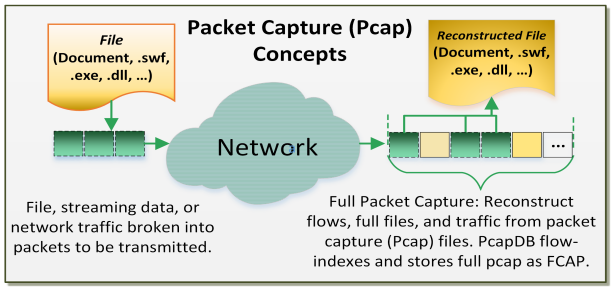
Los Alamos NATIONAL LABORATORY EST 1943

LA-UR-16-25953

PCAPDB

Optimized Full Network Packet Capture for Fast and Efficient Retrieval

Full packet capture is an **essential** component in any cyber security and **incident response** deployment. Access to full packet capture enables **active and post-mortem analysis** that few other data sources can provide. With packet data, analysts can **capture malware** as it enters a network; monitor command and control traffic; **investigate exfiltrated data** during and after a data breach, in addition to many other applications such as cyber forensics and data analytics.



PcapDB is a **new approach** for **packet collection**, **management, searching,** and **collaboration**. This software solution is designed for deployment on commodity hardware and capture cards. PcapDB enables large-scale installations at a significantly lower cost than existing commercial solutions, less than $20K per Capture Node including ~200TB of storage.

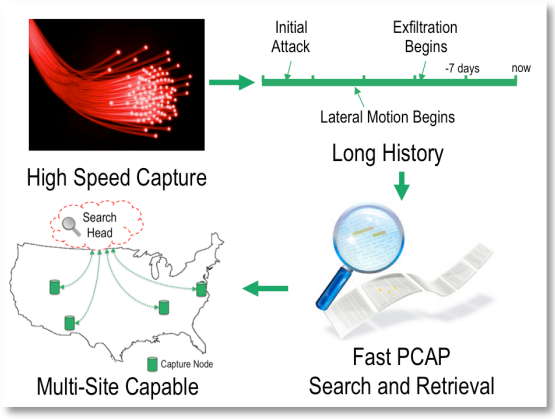
PcapDB is highly **scalable**. It can be installed for single site collection but is ideal for large, **geographically distributed** organizations, such as the Department of Energy.

Grown from **operational needs**, PcapDB's primary goals are:

1. Provide lossless, line-rate packet capture
2. Provide the longest searchable history possible
3. Superior search speeds compared to open source and commercial competitors
4. Multi-site, geographically distributed deployment with central search / retrieval / disk management
5. A low-cost, open-source software solution free from expensive licensing and vendor hardware markup

Cyber incident responders and analysts get what they need:

- Fast searching, orders of magnitude faster for larger searches, vital for time-sensitive response
- Fast, accessible web interface for searching and retrieving Pcap data
- Full Pcap location as part of the search process with lower disk I/O and overall higher efficiency
- No command line packet analyzer needed
- Improved search accuracy, and reduced syntax errors
- Perform search and retrieval **automation via RESTful API** (application programmer interface)



PcapDB is an emerging technology ideal for enterprise-wide deployment, with the following key features:

- Centralized PcapDB Search Head
- Directly manage Capture Nodes: status, storage, user access, and network interfaces via the web interface
- No per-site tunneling or incoming exceptions needed
  - Capture Nodes communicate with Search Head only
- End-to-end encryption between Search Head and Capture Nodes

Pcap data is stored locally at each Capture Node, reducing overall network traffic. Cyber incident responders and analysts can quickly search across the *indexed data* and not raw pcap, drastically reducing the query time, and across multiple capture sites.

- Exceptionally space-efficient PcapDB indexes: < 0.5% the size of captured data, enables very fast searching
- Over 99% of the storage devoted to captured traffic vs. indexes and metadata

PcapDB is currently in Beta deployment at LANL, being piloted at another DOE site, and is part of the DHS Transition to Practice (TTP) program.

Join the community: use, develop, or set up a pilot partnership!

Code and more information at: http://github.com/dirtbags/pcapdb

Shane Steinfadt (shannon@lanl.gov) and Paul Ferrell (pferrell@lanl.gov)