

LAW ENFORCEMENT SENSITIVE
FOR OFFICIAL USE ONLY

Border Searches of Electronic Devices

(b)(2); (b)(7)(E)

he following examples are representative of ICE investigations that are predicated upon searches of electronic media at the border:

CHILD PORNOGRAPHY

CASE # (b)(2); (b)(7)(E)

In July, 2006, SUBJECT entered the (b)(2); (b)(7)(E) driving a Ford van. Accompanying SUBJECT in the van was a five year-old Hispanic boy. As SUBJECT (b)(2); (b)(7)(E) Customs and Border Protection (CBP) officers referred SUBJECT and the child to the secondary lot for further examination. In the secondary lot, a video camera and videotapes were discovered in the van. One of the videotapes contained footage of a prepubescent child being molested digitally and orally by a man who appeared to be SUBJECT. SUBJECT was subsequently arrested for violation of 18 USC 2422(a): Transportation and Possession of Child Pornography.

CASE # (b)(2); (b)(7)(E)(b)(2); (b)(7)(E)

In June 2007, SUBJECT arrived at (b)(2); (b)(7)(E) SUBJECT told CBP that he had traveled to Philippines to visit an orphanage named "House of Joy" (HOJ). SUBJECT said that he entertained the orphans at HOJ through his work as a clown. (b)(2); (b)(7)(E)

CBP deemed it appropriate to review the images on SUBJECT's digital media devices to ensure they did not contain any images of child pornography. During a secondary inspection by CBP officers, in excess of sixty (60) images naked minor Filipino boys were discovered saved on SUBJECT's laptop computer and digital camera memory card. After further review at the (b)(2); (b)(7)(E) it was determined that the images of naked minor Filipino boys on SUBJECT's laptop and digital camera constituted images of child pornography.

CASE # (b)(2); (b)(7)(E)

In December 2006, SUBJECT, a foreign national with Lawful Permanent Resident (LPR) status, made entry into the United States along with his father. CBP received a negative

LAW ENFORCEMENT SENSITIVE
FOR OFFICIAL USE ONLY

oral declaration from both and subsequently referred the subjects and the vehicle for an enforcement examination. CBP conducted the secondary examination of the subjects and the vehicle, during which a laptop computer was observed in the back seat. An initial search of the laptop revealed thousands of images, several of which were pornographic in nature. When questioned, SUBJECT claimed ownership of the laptop and its contents. When asked if the laptop contained images of child pornography, SUBJECT stated that he was not sure because he hadn't been able to check his temporary Internet files. At that point, a further examination of the laptop was conducted which resulted in the discovery of Internet Explorer files with titles including "two year old raped during diaper change" and "seven year old gives her uncle a blow job". After discovering those file titles, CBP terminated his examination of the laptop computer and notified the reporting agent of his findings.

CASE # (b)(2); (b)(7)(E)

In September 2008, SUBJECT entered the United States at the (b)(2); (b)(7)(E). SUBJECT was selected by CBP for a secondary enforcement exam. During the examination CBP discovered an image on SUBJECT's laptop computer of a young female (approximately 5 yrs old) blindfolded and posing in the nude. CBP contacted an (b)(2); (b)(7)(E) who responded and viewed the image. The (b)(2); (b)(7)(E) also found an image of that same child engaged in sexual acts with an adult male.

FINANCIAL

CASE # (b)(2); (b)(7)(E)

In November 2006, CBP at the (b)(2); (b)(7)(E) received information from (b)(2); (b)(7)(E) that SUBJECT would be flying into (b)(2); (b)(7)(E) aboard a specific flight with a large amount of cash. When SUBJECT arrived at (b)(2); (b)(7)(E) CBP explained the US currency reporting requirements to SUBJECT who declared \$18,000. A search of SUBJECT's luggage yielded a total of \$78,883. (b)(2); (b)(7)(E) responded to talk with SUBJECT. CBP also inspected a Toshiba laptop that was found in SUBJECT's possession, which contained files regarding cyanide and nuclear materials. The (b)(2); (b)(7)(E) accepted prosecution, and SUBJECT was arrested for violations of 31 USC 5316 and 5332. SUBJECT was not charged with terrorism related offenses.

NATIONAL SECURITY

CASE # (b)(2); (b)(7)(E)

In September 2006, SUBJECT, a citizen of (b)(2); (b)(7)(E) and nonimmigrant student at a U.S. university, arrived by air at (b)(2); (b)(7)(E). During a search of his luggage, CBP discovered a computer memory stick containing a document stating SUBJECT's opposition to the war in Iraq. SUBJECT voluntarily logged-in to his laptop computer at the request of CBP. A review of the laptop computer

LAW ENFORCEMENT SENSITIVE
FOR OFFICIAL USE ONLY

revealed numerous video files depicting Improvised Explosive Devices (IED) being detonated against U.S. soldiers and vehicles, U.S. Marines under mortar attack, martyrdom training, and a possible terrorist training camp. In addition, a search of an external hard drive found in SUBJECT's luggage revealed additional IED video files and a document written in Arabic containing the term "H₂O₂." H₂O₂ is the molecular compound for Hydrogen Peroxide. A complete translation of the document revealed instructions for producing concentrated Hydrogen Peroxide, a highly volatile explosive element that was associated with the Summer 2006 London plot to destroy airliners over the Atlantic Ocean using liquid explosives.

On this same date, (b)(2); (b)(7)(E) arrested SUBJECT for providing false statements to government officials (CBP) in violation of Title 18, United States Code, Section 1001. Additionally, (b)(2); (b)(7)(E) seized SUBJECT's laptop computer, external hard drive, and computer memory stick. A subsequent search of these items by (b)(2); (b)(7)(E) revealed additional files related to IEDs, bomb-making, and terrorist recruitment. Additionally, (b)(2); (b)(7)(E) discovered that SUBJECT had located an Iraqi Special Weapons Facility and a coalition airbase utilizing Google Earth software.

In December 2006, SUBJECT pleaded guilty in the (b)(2); (b)(7)(E) to violating Title 18, United States Code, Section 1546 – Fraud and misuse of visas, permits, and other documents. SUBJECT was sentenced to time served and agreed to expedited removal to (b)(2); (b)(7)(E). On January 29, 2007, the (b)(2); (b)(7)(E) removed SUBJECT from the United States under escort to (b)(2); (b)(7)(E).

CASE # (b)(2); (b)(7)(E)

In February 2007, SUBJECT, a (b)(2); (b)(7)(E)

(b)(2); (b)(7)(E) SUBJECT sought admission as permanent resident based on an approved immigrant visa for being the immediate relative of a United States citizen and presented CBP Officers with a valid (b)(2); (b)(7)(E) passport and immigrant visa (IR2). During an initial inspection and a subsequent deferred inspection, CBP officers discovered a laptop computer and external hard drive. A preliminary search of the laptop computer revealed open-source jihadist and anti-American publications that were downloaded from the Internet. A search of the external hard drive revealed martyrdom videos of Palestinian suicide bombers. These files included an audio file of an individual stating, "I am going to take part in a suicide mission; I will blow myself up because of what Israel has done to Palestine."

Between February 21, 2007 and February 23, 2007, (b)(2); (b)(7)(E) interviewed SUBJECT. During the interviews, SUBJECT stated that he had been recruited by Hamas, donated money to Hamas, and that his first cousin was a suicide bomber who detonated himself. SUBJECT further stated that while studying at (b)(2); (b)(7)(E) he resided with three Hamas members who participated in the Second

LAW ENFORCEMENT SENSITIVE
FOR OFFICIAL USE ONLY

LAW ENFORCEMENT SENSITIVE
FOR OFFICIAL USE ONLY

Intifada. Subsequently, [REDACTED] conducted extensive forensic analysis of SUBJECT'S computer, revealing hundreds of meticulously-organized pro-jihadi and pro-al Qaeda files. In May 2007, the [REDACTED] (b)(2); (b)(7)(E) filed an additional charged under Section 212(a)(3)(B)(i) of the Act, an alien who has engaged in terrorist activity.

LAW ENFORCEMENT SENSITIVE
FOR OFFICIAL USE ONLY