NetForce

CyberInvestigator

CyberInvestigator is a tool for network forensics. Network Forensics involves gathering different kinds of logs available in machines which were compromised in an attack. The analysis involves tracing down the intrusions, usage of network and creating a detailed forensic report.

Network Forensics analysts should analyze various types of logs such as Linux, Unix and Windows OS logs, Web Server Logs, Database logs, Firewall Logs, IDS logs, VPN Logs, Router Logs, Proxy Logs, Windows Domain Logs, Wireless Access Point Logs etc. Manual analysis of these logs is very cumbersome and analysts need special tools to efficiently analyze and find out different types of attacks and other types of criminal activities.

CyberInvestigator

Tool for Analysing Server logs and Windows Event Logs

- Supports Windows logs, Linux logs
- Supports analysis of wtmp, utmp, secure, mail, message, cron, access & IIS logs
- Investigator friendly user interface
- Finds out Successful Login & Login Failures
- Finds out the insertion & removal of removable media
- Displays software installation & uninstallation details
- Provides intrusion analysis
- Provides web traffic analysis
- Customized reports

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
THIRUVANANTHAPURAM

CyberInvestigator