CYTER’s Digital Forensics Team Relies on FTK® to Discover 90% of Data Overlooked by Competitive Tool During E-Discovery in Government Investigation

**Customer Profile**

CYTER is an Australia-based digital forensics and incident response consulting firm that brings together the brightest and most energetic forensic, cyber and technology professionals. The firm was established in July 2017 and delivers smart technology consulting solutions and services to law firms, individuals and organizations in times of digital uncertainty and cyber threat. CYTER specializes in Digital Forensics, Cybersecurity/Incident Response, Data Analytics, and Technology Disputes.

**Situation**

CYTER was engaged recently by a well-known law firm in Australia to provide e-discovery consulting services for a major government investigation into one of the firm’s clients. Yian Sun, a senior forensics specialist at CYTER, was the lead consultant for the matter.

“I have over 15 years of experience working for a number of professional services firms, primarily in the areas of digital forensics and incident response, so I am familiar with the landscape of government investigations and the importance of conducting accurate data collections,” said Sun. “This engagement was large and highly sensitive, making it crucial..."
for our team to be very thorough with the data discovery, starting with the early case assessment the lawyers asked us to perform.”

Sun is a long-time user of AccessData’s FTK® software. FTK (Forensic Toolkit®) is a court-cited digital investigations platform built for fast processing, stability and ease of use, while handling massive data sets. It provides comprehensive processing and indexing up front, so filtering and searching is faster than with any other product. This means users can “zero in on” the relevant evidence quickly and conduct their analysis faster.

“Sun and his CYTER colleagues used FTK to conduct an early case assessment of the electronic data that was relevant in the investigation and provided a report to their law firm client. At this point, the team found nothing especially out of the ordinary in the matter.

“I have relied on FTK for more than a decade because it is a powerful and fast digital forensics tool for obtaining an accurate first-pass look at a universe of data,” said Sun. “It is one of our firm’s principal software products for investigations worldwide, but little did we know how important it would be in this case.”

Sun’s team extracted this “missing” data by returning to the original FTK early case assessment case and provided it to their law firm client.

“We quickly discovered that the other tool had failed to recover tens of thousands of deleted emails that FTK had properly identified and analyzed.”

—Yian Sun
Senior Forensics Specialist, CYTER

Competitive Tool Misses 90% of Data

After the law firm received CYTER’s early case assessment report, they used a different tool—a well-known competitor to FTK—to reprocess the same raw data universe, following their normal workflow protocols for quality assurance. To the astonishment of both Sun and the lawyers, the competitive tool surfaced just 10% of the data that FTK harvested.

“We were stunned and immediately conducted an analysis so we could get to the bottom of this enormous discrepancy between the results sets,” said Sun. “We quickly discovered that the other tool had failed to

recover tens of thousands of deleted emails that FTK had properly identified and analyzed.”

Sun’s team extracted this “missing” data by returning to the original FTK early case assessment case and provided it to their law firm client.

“Although the specific technical issues with the other tool were unclear, what was obvious to our team is that FTK is much easier to set up prior to processing, comes with excellent training to operate the tool, and is backed by a level of processing robustness that helps to avoid this kind of serious problem,” said Sun.
Further Comparison with Other Well-Known Forensic Tools

Following the discovery of this issue, as a test, Sun used 3 other well-known forensic tools to process the same dataset. The results of the test showed only 1 of the 3 forensic tools for testing yielded same/or close to the same results as FTK. The other 2 forensic tools also did not pick up the additional 90% of deleted emails.

FTK Benefits

Sun uses a wide array of digital forensics and incident response software products on his various engagements, employing the best tool for each specific need, so he has an objective perspective on how the leading products on the market compare to each other. He points to four primary benefits his firm has experienced from using FTK:

1. Robust processing of data up front
   “FTK processes and indexes data on the front end, which eliminates wasted time otherwise spent populating a searchable database,” said Sun. “This is crucial in the fast-paced environments of litigation and government investigations.”

2. Support for all data types
   FTK collects, processes and analyzes data sets of all formats and file types—including Apple® File Systems, LX01 and E01 images, AFF4 images, XFS file systems, McAfee-encrypted drives and many others.

3. Fast searching
   “Whether you’re investigating or performing document review, you have a shared index file, eliminating the need to recreate or duplicate case files amongst your team,” said Sun. “So no matter how many different data sources
you're dealing with or the amount of data you have to cull through, FTK gets you there faster.”

4. Clear reporting
Sun finds the FTK-generated reports to be easily generated, quickly produced and—most importantly—are very clear for the entire team to read and understand. This is a key to effective case management and helps CYTER's clients develop a strategy with greater insights into the evidence that will be surfaced.

5. Flexibility to perform additional analysis
Sun finds that FTK allows him to perform customized processing of various types of data with the flexibility of performing additional processing/analysis of the same dataset all in the same case. “Many other tools do not allow me to customize the processing options to the degree that FTK offers,” said Sun. “So with FTK we are able to perform selective processing to allow us to get to our primary objective quicker with the added flexibility of performing further analysis down the track.”

“Our experience in this case provided a stark example of why FTK is still our go-to digital forensics tool for obtaining a fast and accurate look at the universe of data in a case or investigation,” said Sun. “Digital forensics professionals can be confident that FTK will surface and collect all relevant data right up front, while there is clearly a risk that other tools on the market will overlook potentially important evidence.”

Summary
Some of the leading digital forensics software tools on the market can be so burdensome to implement and so complex to operate that they open the door to serious errors with collection and processing of data. CYTER's experience illustrates that FTK is much easier to set up prior to collection and processing, is accompanied by excellent training from AccessData to operate the software, and is backed up by a world-class level of customer support to help troubleshoot any problems or resolve any challenges.