



**AccessData®**

# Legal Brief

**Recent Court Validation of Forensic Toolkit® Technology**

AccessData's FTK is the standard computer forensic product used by the U.S. Federal Bureau of Investigation. As such, FTK is constantly being recognized by courts as an effective tool to extract and analyze electronically stored information. In addition to the cases mentioned in the main body of this document, here are a few more representative cases:

*United States v. Calimlim, 2005 WL 2922193 (E.D. Wis., November 4, 2005).*

The government's examiner used FTK to search data and unallocated space, which included e-mails, the internet, typed documents, and deleted items. The examiner conducted the forensic examinations using the keyword and scanning methodologies available in FTK.

*United States v. Eberle, 2006 WL 1705143 (W.D. Pa, June 15, 2006).*

In Eberle, the question was whether certain ESI was on a particular computer. The question was resolved using FTK, whereby "Detective Lynn performed a more targeted search known as a 'hash value check,' whereby she searched for a specific identifier, known as an MD5 hash, that is particular to an internet image, much like a fingerprint. This hash check similarly failed to uncover any of the images that had been uploaded onto the Yahoo! Server in 2001." Id. at \*2.

*United States v. Aldeen, 2006 WL 752821 (March 22, 2006).*

Defendant Ahmed Aldeen, moved the court to order the government to provide him with a mirror image of his computer hard drive allegedly containing images of child pornography. This case was prosecuted prior to the Adam Walsh Act that enables the government to prevent release of any material or copies of materials seized that involve child pornography. At the time however, the court did find the defense argument so convincing that it allowed the defendant's computer experts to utilize their own personal computers so that they could run two computer programs, one being FTK, to examine the videos.

*In re Atlantic Intern. Mortg. Co., 352 B.R. 503, 509 (Bankr. M.D. Fla. 2006).*

In this bankruptcy proceeding, attorneys for the debtor hired a forensic examiner to conduct an investigation of certain electronic documents, and the examiner used FTK to perform the examination.

*Sanders v. State, 191 S.W.3d 272 (Tex.App. - Waco, March 8, 2006).*

In this case, the examiner, who was trained and well versed in FTK, discovered multiple instances of child pornography on the Defendant's computer. The appellate court refused to overturn the lower court's acceptance of the expert's testimony.

*United States v. Butts, 2006 WL 3613364 (D. Ariz., December 6, 2006).*

In this Adams Walsh Act issue, the government moved the court to limit Defendant's access to the electronic evidence. Since the Adams Walsh Act was effective *after* the filing of the present case, the court had the option of denying the government's motion for reconsideration. However, the court granted the government's motion and limited the Defendant's ability to review the evidence. FTK was used by the Defendant's expert to examine the evidence.

*Commonwealth v. Koehler, 914 A.2d 427 (Pa. Super. 2006).*

In this criminal case, the Court found that there was reasonable suspicion to conduct a warrantless property search of a parolee's residence and computer. The search resulted in a computer forensic analysis that uncovered sufficient evidence that Mr. Koehler possessed child pornography. The computer forensic examination of Koehler's computer hard drive was performed by Erie County Detective Jessica Lynn, who used FTK to analyze the images on Koehler's computer. Detective Lynn discovered 235 video clips depicting children and more than 300 items that were suspect as child pornography. Detective Lynn's findings against Appellant resulted in 19 charges filed against him which lead to Koehler being sentenced to 12 to 24 months of incarceration for each of his fourteen counts.

*United States v. Flinn, 521 F.Supp.2d 1097 (E.D. Cal., October 16, 2007).*

In Flinn, the Defendant was charged with receiving and possessing child pornography. The government seized the defendant's computer where he had allegedly received and stored the child pornography. Due to the Adam Walsh Act, the government could not release any copies or duplicative material since the material contained child pornography. Rather, under 18 U.S.C.A. § 3509(m)(2)(B), the government was required to provide the Defendant "ample opportunity for inspection, viewing, and examination at a government facility." The Court recognized this statute to mean that, where the government can supply "reasonably up to date hardware and software tools and facilities such that a defendant can construct a reasonable, available forensic defense." The facility used was the former McClellan Air Force Base where computers were available with all of the relevant materials to perform a forensic analysis. The software implemented and made available for use was FTK-1 which the Court recognized as a "standard." The Court found that the available hardware and software provided was sufficient to uphold the Defendant's discovery rights and thereby denied the Defendant's motion to use its own facilities to examine mirror images of the evidence on their own computer.

*Tauck v. Tauck, 2007 Conn. Super. LEXIS 2618 (Conn. Super. Ct., Sept. 21, 2007).*

In a bitter divorce case, which cost more than \$13 Million in legal fees for both sides, computer forensics was used to determine whether allegations, made by Nancy Tauck against her husband, Peter Tauck, were valid. Nancy Tauck accused her husband of possessing child pornography, and Peter Tauck's old Toshiba laptop was one of the materials seized and examined. An expert from Global CompuSearch LLC, a computer forensics service provider, examined the laptop for the husband and served as his expert witness, testifying at the trial. After forensic analysis, Marcus Lawson, President of Global CompuSearch LLC, refuted the claims made by Nancy Tauck. Global CompuSearch was given six hard drives to examine in which there were found numerous "suspect" images. However it was also discovered that 148 of those images were downloaded on May 5, 2005, which was the date Peter Tauck's passport verified that he was in Tahiti. The question then became: "From what location were the images downloaded?" Global CompuSearch found an Internet protocol ("IP") address that led them to conclude the download took place from within the state of Connecticut, where the wife was at the time. The forensic expert further stated that he found no evidence that anyone had altered the system date on the computer. Furthermore, Global CompuSearch found that a substantial number of files on other computers had been deleted from the internet cache folders. With this information, they were able to illustrate that some deliberate action was taken to eliminate information on that computer so there would be no internet browsing history to show which sites were visited. The Court found that the evidence did not corroborate Nancy Tauck's allegations and that it was clear that the download of the suspected photographs took place when Peter Tauck was half way across the globe. The Court concluded from the forensic evidence that Nancy Tauck, or other unknown persons, planted the images onto the computer while Peter Tauck was away.

*United States v. Fumo, 2007 WL 3232112 (E.D. Pa, October 30, 2007).*

In this case, the government had used FTK to examine Fumo's computer system. The Defendant moved the court to compel the government to disclose the search protocol and keyword terms under Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure in order to determine whether the search and seizure violated his Fourth Amendment Rights. The Court concluded that the "requested information [was] not material to application of the exclusionary rule" and denied the motion.

*United States v. Luken, 515 F.Supp.2d 1020 (D.S.D, August 21, 2007).*

In this opinion, the Magistrate Judge recommended that the Defendant's motion to dismiss be denied. The Magistrate determined that the Defendant had consented to the search of his laptop, and the evidence of child pornography found using FTK by the agent was admissible.

*United States v. Sage, 2007 WL 4592074 (W.D.Mo., December 27, 2007).*

In this statutory rape case, a motion to suppress the computer evidence was denied. The forensic examiner used FTK to examine the Defendant's computer and used FTK to organize the materials and retrieve the evidence that linked the Defendant to the under-aged victim and other younger males.

*United States v. Potts, 2008 WL 2051090 (D. Kan. 2008).*

In this case, the defendant moved to suppress evidence gathered through an "overly broad" search warrant. Attachment B of the warrant "lists evidence pertaining to images of child pornography, and sexual activity with children." *Id.* at \*5. "The search warrant authorized a search of defendant's residence, including any computers and electronic storage devices found in defendant's residence." *Id.* The judge noted that the examiner of the computer, Sergeant Owen, "did not engage in an impermissibly broad search for the items listed in the warrant." *Id.* at \*22. Because, "[w]hile the warrant allowed Sergeant Owen to open every file and look at the first few pages, he did not need to do so because such a broad search is unnecessary with modern forensic software." *Id.* at \*21. The court specifically identified "forensic software, including Forensic Toolkit" (FTK). *Id.* at \*10.

*United States v. Richardson, 583 F.Supp.2d 694 (W.D. Pa. October 31, 2008).*

Agents used FTK to search the Defendant's laptops, where child pornography was found.

*Gutman v. Klein, 2008 WL 4682208 (E.D.N.Y., October 15, 2008).*

In this civil action, the defendant was suspected of accessing the website [www.ntfs.com](http://www.ntfs.com) and deleting files from a laptop before handing over the device for discovery. The plaintiff's examiner used FTK to image the hard drive of the laptop. The court-appointed forensic expert, Stroz Friedberg, referenced in his report that FTK version 2.2 is an "accepted tool under industry standards, to perform the imaging and create a forensic duplicate of the hard drive."

*State v. Voorhees, 2008 WL 2579709 (Ohio App. 3 Dist., June 30, 2008).*

In a child rape case, the State's forensic examiner used FTK to find more than 1,700 images of child pornography and videos on the Defendant's computer and under which account they existed and/or were accessed.

*United States v. Mann, 2008 WL 1701743 (N.D. Ind., April 8, 2008).*

In this criminal case involving child pornography, a laptop was seized into evidence and examined using FTK. The court indicated that FTK is a "software commonly used by many forensic computer examiners." FTK was used for various purposes of the computer investigation, including KFF alerts (known file filter) and uncovering websites that the Defendant had visited. A motion to suppress the evidence by Defendant was only granted in part for the physical objects recovered (papers, cords, adapters). However, the motion to suppress evidence from computer investigation was denied.

*United States v. Graziano, 558 F.Supp.2d 304, 75 Fed. R. Evid. Serv. 1220 (E.D.N.Y., March 20, 2008).*

In an arson case, the defendant moved to suppress fruits of the search of his home and computer. "In terms of the procedure employed during the search of the computer, [the examiner] used a software package called Forensic Tool Kit ("FTK"), which searches through the entire file system..." *Id.* 558 F.Supp.2d at 313. "In the instant case, when the files were sorted by FTK, [the examiner] recognized that there was a significant amount of evidence found in the internet history files." *Id.* at 314. Further utilizing FTK, the examiner was able to identify a file "search [3].htm" that contained evidence of "an AOL search using the terms 'arson rico laws' at one time in the search box." *Id.* The Court concluded that "the examiner's search of the computer and discovery of that evidence was executed in a manner that was within the scope of the warrant and was reasonable under the Fourth Amendment." *Id.* at 317.

*United States v. Gaynor, 2008 WL 113653 (D.Conn., January 4, 2008).*

This opinion focused on a motion to provide copies of ESI to Defendants who were charged with possession of child pornography. The Adam Walsh Act prohibited the Defendants from obtaining copies of child pornography (even as evidence) limited its exposure to the Defendants by requiring any viewing to be done at a government facility. The Court acknowledged FTK and EnCase as the most commonly used forensic tools used by forensic examiners for computer investigations. The government offered to provide Defendant's examiner with a computer that met the minimum system requirements for both FTK and EnCase so that an examination could be conducted.