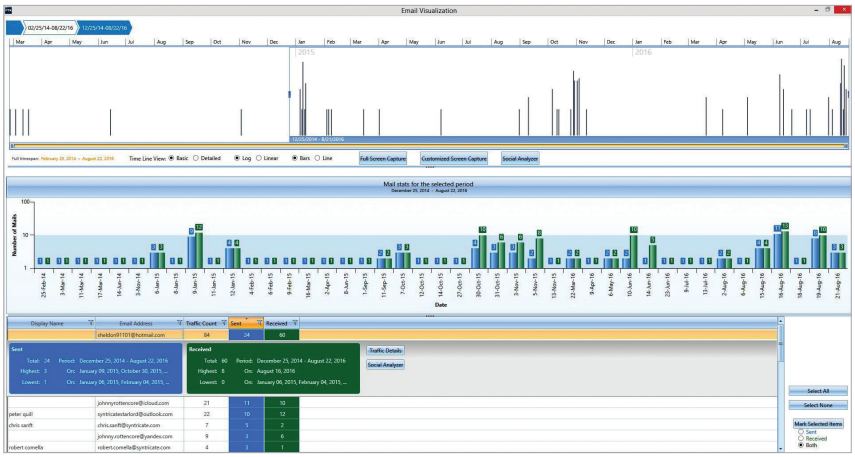

AccessData
Forensic Tool Kit (FTK)

FTK has been a staple workhorse in many forensic shops. We used it as the core computer forensics tool for our university classes because of its ease of use, fast learning curve and comprehensive visualization. In a university class, unlike a typical training class, we wanted to focus on the forensic process rather than the tools. With just a few weeks in a semester to teach the fundamentals of digital forensics there is no time to spend teaching complicated tools. FTK was perfect because it is quick to learn and it gathers a huge amount of information.

FTK is database-driven. As you collect data from a hard drive, the tool puts it into a back-end database and indexes it. Index searches are very fast. If index searching is not for you in a particular circumstance, the live search lets you search for items using search patterns, hex or text. Because the live search seeks cluster to cluster instead of accessing the index, it is much slower. However, this type of searching is not as frequent as index searches.

In earlier versions you had to install each of the components - GUI, database and processing engine - separately and manually. Today the install is all at once and it goes smoothly and quickly. You can deploy up to four separate processing engines and this can speed up evidence processing measurably. Data from other computers over your network can be added to a case simply by deploying an agent. This is useful for threat hunting over an enterprise. FTK can gather data from Windows, Apple and Linux images. The tool can process virtual machine images such as VMWare vmdk files or snapshot files. This greatly speeds up processing VMs but we recommend using the snapshot image since it usually contains the memory capture. The process for that would be to snapshot a VM under attack and then analyze the VM using FTK.

In addition to its simplicity and comprehensive analysis capabilities, FTK has built-in visualization that greatly eases analysis by displaying evidence in various useful ways. For example, there is a timeline display that allows analysis of events on a timebase. The timeline can be basic or detailed - showing the details of each event. Distribution charts also help with analysis. There is a chart for file extension distribution and one for categories distribution, for example.

We use FTK in our lab for all file analysis that we perform as part of our research. The results are predictably useful and the performance in production is excellent. The website is detailed and has a lot of information about AccessData products. Licensing usually is by a dongle but you have the option of a software dongle as well. Pricing is very reasonable and has stayed relatively stable for several years. There are different levels of support available. There are some usful addons, chief among these is the Cerebus a malware forensics tool.

FTK has been one of our Lab Approved products since we started the Lab Approved program and we will continue its SC Lab Approved designation for another year.

– Peter Stephenson, technology editor

DETAILS

Vendor AccessData

Price $3,995.00

Contact accessdata.com/

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Speed, ease of use, comprehensive analysis and fast learning curve.

Weaknesses None that we observed

Verdict FTK will continue to be our computer forensic workhorse and we make it SC Lab Approved for another year.

ACCESSDATA

www.accessdata.com
588 West 400 South Suite 350
Lindon, UT 84042
Main: 801-377-5410