



RESEARCH ARTICLE

Network Monitoring and Forensics

¹Subhay Chandra, ²Rakesh Kumar Yadav

¹School of Engineering & Technology, IFTM University, Moradabad, U.P, India

²Department of Computer Science & Engineering, IFTM University, Moradabad, U.P, India

subhaychandra@gmail.com

Abstract— In the study of network forensics Mostly tools give you view of movement in real time, But monitoring in real- time at any stage requires hardware resources and human significant, and doesn't ratio to workgroups larger than a single network. It is normally more practical to archive all intercommunication service and analyse subsets as necessary. This process is called as network forensics, or reconstructive traffic analysis. Practically, it is frequently limited to data digest and packet-level inspection supervision; in spite of, a network monitoring forensics tool can endow a richer look of the data gathered, permission you to inspect the intercommunication service from further up the protocol stack? The forensic network is very simple to monitor and identify problem conveniently. It is very useful to rummage security infringement. It is completely analysing the record of network traffic.

Full Text: <http://www.ijcsmc.com/docs/papers/August2013/V2I8201346.pdf>