IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
	:	**Criminal Action No. 1:07-cr-211**
v.	**:**	
	:	**(Chief Judge Kane)**
ROBERT ELLSWORTH CRIST, III,	**:**	
Defendant	**:**	

MEMORANDUM

Before the Court is Defendant Robert Ellsworth Crist's motion to suppress evidence. Crist's motion presents a question involving the important and developing law concerning the manner in which established principles of Fourth Amendment law apply to police searches of electronically stored information. In his motion, Crist challenges the warrantless search of his computer and moves for the suppression of video files of child pornography recovered from his computer. Crist also seeks to suppress statements elicited from him during an interview conducted at his home in January 2007. He contends that these statements were made involuntarily and should therefore be suppressed. For the reasons that follow, Crist's motion will be granted in part and denied in part.

I. BACKGROUND

A. Factual Background

Beginning in June 2004, Crist rented a house in Camp Hill, Pennsylvania. He was not a model tenant: Crist did not make rent payments in January, March, or April 2005. Though his lease was set to expire on May 31, 2005, Crist's mother made back payments on his behalf in May, and his landlord agreed that Crist could remain in the house as a month-to-month tenant. After Crist failed to make full rent payments for July and August, Crist's landlord hired Jeremy Sell and his father, Kirk Sell, to move Crist's belongings from the house. Meanwhile, Crist had

made arrangements to move at least some of his possessions and most of his furniture. Crist had not finished moving all of his belongings by the time the Sells arrived at his house.

The Sells observed squalid conditions in Crist's house. They found wet clothes strewn in the garage, and they discovered mouse feces on the kitchen countertop. Scattered throughout the nearly vacant rooms were Crist's possessions, including a keyboard, a PlayStation gaming console, and a personal computer. After taking photographs of the house, the Sells began removing Crist's possessions and placing them on the curb for trash pickup.

On or about August 10, 2005, young Jeremy Sell called his friend Seth Hipple, who Sell knew was looking for a computer, to let Hipple know that he would be putting Crist's computer out for trash. Hipple came shortly thereafter and claimed the computer. Later that day, Crist came to his house, discovered the Sells removing his possessions, and confronted them. After the Sells explained what they were doing, Crist angered. Tr. 21.[1] Crist "went in the house, started going through bags out in the street. And he specifically asked [Kirk Sell], where is my computer?" Id. The Sells, knowing that Hipple had already taken the computer, professed ignorance as to its whereabouts. Soon after, Crist called the East Pennsboro Township Police Department to complain of the theft of his computer, and Officer Adam Shope took a report of his complaint. Tr. 47.

In the meantime, Hipple took Crist's computer to his friend's house, where they "tried to get it running, tried to basically just clean it up, get past the profiles, if there were any." Tr. 33.

---

[1] The suppression hearing transcript in this case consists of two volumes and the transcript from a second oral argument. The Court will refer to the first volume as "Tr.", the second volume as "Supp. Tr.", and the transcript from the October 8, 2008 oral argument as "2d Supp. Tr."

Hipple then took the computer to his home, where he began to "go through it to see what [he] could delete." Id. After looking through a "bunch of songs" on a media folder, Tr. 37, Hipple opened up a couple of video files depicting children performing sexual acts. Tr. 33-34. Hipple "freaked out," deleted the entire folder, "songs and everything," and turned off the computer. Tr. 34.

A few days later, on August 13, 2005, Hipple contacted the East Pennsboro Township Police Department. When an officer arrived, Hipple explained that he had found the computer and that he had discovered child pornography on it. Hipple also "reported that he deleted the file right away." (Def.'s Ex. 1, at 6.) A report was taken, and the computer was logged into evidence.

Detective Michael Cotton at the East Pennsboro Township Police Department was assigned to conduct an investigation into suspected child pornography. Detective Cotton was informed that the computer in question belonged to Crist, that Hipple took possession of the computer while Crist was being evicted from his home, and that Hipple discovered "several items or several files" containing suspected child pornography. Detective Cotton also became aware at some point that Crist had reported his computer stolen. Despite that fact, Cotton contacted the Pennsylvania Attorney General's Office ("AG's Office") to have the computer forensically examined.[2]

On September 30, 2005, the AG's Office took custody of Crist's computer in order to conduct a forensic examination. The AG's Office was informed that the computer was "seized

[2] The record is not clear on when Detective Cotton became aware of Crist's complaint regarding his computer. At various points in his testimony, it seemed that he was aware from the outset, see, e.g., Tr. 42, 47, but at other points, he claimed to have learned of the complaint only *after* the computer was brought in by Hipple, see Tr. 51. In any event, it is clear that Detective Cotton knew that Crist had reported his computer stolen before he contacted the AG's Office.

pursuant to consent from its owner" and that the purpose of the exam was to "analyze and recover any data related to the possession of child pornography and as otherwise directed by the case investigator." (Def.'s Supp. Ex. 1, at 1.) On October 3, 2005, David Buckwash, a special agent within the computer forensics department, conducted the forensic examination of Crist's computer.

In the forensic examination, Agent Buckwash used the following procedure. First, Agent Buckwash created an "MD5 hash value" of Crist's hard drive. An MD5 hash value is a unique alphanumeric representation of the data, a sort of "fingerprint" or "digital DNA." When creating the hash value, Agent Buckwash used a "software write protect" in order to ensure that "nothing can be written to that hard drive." Supp. Tr. 88. Next, he ran a virus scan, during which he identified three relatively innocuous viruses. After that, he created an "image," or exact copy, of all the data on Crist's hard drive.

Agent Buckwash then opened up the image (not the actual hard drive) in a software program called EnCase, which is the principal tool in the analysis. He explained that EnCase does not access the hard drive in the traditional manner, i.e., through the computer's operating system. Rather, EnCase "reads the hard drive itself." Supp. Tr. 102. In other words, it reads every file—bit by bit, cluster by cluster—and creates a index of the files contained on the hard drive. EnCase can, therefore, bypass user-defined passwords, "break[] down complex file structures for examination," and recover "deleted" files as long as those files have not been written over. Supp. Tr. 102-03.

Once in EnCase, Agent Buckwash ran a "hash value and signature analysis on all of the files on the hard drive." Supp. Tr. 89. In doing so, he was able to "fingerprint" each file in the

computer. Once he generated hash values of the files, he compared those hash values to the hash values of files that are known or suspected to contain child pornography.[3] Agent Buckwash discovered five videos containing known child pornography. Attachment 5.[4] He discovered 171 videos containing suspected child pornography. Attachment 8.

Afterward, Agent Buckwash "switch[ed] over to a gallery view, which gives us all the pictures on the computer," and was able to "mark every picture that [he] believe[d] is notable, whether it be child pornography or . . . something specific." Supp. Tr. 95. Ultimately, he discovered almost 1600 images of child pornography or suspected child pornography.

Finally, Agent Buckwash conducted an internet history examination by reviewing files known as "index [dot] dat" files, which roughly amount to a history of websites the computer user has visited. After extracting the index [dot] dat files, Agent Buckwash used a program called NetAnalysis, which "allows you to sort for suspected child pornography." Supp. Tr. 96. After Agent Buckwash completed the forensic examination, he generated a report of his findings and presented it to Detective Cotton.

In January 2007, more than a year after the computer had been sent to the AG's Office for an examination, Detective Cotton and two agents from the Federal Bureau of Investigation

---

[3] According to Agent Buckwash's testimony, the National Center for Missing and Exploited Children maintains a database of hash values of "known" child pornography files, which are files that have been found to contain child pornography and the name of the victim is known. The database also contains hash values of "suspected" child pornography files, which are files that contain depictions of child pornography but the name of the victim is not known.

[4] Agent Buckwash's memorandum to Detective Cotton, submitted at the March 13 hearing as Defendant's Exhibit 2, refers to the parts of his Computer Forensics Analysis as "Attachments." To maintain consistency, the Court also refers to parts of such exhibit as Attachments.

("FBI") went to Crist's house to attempt to interview him. Very early in the morning and dressed in suits, the officers arrived at Crist's house and knocked on the door. After several knocks, Crist "jumped off the couch and came to the front door." Tr. 44 (punctuation omitted). After the officers identified themselves, Crist invited them into his dining room.

In the dining room, Detective Cotton informed Crist that "he was not under arrest and [that] he did not have to talk to [the officers], but probably it would be in his best interest to sit down and talk to us and listen to what [they] said." Id. The officers began to ask Crist questions and ultimately told him that they had discovered child pornography on his computer, at which point Crist admitted that he had put the files on the computer. At some point during the conversation, Crist asked "Do I need a lawyer?" to which Agent Thew replied that it was his choice whether to seek counsel. Tr. 50. According to Crist, he stated on at least two occasions that he thought he should be speaking to an attorney, but he was told that he did not need an attorney and that he was in the best position to make the choice of whether to consult with an attorney. At no point, however, did the officers advise Crist of a right to counsel or a right to remain silent.

B. Procedural Background

On May 23, 2007, a grand jury returned a two-count indictment charging Crist with knowingly receiving and possessing digital images and video files containing child pornography in violation of 18 U.S.C. §§ 2252A(a)(2)(A) & 2252A(b). (Doc. No. 1.) He pleaded not guilty, and on July 24, 2007, Crist was released on conditions. (Doc. No. 27.)

On August 15, 2007, Crist filed the instant motion to suppress evidence (Doc. No. 30) and a brief in support of the motion (Doc. No. 31). The Government thereafter filed a brief in

opposition (Doc. No. 41), to which Crist replied (Doc. No. 44). On January 24, 2008, the Court held a hearing on the motion at which the following individuals testified: Crist's landlord, Kirk Sell, Jeremy Sell, Seth Hipple, Detective Cotton, Crist, and Agent Thew. After the hearing, the Court ordered a supplemental hearing on the "nature, scope and methodology of the Office of the Attorney General's forensic examination of Defendant's computer." (Doc. No. 54.) That supplemental hearing was held on March 13, 2008, and Agent Buckwash testified. The Court then permitted supplemental briefing (Doc. No. 64), and on April 18, 2008, Crist filed a supplemental brief in support of the motion (Doc. No. 66). On May 22, 2008, the Government filed a supplemental brief in opposition (Doc. No. 72), to which Crist replied on June 4, 2008 (Doc. No. 75). The Court then held an additional oral argument on October 8, 2008.

II. SUPPRESSION OF COMPUTER EVIDENCE

A. General Principles

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

It is a "most basic constitutional rule . . . that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions.'" Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)). Warrantless searches are thus presumptively unreasonable. Kyllo v.

United States, 533 U.S. 27, 31 (2001). However, under the test applied by the Supreme Court, "a Fourth Amendment search does not occur . . . unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society is willing to recognize that expectation as reasonable.'" Id. at 33 (quoting California v. Ciraolo, 476 U.S. 207, 211 (1986)). As the Supreme Court recently stated: "Official conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." Illinois v. Caballes, 543 U.S. 405, 408 (2005) (quoting United States v. Jacobsen, 466 U.S. 109, 123 (1984)).

B. Abandonment

The Government first argues that Crist retained no reasonable expectation of privacy in his computer because he abandoned it. The Government argues that because Crist failed to make rent payments and "left the property in a condition that not only made it uninhabitable but also violated [a] provision of the lease" (Doc. No. 41, at 13), he maintained no objectively reasonable expectation of privacy. The Court disagrees.

It is settled that an individual does not retain a reasonable expectation of privacy in items that are abandoned. California v. Hodari D., 499 U.S. 621, 629 (1991) (upholding warrantless seizure of narcotics that defendant threw away while fleeing from police); Abel v. United States, 362 U.S. 217, 241 (1960) (upholding warrantless seizure of items thrown away in hotel trash can where individual had checked out of the hotel); United States v. Fulani, 368 F.3d 351, 354 (3d Cir. 2004) (upholding search of personal luggage contained in bag where defendant disclaimed ownership of bags in overhead rack). However, as the Third Circuit has held, "[a]bandonment for purposes of the Fourth Amendment differs from abandonment in property

law; here the analysis examines the individual's reasonable expectation of privacy, not his property interest in the item." Fulani, 368 F.3d at 354. In order to find that an individual has abandoned his property, the court must "determine from an objective viewpoint whether property has been abandoned," and the court must find, by "clear and unequivocal evidence" that the individual intended to abandon the property. Id. (citing United States v. Moody, 485 F.2d 531, 534 (3d Cir. 1973)); see also United States v. Sinkler, 91 F. App'x 226, 231 (3d Cir. 2004) ("Abandonment requires some type of a showing that the defendant *intended* to relinquish possession and control of the object in question."). At least one circuit has found that late rent payments and the removal of certain belongings from a dwelling are insufficient to establish an intent to abandon. See United States v. Robinson, 430 F.2d 1141 (6th Cir. 1970) (finding one month's absence, failure to pay rent, and removal of some belongings insufficient evidence to demonstrate intent to abandon); but see United States v. Stevenson, 396 F.3d 538 (4th Cir. 2005) (upholding trial court decision that a tenant who no longer lives on the premises, has verbally expressed an intention to vacate the premises, gives away all personal property within the premises, and abandons the leasehold interest in the property expressed an intent to abandon).

Here, the evidence does not support a finding of unequivocal intent by Crist to abandon the computer. Crist returned to the house on August 10, twenty six days after his rent became overdue. No eviction proceedings had begun. Nor had Crist received notice that his property would be removed. In fact, when the Sells were hired to clean out his house, Crist was in the process of "sorting through things." Tr. 54. He returned to the premises in the midst of the Sells' removal of his belongings and proceeded to search for certain items. His strong reaction to the missing computer and nearly contemporaneous filing of a police report to retrieve his missing

property, demonstrate anything but a "clear and unequivocal" intent to abandon the property. From this evidence, the Court finds that there is insufficient evidence to conclude that Crist intended to abandon his computer.[5]

At argument, the Government argued alternatively that any expectation of privacy that Crist maintained in the property was not objectively reasonable. This Court cannot so find from the evidence presented. Crist's landlord testified that she visited him several times to discuss overdue rent, but never made contact with him. After she visited his residence and heard no barking dog, as was usually the case, she determined to have Crist's belongings removed. She did not notify him of this fact, and Crist was not otherwise placed on notice that his previously exclusive occupancy over the leased premises had ended. On this record, the Court cannot agree that Crist's expectation of privacy was not objectively reasonable.

C. The Private-Search Doctrine

The Government argues alternatively that the warrantless search of Crist's computer was lawful because Crist did not retain a reasonable expectation of privacy in his computer. Because a private party had already searched Crist's hard drive, the Government argues, and the Government's conduct never exceeded the scope of the private search, the search was permissible. In particular, the Government argues that Agent Buckwash never "accessed the computer," but "simply ran hash values on the computer" (2d Supp. Tr. 13-14), which does not constitute a search within the meaning of the Fourth Amendment. Then, once the Government

---

[5] The Government's reliance on an unpublished decision from the United States Court of Appeals for the Sixth Circuit, United States v. Ross, 43 F. App'x 751 (6th Cir. 2002), is misplaced in this case. Aside from being unpublished, Ross is plainly distinguishable. In Ross, the defendant had failed to pay rent for four months and failed to return to his house for three months. Id. at 758.

"compared the hash values of the files that were on the hard drive or the image of the hard drive with hash values of known child pornography" (2d Supp. Tr. 13-14), it knew with "substantial certainty" that the computer contained contraband, and thus, all further searches were justified by the principles of Jacobsen and Runyan.

Crist argues that the hash value analysis was more intrusive than Hipple's search, and thus the Fourth Amendment protects his privacy interest in the computer from warrantless government searches, including the initial forensic examination undertaken by Agent Buckwash. The Fourth Amendment's protection of a warrantless computer search and hash value examination is a novel issue in this Circuit, and as such, requires substantial discussion.

1. Private Searches and the Fourth Amendment

The Fourth Amendment does not apply to private searches or seizures. Burdeau v. McDowell, 256 U.S. 465, 475 (1921) ("[The Fourth Amendment's] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies . . . ."). And if a private party presents law-enforcement authorities with evidence obtained in the course of an unlawful search it is "not incumbent on the police to stop her or avert their eyes," Coolidge v. New Hampshire, 403 U.S. 443, 489 (1971). Similarly, the Supreme Court has "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976); see also Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that

the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."). In all of those circumstances, the Supreme Court held that it is appropriate for the Government to rely upon evidence obtained by a private third party.

In United States v. Jacobsen, 466 U.S. 109 (1984), the Supreme Court confronted a different, but related, issue: whether an individual has a legitimate expectation of privacy when the Government's search goes *beyond* a private search. In Jacobsen and its predecessor, Walter v. United States, 447 U.S. 649 (1980), the Supreme Court affirmed that an individual can retain a legitimate expectation of privacy after a private individual conducts a search, but in Jacobsen the Court clarified that "additional invasions of [an individual's] privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." Jacobsen, 466 U.S. at 115. Since Jacobsen, the Supreme Court has not elaborated on the meaning of this standard. And though other circuits have done so, the Third Circuit has never addressed the private-search doctrine as set forth in Jacobsen. The Fifth Circuit, however, has applied the standard articulated in Jacobsen to searches of computer disks. United States v. Runyan, 275 F.3d 449 (5th Cir. 2001). In Runyan, relied upon by the Government, the Fifth Circuit held that the expectation of privacy in all the files contained on a single computer disk is breached by a private examination of any file on that disk, but the expectation of privacy in other, unmarked disks located near the privately searched disk remains intact. 275 F.3d at 464-65. Based on the principles of Jacobsen and Runyan, the Court finds that the Government exceeded the scope of Hipple's private search when it conducted the forensic examination of Crist's computer and all searches thereafter.

2. United States v. Jacobsen

The Government's argument relies on Jacobsen and the Fifth Circuit's application of Jacobsen to computer disk searches in Runyan. In Jacobsen, two FedEx employees opened a damaged package and discovered crumpled newspapers and a ten-inch, duct-tape tube containing bags of white powder. 466 U.S. at 111. After observing what they suspected to be cocaine, the employees then contacted the Drug Enforcement Administration ("DEA"), replaced the bags inside the tube, and put the tube back into the box. Id. When a DEA agent arrived, he "saw that one end of the tube had been slit open; he removed the four plastic bags from the tube and saw the white powder [and then] opened each of the four bags and removed a trace of the white substance with a knife blade." Id. at 111-12. A field test revealed that the white substance was cocaine. Id. at 112.

The Court found, among other things, that the DEA agent's inspection of the package's contents—and in particular the removal of the bags from the duct-tape tube—did not constitute a search or seizure within the meaning of the Fourth Amendment. The Court, with Justice Stevens writing for the majority, held that "additional invasions of respondents' privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." Id. at 115. According to the Court, "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information." Id. at 117.

Applying that standard to the facts of that case, the Court found that the FedEx employees had eliminated any expectation of privacy in the contents of the package because the DEA agent "knew it contained nothing of significance except a tube containing plastic bags and, ultimately,

white powder." Id. at 118. Significantly, the Court emphasized the limited nature of the search and the limited extent to which that search intruded upon the defendants' expectation of privacy:

> [I]t hardly infringed respondents' privacy for the agents to re-examine the contents of the open package by brushing aside a crumpled newspaper and picking up the tube. The advantage the Government gained thereby was merely avoiding the risk of a flaw in the employees' recollection, rather than in further infringing respondents' privacy. Protecting the risk of misdescription hardly enhances any legitimate privacy interest, and is not protected by the Fourth Amendment.

Id. at 119. In addition, the Court repeatedly returned to the fact that "there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told," to highlight the very limited nature of the additional invasion by the government.[6] Id.

Thus, Jacobsen requires a court to test "additional invasions of respondents' privacy" by law-enforcement officials against the "degree to which [the additional invasions] exceeded the scope of the private search." Id. at 115.

3. United States v. Runyan

In some cases, like Runyan, Jacobsen has easy application, and a court can determine whether the privacy interest is extinguished by defining an object as an additional container. Runyan involved a pre-warrant search of compact disks, ZIP disks, and floppy disks recovered by

---

[6] See id. at 120 ("Similarly, the removal of the plastic bags from the tube and the agent's visual inspection of their contents enabled the agent to learn nothing that had not previously been learned during the private search."); id. at 120 n.17 ("[T]he precise character of the white powder's visibility to the naked eye is far less significant than the facts that the container could no longer support any expectation of privacy, and that it was virtually certain that it contained nothing but contraband."); id. at 121 ("[S]ince it was apparent that the tube and plastic bags contained contraband and little else, this warrantless seizure was reasonable.").

Runyan's ex-wife after she and several of her friends entered Runyan's residence. 275 F.3d 449, 453 (5th Cir. 2001). Though she and a friend had "examined only a randomly selected assortment of the floppy disks and CDs . . . [and none] of the ZIP disks," the government examined all of the CDs and disks provided by Runyan's ex-wife. Id. at 460. Before trial, Runyan moved to suppress the evidence obtained through the government's search on the grounds that it exceeded the scope of the private search. On appeal, the Fifth Circuit considered two separate questions that are relevant to the case *sub judice*: whether the government could search more files on a disk that was previously examined by the private searchers and whether the government could search disks that the private searchers did not examine.

Applying Jacobsen's rule, the Fifth Circuit in Runyan broadly upheld a search of any material on a computer disk if at least one file on that disk had been viewed by a private party. Id. at 465 ("[W]e find that the police do not exceed the scope of a prior private search when they examine particular items within a container that were not examined by the private searchers."). At the same time, the Fifth Circuit rejected a *carte blanche* approach that would have allowed government officers to search an entire group of similar containers when only some of them had been previously viewed by a private party. Id. at 464 ("The mere fact that the disks that [the private parties] did not examine were found in the same location in Runyan's residence as the disks they did examine is insufficient to establish with substantial certainty that all of the storage media in question contained child pornography.").

The two holdings in Runyan hinged on the classification of each disk as one closed container. The "look-see" confirmation that the information on one disk was what the private parties had seen was upheld because it was merely a "more thorough" investigation of what a

private searcher had told the police. In reaching this conclusion, the court considered Jacobsen and other circuit decisions following Jacobsen to derive the following guideline:

> [P]olice exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers unless the police are already substantially certain of what is inside that container based on the statements of the private searchers, their replication of the private search, and their expertise.

Id. at 463.

Applying this standard to the issue of separate disks, the court found that the police could not have known with substantial certainty whether similar information was on separate, unmarked disks because each individual disk was a separate closed container for Fourth Amendment analysis. Therefore, the court determined that it runs afoul of the Fourth Amendment for the police to conduct warrantless searches of computer disks when the privacy interest has not already been breached by a private party. Id. at 465.

4. Forensic Examination of Crist's Computer

The Government urges the Court to expand Runyan further to hold that because the Government had in its possession reliable information that Crist's computer housed several files containing contraband, it was permitted to conduct a warrantless examination of the hard drive. The argument requires this Court to find that the removal and copying of Crist's hard drive, the "running of hash values" of every file on Crist's computer, and the comparison of those hash values to the hash values of known child pornography is less intrusive than a private party's opening "two or more" (Tr. 37) media files. This Court would also need to conclude that once the hash values proved contraband was on the computer, all further searches of the contents of Crist's computer were reasonable because the government was "substantially certain" the

computer contained contraband. The Court cannot embrace the Government's view of Jacobsen and Runyan. The Court finds that the EnCase search exceeded the scope of the private party search, and all further searches were, likewise, unreasonable under the Fourth Amendment.

i. The EnCase Examination Constituted a Search and Exceeded the Scope of the Private Search

The Government argues that no search occurred in running the EnCase program because the agents "didn't look at any files, they simply accessed the computer." 2d Supp. Tr. 16. The Court rejects this view and finds that the "running of hash values" is a search protected by the Fourth Amendment.

Computers are composed of many compartments, among them a "hard drive," which in turn is composed of many "platters," or disks.[7] To derive the hash values of Crist's computer, the Government physically removed the hard drive from the computer, created a duplicate image of the hard drive without physically invading it, and applied the EnCase program to each compartment, disk, file, folder, and bit. 2d Supp. Tr. 18-19. By subjecting the entire computer to a hash value analysis—every file, internet history, picture, and "buddy list" became available for Government review. Such examination constitutes a search.

Moreover, the EnCase analysis is a search different in character from the one conducted by Hipple, and thus it cannot be defended on the grounds that it did not exceed the private party search. As noted above, the rationale for authorizing warrantless searches in Jacobsen is that the private search was so complete, no privacy interest remained. That is certainly not the case here.

---

[7]A platter is defined as "a round plate coated with magnetic material, on which data is stored in a hard drive." Oxford English Dictionary, 2d ed., s.v. "platter." A hard drive is "a high-capacity self-contained storage unit containing a read-write mechanism together with one or more hard disks inside a sealed unit." Id. s.v. "hard drive."

Hipple opened "a couple of videos" (Tr. 12) and deleted them, a far different scenario from the search in Jacobsen, wherein the opening of a package and the testing of its previously examined contents necessarily obviated any expectation of privacy. Here, the Hipple private search represented a discrete intrusion into a vast store of unknown electronic information. While Crist's privacy interest was lost as to the "couple of videos" opened by Hipple, it is no foregone conclusion that his privacy interest was compromised as to all the computer's remaining contents.

Indeed, this conclusion comports with the Runyan court's application of Jacobsen, as well. The Runyan court, too, focused on the remaining privacy interest after an intrusion by a non-governmental party. Comparing a disk containing multiple files to the opened package breached in Jacobsen, the Runyan court found that no privacy interest remained in a disk once some of its contents had been viewed. As to the unopened disks, the court found privacy rights intact, and held unlawful a warrantless search of such disks. Where, as here, substantial privacy rights remained after the private search and the government actors had reason to know that the EnCase program would likely reveal more information than they had learned from Hipple's brief search, the Court finds that the scope of the private search was exceeded.

In so holding, the Court specifically rejects the Government's initial approach asking the Court to compare Crist's entire computer to a single closed container which was breached by the Hipple search. A hard drive is not analogous to an individual disk. Rather, a hard drive is comprised of many platters, or magnetic data storage units, mounted together. Each platter, as opposed to the hard drive in its entirety, is analogous to a single disk as discussed in Runyan. As such, the EnCase search implicates Crist's Fourth Amendment rights.

ii. The Post-EnCase Searches Were Also Protected

After initially running the hash values and discovering five videos of known child pornography, the Government examined the contents of Crist's computer in "gallery view, which gives [them] all the pictures on the computer," and discovered "approximately 1600 images of child pornography or suspected child pornography." Supp. Tr. 95. Assuming arguendo that the EnCase analysis was not a search, the Government justifies this second warrantless intrusion on the basis that the EnCase analysis and Hipple's statements provided "substantial certainty" that contraband existed on Crist's computer, and thus Jacobsen authorizes the search. Under the Government's reading of Jacobsen, the post-EnCase search into the contents of Crist's hard drive is permissible because the intrusion occurred only after police were certain that contraband would be found within. Jacobsen is not nearly so expansive as the Government suggests.

In Jacobsen, the Court explicitly *rejected* the suggestion that "this case is indistinguishable from one in which the police simply learn from a private party that a container contains contraband, seize it from its owner, and conduct a warrantless search[,] which . . . would be unconstitutional." Jacobsen, 466 U.S. 120 n.17. Rather, the Court explained that "the facts that the container could no longer support any expectation of privacy, and *that it was virtually certain that it contained nothing but contraband*," were of controlling significance. Id. at 119 (emphasis added). Thus the Government misinterprets the "substantial certainty" test when it argues that as long as there is substantial certainty that some contraband is in the container, all contents of the container may be searched. The Jacobsen Court flatly refused to "sanction warrantless searches of closed or covered containers or packages whenever probable cause exists as a result of a prior private search," noting instead that a "container *which can support a*

reasonable expectation of privacy may not be searched, even on probable cause, without a warrant." Id. (emphasis added); see also Illinois v. Caballes, 543 U.S. 405, 408 (2005) (interpreting Jacobsen to hold that "any interest in possessing contraband cannot be deemed legitimate, and thus, governmental conduct that only reveals the possession of contraband compromises no legitimate privacy interest.").

This reasoning requires the Court to find that the Government's post-EnCase search of Crist's computer violated the Fourth Amendment. The Government's warrantless search of Crist's computer exceeded the scope of the private search because the Government was not substantially certain the computer contained only contraband. The Government only had substantial certainty that five files on Crist's computer were contraband; Crist's expectation of privacy was not extinguished as to the contents of the thousands of other files unseen by Hipple. Thus, even if the initial EnCase analysis had not violated the Fourth Amendment, the evidence found on Crist's computer must be suppressed because the further search of Crist's computer exceeded the scope of the private search in violation of the Fourth Amendment.

D. Good-Faith Exception to the Fourth Amendment

The Government argues that, even if the searches in question were unreasonable, the Court should nonetheless allow the Government to introduce the evidence obtained in the course of those searches because the "police reasonably and in good faith relied on the appearance that the computer and its contents had been abandoned." (Doc. No. 41, at 14-15.) In this case, however, the Court finds that no good-faith exception applies.

In United States v. Leon, 468 U.S. 897 (1984), the Supreme Court determined that suppression of evidence is not an appropriate remedy when a police officer executes a search on

an objectively reasonable belief that a warrant issued by a neutral, detached magistrate was valid, though the warrant was later found to be invalid. Id. Following Leon, the Third Circuit has held that "[t]he test for whether the good faith exception applies is 'whether a reasonably well trained officer would have known that the search was illegal despite the magistrate judge's authorization.'" United States v. Hodge, 246 F.3d 301, 307 (3d Cir. 2001).

The Supreme Court has applied the good-faith exception to warrantless searches. In Illinois v. Krull, 480 U.S. 340, 346 (1987), the Supreme Court found that a "good-faith exception to the Fourth Amendment exclusionary rule applies when an officer's reliance on the constitutionality of a statute is objectively reasonable, but the statute is subsequently declared unconstitutional." Id. More recently, in Arizona v. Evans, 514 U.S. 1, 14 (1995), the Supreme Court found that a good-faith exception to the exclusionary rule would apply where an officer's reliance on a computer record of an arrest warrant was objectively reasonable, though no warrant had actually been issued, if the error was the result of a clerical error of court employees. Id.

Significantly, though, neither the Supreme Court nor the Third Circuit has ever extended the good-faith exception to the exclusionary rule "beyond circumstances where an officer has relied in good faith on a *mistake made by someone other than the police*; that is, on someone outside the police officer's 'often competitive enterprise of ferreting out crime.'" United States v. Herrera, 444 F.3d 1238, 1251-52 (10th Cir. 2006) (quoting Leon, 468 U.S. at 914 (emphasis added)). Indeed, as the United States Court of Appeals for the Tenth Circuit has explained, "because the purpose underlying this good-faith exception is to deter *police* conduct, logically Leon's exception most frequently applies where the mistake was made by someone other than the officer executing the search that violated the Fourth Amendment." Id.

The limited circumstances of the good-faith exception do not apply in this case. At no point did the officers seek out a warrant from a detached, neutral magistrate. When the officers searched Crist's computer, even if they acted in good faith,[8] they did not rely in good faith on the conduct of a neutral third-party that was later determined to be a mistake. The Third Circuit has said that "[g]ood faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." United States v. Zimmerman, 277 F.3d 426, 438 (3d Cir. 2002) (quoting United States v. Reilly, 76 F.3d 1271, 1280 (2d Cir. 1996)). In a case such as this, where the police officers were the source of their own trouble, the good-faith exception does not apply.[9]

E. Remedy

Finally, even though the Court concludes that no good-faith exception applies in this case, the Court will consider whether suppression is an appropriate remedy in light of Hudson v. Michigan, 547 U.S. 586 (2006). In Hudson, the Supreme Court held that suppression is not available as a remedy for evidence uncovered subsequent to a violation of the knock-and-announce rule. The knock-and-announce rule, which is codified at 18 U.S.C. § 3109, requires police, in executing a warrant granting entry to a dwelling, "to signify the cause of [their] coming, and to make request to open [the] doors . . . ." Semayne's Case, (1604) 5 Co. Rep. 91a, 91b, 77 Eng. Rep. 194, 195 (K.B.).

---

[8] The Court declines at this point to determine whether it was objectively reasonable for the officers to conclude that Crist's computer had been abandoned.

[9] Incidentally, the Pennsylvania Supreme Court does not recognize any good-faith exception to the exclusionary rule under the Pennsylvania Constitution. Commonwealth v. Edmunds, 586 A.2d 887, 906 (Pa. 1991).

It is unclear whether the Supreme Court intended the exception to the exclusionary rule articulated in Hudson to apply narrowly to knock-and-announce violations or more broadly to all searches governed by the Fourth Amendment. Though the lower courts are not in agreement on the matter,[10] the Court ultimately finds that the exclusionary rule should apply. In considering whether to suppress, this Court is guided by the Third Circuit's decision in United States v. Mosley, 454 F.3d 249, 269 (3d Cir. 2006), which stated that "[t]he exclusionary rule is a judge-made remedy designed to deter illegal police conduct . . . [D]ecisions about [] the application of the rule are pragmatic decisions requiring practical wisdom rather than syllogisms." Id. In making this decision, the court must

> look not only to the logical relationship between the violation and the discovery of the evidence, but also to the nature of the personal and social interests the Constitution protects, the prevalence of the illegal police practice at issue, the deterrent value of the suppression remedy, and the likely practical effects of a particular rule.

Id. at 268 (citing Hudson). While exclusion may be inappropriate when police fail to wait a few seconds before breaking down the door of a house to execute a valid warrant, the instant case is quite different. Here, the core of the Fourth Amendment is implicated—the officers, without exigency and without authorization conducted an unbounded, warrantless search of a person's computer, despite the fact that a warrant could easily be obtained.

In sum, the Court finds that the evidence obtained through the forensic examination of the computer must be suppressed.

---

[10] Compare, e.g., United States v. Jones, 523 F.3d 31, 36 (1st Cir. 2008) (Hudson limited to knock-and-announce violations), and United States v. Cos, 498 F.3d 1115, 1132 n.3 (10th Cir. 2007) (same), with United States v. Cazera-Olivas, 515 F.3d 726, 729 (7th Cir. 2008) (extending Hudson to case where no warrant was issued "because had the procedures of [Federal Rule of Criminal Procedure] 41 been followed, the agents would have obtained a valid warrant").

III. SUPPRESSION OF STATEMENTS

Crist also seeks to suppress any statements elicited from him during the interview at his home in January 2007. Crist correctly acknowledges that the Fifth Amendment protections afforded by Miranda v. Arizona, 384 U.S. 436, 479 (1966), do not apply in this case because he was not in custody. He further acknowledges that the Sixth Amendment right to counsel had not attached during the interview because adversarial proceedings had not commenced. McNeil v. Wisconsin, 501 U.S. 171, 175 (1991). Nonetheless, he argues that his statement was not "the product of a rational intellect and a free will," Townsend v. Sain, 372 U.S. 293, 307 (1963) (quoting Blackburn v. Alabama, 361 U.S. 199, 208 (1960)), and is therefore inadmissible under the due process protections of the Fifth and Fourteenth Amendments. In particular, Crist argues that his admissions were made involuntarily because he "was confronted by three law enforcement officers, accused of a crime, and advised that he should confess," and because when "he requested an opportunity to consult with counsel[,] . . . this request was ignored." (Doc. No. 31, at 9.)

The determination of whether a confession is voluntary is based upon the "totality of circumstances." Arizona v. Fulminante, 499 U.S. 279, 285-89 (1991). As the Third Circuit has explained in United States v. Swint, 15 F.3d 286, 288 (3d Cir. 1994), the totality of the circumstances analysis includes:

> not only the crucial element of police coercion, the length of the interrogation, its location, its continuity, the defendant's maturity, education, physical condition, and mental health[, but also] . . . the failure of police to advise the defendant of his rights to remain silent and to have counsel present during custodial interrogation.

Id. at 288-89. Here, as the Government notes, Crist is a middle-aged man with prior experience in the criminal justice system, with a personal and employment history indicating a modest amount of education, who spoke for a period of a few hours with three agents whom he invited into his home. No threats, coercion, or force was involved. Though it would certainly be natural for Crist to be uncomfortable, his expressed belief that he should speak with an attorney does not suggest that his admissions were made involuntarily. Rather, the Court finds that, based on the totality of the circumstances, Crist's statements were made knowingly, intelligently, and voluntarily.

Accordingly, the Court will deny Crist's request to suppress the statements made during the January 2007 interview in his house.

V. CONCLUSION

For the foregoing reasons, the Court will grant in part and deny in part Crist's motion to suppress evidence. The Court will suppress that evidence recovered from Crist's computer through the forensic examination conducted by the Pennsylvania Attorney General's Office but will deny Crist's motion in all other respects. An appropriate order follows.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
	:	**Criminal Action No. 1:07-cr-211**
v.	**:**	
	:	**(Chief Judge Kane)**
ROBERT ELLSWORTH CRIST, III	**:**	
Defendant	**:**	

ORDER

AND NOW, on this 22nd day of October 2008, for the reasons set forth in the accompanying memorandum, **IT IS HEREBY ORDERED THAT** Defendant's motion to suppress is **GRANTED** in part as follows:

1. All evidence obtained from the forensic search of Crist's computer is **SUPPRESSED**.

2. In all other respects, Defendant's motion is **DENIED**.

S/ *Yvette Kane*
Yvette Kane, Chief Judge
United States District Court
Middle District of Pennsylvania