

Active Tracking and Archiving Forensic (ATAF) Tool

The ability of the Government to protect essential information, intellectual capital, and law enforcement to detect, identify, arrest, and prosecute criminal and foreign intelligence activities that is targeted against, controlled by, and/or leverage computers and networks is greatly inhibited. This is primarily attributed to a lack of active cyber tracking combined with real-time digital forensics and archiving technologies. Such technologies are autonomous, provide continuous time-based tracking, perform data collections, detect and intercept suspicious activities, categorize data, and separately archive data all at the speed of the machines in the network. Such technologies must be autonomous, provide continuous time-based tracking, perform data collections, detect and intercept suspicious activities, categorize data, and separately archive data all at the speed of the machines in the network.

In parallel with the increasing need to protect sensitive and high-value data, the government has a critical need to detect, investigate, and counter insiders and adversaries intent on using computer and Internet technology to control, attack and/or perpetrate crimes on the US critical information infrastructure. While law enforcement agencies have some computer forensics capabilities, adversaries are aggressively developing and employing new and innovative mechanisms that are currently difficult to detect that hide their activities on their systems and systems they compromise. The recent focus on these mechanisms, called "counter-forensics" at the Black Hat Briefings and DEFCON in Las Vegas (July 2005) demonstrate the importance of developing a whole new paradigm to computer forensics, focused on detecting and defeating these counter-forensics techniques.

The Cyber Space & Information Intelligence Group's Active Tracking and Archiving Forensic (ATAF) tool is a next generation cyber forensic solution with the goal of constantly defeating counter-forensic technologies and empowering law enforcement. ATAF operates in real-time in a heterogeneous, networked environment and performs in a non-intrusive, 24/7 manner. ATAF is comprised of Monitors, each of which resides on a designated networked machine forming an Area of Interest (AOI). These Monitors continuously observe, detect and record all events as directed by the law enforcement operator. This can be as simple as monitoring a file on a computer to tracking, detecting, and logging the activities of one or a group of users.

When the Monitor identifies an event or pattern on a computer or the network, it records the event by creating data about the type of event, associates who performed the event, the time, results of the event, and other related data. The Monitor securely sends this data to a unique Remote File Exchange (RFE) - located separate from the AOI. At the RFE, all data about assets, files, and events are stored in a time-based, versioning data repository that can include a relational database (i.e. SQL - structured query language). With the RFE, analysts have a secured and independent repository of

forensic data that mitigates counter-forensic technologies and can be used to gather and analyze activities of insider criminals or detect and thwart external attackers. RFE provides a pro-active backup mechanism for forensic data and evidence that could potentially be removed or modified, automated Alert Reporting, knowledge extraction, data protection, interrogation and an open, consistent forensic data schema.

POC: Joseph P. Trien, Bob Schlicher, Michael Neergaard, Dave Richardson, Erik Ferragut
Cyberspace Sciences & Information Intelligence Research (CSIIR) Group
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418
www.ioc.ornl.gov