, vol 7, pages S96-S103, Dec 2010.

[7] Natarajan Meghanathan, Sumanth Reddy Allam (2009). "Frameworks and Techniques For Network Forensics. International Journal of Network Security & Its Applications." (IJNSA), Vol .1, pages 14-25, April 2009.

[8] Tatsuro Fujii, Yizhi Ren (2010) "Security Analysis for P2P Routing Protocols." Proceedings of the International Conference on Availability, Reliability and Security,vol 9, pages 899-904, Dec 2010.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301 Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com