

Guide to access IEEE Computer Society Digital Library



1. Basic Search

The screenshot shows the IEEE Computer Society Digital Library homepage. At the top, there is a navigation bar with links for Jobs, Tech News, Resource Center, Press Room, Advertising, About Us, and Cart. Below this is a secondary navigation bar with links for My Subscriptions, Magazines, Journals, Conference Proceedings, and Institutional Subscriptions. The main search area features a search bar with a dropdown menu set to 'All'. A callout box points to the search bar with the text 'Key in your search term in the search'. Below the search bar, there is a banner for 'Your New Discovery Platform' with the text 'Browse more than 700k articles on advanced computing topics' and a button for 'Access My Subscriptions'. The main content area displays three featured articles: 'Project Management in Plan-Based and Agile Companies', 'Virt-B: Towards Performance Benchmarking of Virtual Machine Systems', and 'Automation and Future Unemployment'. A 'Latest Articles' section is visible at the bottom left, and a 'Trending' section is at the bottom right.

2. Advanced Search

The screenshot shows the IEEE Computer Society Digital Library advanced search interface. The top navigation bar is the same as in the previous screenshot. Below it is a banner for the '2019 CS Election'. The main search area is titled 'Advanced Search' and features a search bar with a dropdown menu set to 'Keywords, etc.' and a search button. A callout box points to the search bar with the text 'Use Advanced Search to search for specific information.' Below the search bar, there is a filter section with a dropdown menu set to 'AND' and a search button. A callout box points to the filter section with the text 'Narrow your search result by using the filter'. The search results are displayed in a list format, with the first result titled 'A high-performance switch fabric for integrated circuit and packet switching'. A callout box points to the title of the first result with the text 'Click on the title to view the articles'. The search results are filtered to show 'Results 1-10 of 754,501 from the entire library'.

Guide to access IEEE Computer Society Digital Library



3. Search Result

CONFERENCE PROCEEDINGS

Download Export Citation

Home / Proceedings / INFOCOM 1988

IEEE INFOCOM 1988, Seventh Annual Joint Conference of the IEEE Computer and Communications Society

Click Download to view the content if you wish to keep the article in your collections.

Authors

- H. Ahmadi, IBM Zurich Res. Lab., Ruschlikon, Switzerland
- W.E. Denzel, IBM Zurich Res. Lab., Ruschlikon, Switzerland
- C.A. Murphy, IBM Zurich Res. Lab., Ruschlikon, Switzerland
- E. Port, IBM Zurich Res. Lab., Ruschlikon, Switzerland

An architecture is described for a high-performance switching fabric that can accommodate circuit-switched and packet-switched traffic in a unified manner. The switch fabric is self-routing and uses fixed-length minipackets within the switching fabric for all types of connections. Its architecture provides full input/output connectivity paths with FIFO (first-in-first-out) queueing at each output. The connection paths are non-overlapping, so there is no internal blocking. Because of output queueing, there is also practically no output port blocking. The uniformity in architecture allows the construction of any size fabric from a single basic module which could be realized on a single chip. Larger-size configurations can be realized either as single-stage

4. Save the Article

1 of 7

An Intuitive Computer Forensic Method by Timestamp Changing Patterns

Gyu-Sang Cho
Department of Computer Information
Donggang University
Yeongju, Rep. of Korea
cho@dyu.ac.kr

Abstract—This proposes an intuitive computer forensic method by timestamp changing patterns of operations on file in Windows NTFS file system. It is categorized by seven file operations and has its distinguishable patterns by their timestamp changes. The distinct timestamp changing patterns make decision on identifying what kind of file operation is performed. Some patterns are easily identified by their distinct timestamp feature intuitively, and some patterns are needed past timestamp to identify the file operation clearly, and some patterns have ambiguity with similar timestamp patterns. With some performed cases, the forensic method is tested and presented for its usage.

Digital forensics, timestamp changing patterns, intuitive forensic, event reconstruction, NTFS filesystem

1. Introduction

Timestamp evidence is a fundamental ingredient of many forensic computing examinations to reconstruct the event, and the determination of event times is an important and difficult task in computer forensics. MAC times are pieces of file system metadata which record when certain events pertaining to a computer file occurred most recently[1].

There are many researches on timelines based on file system time. Casey[2] has indicated that MAC times analysis is necessary to the reconstruction of digital events. MAC timestamps record a file's most recent modification, access, and creation times. By reconstructing these on a timeline, forensic investigators can find filesystem activity, and computer usage of a particular time. An investigator can also draw a historical plot of filesystem activity per time period[2,3]. Boyd and Forster discussed time structure and their use in Microsoft Internet Explorer with local and UTC time translation issues[4]. Chow et al. presented behavioral characteristics

model that can account for the various factors that affect the behavior of digital clocks such as those used in computers and other digital electronic devices[5]. Willassen presents a hypothesis-based investigation methods to solve the problems of timestamps manipulation and a clock that is erroneous or improperly adjusted[7].

J. Olsson and M. Boldt[8] developed a computer forensic timeline visualization tool that the way of visualizing the evidence allows the investigators to find coherent evidence faster and more intuitively. C. Hargreaves and J. Patterson[9] proposes a technique that can automatically reconstruct high-level events from set of low-level events, analyzing patterns automatically. They described a framework that extracts low-level events to a SQLite backing store, the provenance of any high-level events is also preserved, and the raw data that caused the low-level event to be initially created can also be viewed.

Recently, Choi[10] proposed a method for detecting timestamp forgery in NTFS filesystem. Log records operate on files leave large amounts of information in the \$LogFile that can be used to reconstruct operations on the files and also used as forensic evidence. If the past timestamps can be found before any changes to the file are made, this could act as evidence of a file time forgery. Rule sets for detecting timestamp forgery based on using difference comparison between changes in timestamp patterns by the file time change tool and normal file operations is provided, and the forensic rule sets for ".txt", ".docx" and ".pdf" file types is applied for forensic cases.

There are some forensic researches on other file system. Kevin D. Fairbanks[11] presented a research that a low-level study and analysis of Ext4 file system data

Use the navigation bar to save the document or you can download directly from the website.