United States District Court
Northern District of Florida
PENSACOLA DIVISION

UNITED STATES OF AMERICA

WARRANT FOR ARREST

v.

**DANIEL CASTLEMAN**

CASE NUMBER: 3:08mj 23

5:08-mj-027

TO: The United States Marshal
    and any Authorized United States Officer

YOU ARE HEREBY COMMANDED to arrest DANIEL CASTLEMAN

and bring him or her forthwith to the nearest magistrate to answer a(n)

☐ Indictment ☐ Information ☒ Complaint ☐ Violation Notice ☐ Probation Violation Petition

charging him or her with engaging in a child exploitation enterprise and conspiring to advertise, transport, ship and receive child pornography in violation of Title 18, United States Code, Section(s) 2252A(g) and 2252A(a)(1) and (2).
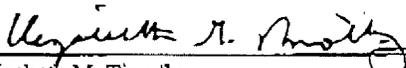
Elizabeth M. Timothy
United States Magistrate Judge

2-29-08
Date

@ Pensacola, FL
Location

Bail Fixed at $_____ by _____ - E.Timothy
                         Name of Judicial Officer

RETURN

This warrant was received and executed with the arrest of the above-named defendant at : _____

Date Receive	Name and Title of Arresting	Signature of Arresting Officer
Date of Arrest		

AO (Rev. 5/85) Criminal Complaint

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION

UNITED STATES OF AMERICA

vs.

DANIEL CASTLEMAN

CRIMINAL COMPLAINT

CASE NUMBER: 3·08ᴍᵢ 23

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief. From on or about August 31, 2006, in Walton County, in the Northern District of Florida, and elsewhere, defendant(s) did, engage in a child exploitation enterprise and conspire to advertise, transport, ship and receive child pornography in violation of Title 18, United States Code, Section(s) 2252A(g) and 2252A(a)(1) and (2). I further state that I am a(n) Special Agent with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Signature of Complainant
Robert Cochran

Sworn to before me and subscribed in my presence,

February 29, 2008   at   Pensacola, Florida.
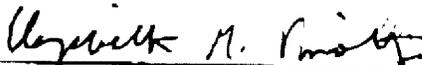
Elizabeth M. Timothy
U.S. Magistrate Judge

CERTIFIED A TRUE COPY
WILLIAM M. McCOOL, Clerk
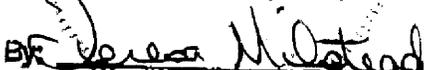
BY: _____
Deputy Clerk

FILED February 29, 2008
(Date)
NORTHERN DISTRICT OF FLORIDA
U.S. MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF FLORIDA

AFFIDAVIT

I, Robert R. Cochran, being duly sworn, depose and say that I am a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

BACKGROUND OF AFFIANT

1.   I am a Special Agent for the FBI and have been so since 2002. I am currently assigned to The Jacksonville Division, Pensacola Resident Agency. As such, I am currently assigned to investigations relating to crimes against children, including the trafficking and possession of child pornography.

2.   I have received specialized training in the investigation of child pornography and the sexual exploitation of children. I have observed and reviewed numerous examples of child pornography in various media formats, including computer-based formats. I have received particularized training in the investigation of computer-related crimes, Usenet, peer-to-peer computer networking, and online (i.e. Internet based) crimes against children.

3.   As a federal agent, I am authorized to investigate the violation of United States law and have the authority to arrest individuals under the authority of the United States.

FACTS AND CIRCUMSTANCES

4.   The statements in this affidavit are based in part on information provided by other

1

Special Agents of the FBI, other law enforcement officers, and on my own investigation, experience, training and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that criminal violations of Title 18, United States Code, §§ 2252A(a)(1), 2252A(a)(2), and 2252A(g) have taken place.

STATUTORY AUTHORITY

5.   This investigation concerns alleged violations of Title 18 U.S.C. § 2252A, relating to the sexual exploitation of minors. Title 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer. Title 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer. Title 18 U.S.C. § 2252A(g) prohibits a person from engaging in a child exploitation enterprise where the enterprise is a part of a series of felony violations constituting three or more separate incidents and involving more than one victim and the offense is committed in concert with three or more other persons.

DEFINITIONS

6.   The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a.   "Child Pornography," is defined in Title 18 U.S.C. § 2256(8) as any visual

2

depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct, as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct.

b.   Title 18 U.S.C. § 2256(5) states: "visual depiction' includes undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image."

c.   Title 18 U.S.C. § 2256(2) defines "sexually explicit conduct" as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See Title 18 U.S.C. § 2256(2).

d.   "Computer," as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e.   "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, digital, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, compact disks, flash/thumb drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f.   "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g.   "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h.   "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming

4

code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices or to access/open files resident on a computer. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which preform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i.   The "Internet" is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone, cable, fiber optic, wireless and satellite communications for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet frequently crosses state and international borders, even if those computers are in the same state. A network is a series of devices, including computers, servers, and telecommunication devices, connected by communication channels.

j.   An Internet Service Provider (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines/cables, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP such as Usenet (newsgroups) and chat/messaging functions. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and

billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, customer service information and other information, both in computer data format and in written record format.

k.   A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients."

l.   "Usenet" is a service on the Internet which utilizes a network of computers to facilitate the posting of messages, also referred to as articles, in public virtual locations known as "newsgroups." Usenet began as a simple discussion forum for exchanging text messages, but has grown into a hugely distributed file sharing network where software, music, pictures, and videos can be easily traded and shared. These files are posted and retrieved from newsgroups by attaching them to newsgroup messages/articles. Usenet hosts more than 150,000 newsgroups that are organized by topic. To use this service, an individual must use a client application (software), commonly referred to as a news reader, to post and/or read messages to/from a Usenet server. Through the Internet, the server then passes the message on to other servers until it has been replicated or propagated on Usenet servers worldwide. Other individuals can then download the message by accessing their respective Usenet server via their personal (client) computers. To participate in a newsgroup, an individual must either access a Usenet server operated by their ISP, or subscribe to a separate

6

Usenet service, commonly referred to as a News Service Provider (NSP), which is typically a commercial entity or organization that provides Usenet news as its primary or sole activity.

  m. Newsgroups follow a particular naming convention which provides the user with an idea of what type of group, or what type of material or discussion a person would expect to find in that specific newsgroup location. Many Usenet newsgroups have a branch from the root alt. category (i.e. alt.binaries) where hundreds of newsgroups exist that are solely for the purpose of transferring binary files, rather than readable text messages. Newsgroups are categorized by one of approximately eight different Usenet categories:

   Alt.* = alternative material

   Misc.* = misc. topics (e.g. education, items for sale, etc.)

   News.* = discussions about news material

   Rec.* = recreation and entertainment topics

   Sci.* = science related topics

   Soc.* = social issues and topics

   Rel.* = religious related topics

   Humanities.* = fine arts, literature and philosophy

  n. An example of the newsgroup "alt.binaries.pictures.erotica.pre-teen" would breakdown as follows:

   "alt" ... "alternative" - not yet formally accepted material.

   "binaries" ... a file of some kind: image, sound, program, etc. (typically

means 'not just text').

"erotica" and "pre-teen" ... more than likely discusses or depicts images of erotic or pre-teen material.

o.   There are generally two types of files uploaded to newsgroup locations: text or binary. A text file is just that, it includes readable words (i.e. a message/article). A binary file is comprised of digits rather than text, and can be a music file, picture/video file, a software program, etc.

p.   A newsgroup message is preceded by header lines which contain specific or unique information associated with that particular posting. Through the use of this header information, it is possible to identify an individual that posted the newsgroup message. The header contains at least the following header lines:

"From" - contains the electronic mail address and/or a self created nickname of the person who sent the message;

"Date" - the date and time stamp when the message was originally posted to the network;

"Subject" - a short summary of the content of the message to enable a reader to make a decision based on the subject whether to read the message;

"Message ID" - the message's unique identifier. To ensure the uniqueness of the Message ID, it may not be reused during the lifetime of the message;

"Path" - the network path the message took to reach the current system.

When a system forwards the message, it should add its own name to the list of systems in the "Path" line.

q.   Computers connected to the Internet are identified by addresses. Internet addresses take on several forms, including Internet Protocol(IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique for a particular date, time, timezone, and can be traced to an identifiable physical location and possibly a specific computer. The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.187). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address, it enables Internet sites to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs. There are two types of IP addresses, dynamic and static. To assign dynamic IP addresses, the ISP randomly assigns one of the available IP addresses, in the range of IP addresses controlled by the ISP, each time a customer dials in or connects to the ISP in order to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, that IP address becomes available to other customers who dial in at a later time. Thus, an individual

9

customer's dynamic IP address may, and almost always will, differ each time he dials into or connects to the ISP. To assign static IP addresses, the ISP assigns the customer a permanent IP address. The customer's computer would then be configured with this IP address every time he dials in or connects to the ISP in order to connect to the Internet.

r.   Some numerical IP addresses may have corresponding domain names. For instance, the IP address 149.101.1.42 traces to the corresponding domain name "www.cybercrime.gov." The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

s.   The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CDs, DVDs, flash/thumb drives, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic

storage device).

t.   Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

u.   The term "encryption" is the translation of data into a cipher (i.e. secret code). It is the process of transforming information (referred to as plain text) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a "key." In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption," like software know as Pretty Good Encryption (PGP), can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted). Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key, password or pass phrase that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption (also called single-key or one-key encryption). The public-key method requires both a "Public-key" and "Private-key" combination (two

different and separate keys) to decode data. The symmetric-key method typically uses the same key to both encrypt and decrypt the file/data.

    v.   There are a number of commercial services and software programs available to assist computer users who want anonymity while using the Internet, whether it be for the purpose of accessing/viewing websites, sending email messages, or posting Usenet (newsgroup) messages or files. Below are some of the more common terms and services associated with anonymity on the Internet:

    Anonymizers/proxy servers: a proxy server functions as a relay between the user and the destination site, hiding the user's IP address. The user's Internet traffic is routed from the user's computer, to a proxy server (computer), which then drops all identifying information and the IP address, and then forwards the Internet traffic to its actual/intended destination.

    Remailer: an address through which an electronic message passes before continuing to its actual/intended destination. It is a computer that uses a program to forward mail from the user's computer through several other computers to the final destination. Each computer strips (wipes) out identifying information from the header which can disclose the users identity, and sends the message along without revealing where it originally came from.

    TOR: a network of virtual tunnels that allow users and groups to improve their privacy and security on the Internet. It is a program AND network of

freestanding computers that act as a three chain anonymous encrypted proxy. Everything is encrypted from the user's computer to the last computer. All user communications are bounced around a distributed network of relays run by volunteers (computer nodes) located around the world. Generally speaking, a user's communication travels through three other participating user computers (nodes), before being sent to its final destination.

BACKGROUND OF THE INVESTIGATION

7.   During June 2006, representatives from the Queensland Police Service, Brisbane, Australia, informed members of the FBI's Innocent Images Unit of an international child pornography investigation regarding numerous subjects residing in various countries. Investigation to date indicates that a number of individuals (i.e. members) participating in this enterprise are located in the United States. The investigation involves a sophisticated and extremely organized group, hereafter referred to as "enterprise," of Internet Usenet users involved in the prolific trade/distribution of child pornography. The enterprise employs highly technical and advanced security measures to avoid law enforcement detection. Such techniques include, but are not limited to, the use of Pretty Good Encryption (PGP) software to encrypt messages posted to the enterprise's pre-designated newsgroup location where members communicate with each other, PGP encryption of binary files (which generally contain child pornographic material) uploaded to other newsgroup locations, and the swapping of file extensions which subsequently must be re-swapped in order to successfully

13

download a particular picture or movie file.

8.   This investigation is predicated on information obtained from an individual who has been charged criminally in an unrelated child pornography investigation. This individual informed law enforcement that he/she was a member of this enterprise and identified a newsgroup titled "alt.anonymous.message" as the location at that time where members of the enterprise conducted/uploaded text [message] postings to communicate with each other. It is noted that since the time that the above referenced information was provided by the cooperating individual, the newsgroup location has changed several times. At this particular newsgroup location, members inform each other as to the newsgroup location (i.e. a different location) of where they have uploaded child pornography for members to go to download for their own personal collections. The child pornography binary files, either still pictures or video files, are never uploaded (i.e. distribution/transportation) to the newsgroup reserved for text [message] communications between members. Rather, the child pornography is uploaded to other innocuous newsgroup locations where members must go to retrieve/download the material. Specific directions are posted in the enterprise's newsgroup location, such as passwords, to ensure the successful retrieval/download of the image and/or video files.

9.   The subject of the aforementioned investigation provided investigators with his/her PGP encryption keys which have allowed law enforcement to access, decrypt and monitor all activity/postings associated with the enterprise. Basically, law enforcement has infiltrated

14

the enterprise. To date, investigators have collected extremely valuable and incriminating evidence from various members of the enterprise. Since the initial monitoring of the newsgroups, approximately 403,442 images and 1,128 video files have been advertised, distributed and/or received by the enterprise (period of 08/31/2006 through 12/15/2007).

10.   The enterprise currently consists of approximately 45 active members. There is a defined hierarchy or structure to the enterprise and all members must abide by strictly enforced written security measures and standard operating procedures in order to retain their membership status. To become a member of the enterprise, one must be invited in by an existing member, he/she must be known to trade child pornography material (i.e. demonstrated by being involved in other newsgroups involved in this activity), and must pass a timed written test to determine their knowledge of child pornographic material (e.g. knowledge of the names of various child pornography series; must be able to describe a particular series in question, etc.). The test also serves as a measure to assess whether the interested party could be an undercover law enforcement officer attempting to infiltrate the enterprise. Members of the enterprise are told never to provide their true identities to another member of the enterprise. They are never to communicate with one another using traditional email, chat, Yahoo!, ICQ, or telephone. For the security of the enterprise as a whole, their relationship with other members of the enterprise is strictly via the Internet. In this manner, if one of the members of the enterprise is ever arrested by law enforcement, that member cannot provide any identifying information to law enforcement on other members of the

enterprise.

11.   The enterprise has developed outside contacts in the child pornography industry whereby they have made specific requests for the production of new child pornography material.   In several instances, it appears the enterprise has been able to order new (unreleased) child pornography movies produced solely for the benefit of the enterprise (i.e. material which had not been distributed to the public in other child pornography forums). In addition, the enterprise has established an E-gold account, funded by the members, in order to purchase newly released child pornography material from various international producers.

12.   As indicated above, the enterprise periodically moves from one newsgroup location to another where they conduct their primary text [chat] message communications with each other.   This is done primarily for two reasons: 1) as a general principle to avoid law enforcement detection, and/or 2) because someone in the group made a mistake, violating the enterprise's written security procedures (e.g. failure to encrypt a message/posting, thus making it readily available for anyone to access and read), which would jeopardize the security of the group. Each time the enterprise moves from one newsgroup location to another, they also change all of their PGP encryption keys so there is no trail from one newsgroup location to the next location. Additionally, each time the enterprise moves, all of the members change their nicknames. For the most part, the selection of new nicknames is based on a particular theme that the leader of the group established for all of the members

16

to use/follow. For example, during one of the enterprise moves from one newsgroup location to another, the group adopted a theme related to cars (motor vehicles). As such, each of the members created a new nickname based on this theme (e.g. Thunderbird, Jaguar, Fender, Big Block, etc.). During a recent move from one newsgroup location to the current newsgroup location, all PGP encryption keys and nicknames changed; however, it was decided the theme would revert back to the previously used "Japanese" theme. In summary, the following chart depicts information or intelligence obtained during this investigation relating to newsgroup locations, themes, and nicknames associated with each of the subjects of this investigation:

Original Nickname	alt.anonymous.email / Car Theme / Time frame Unknown - unknown	alt.anonymous.message / Cooking Theme / 12/02/08-12/01/08	alt.lpl.mp3.encrypted / Music Theme / 12/02/06-01/19/07	alt.anonmail.net.messages / (no theme) / 01/20/07-03/16/07	japan.security.pgp / Japanese Theme / 03/17/07-09/07/07	alt.os.security / (no theme) / 09/08/07-01/06/08	japan.security.pgp / Japanese Theme / 01/07/08-present
Yardbird	Thunderbird	Gyro	Musik	Asterisk	Arigato	White Hat	Kishi Kasei
Helen	Jaguar	Menge Toute	Pan	Spock	Honda	Thor	Wong
Nimo	64GTO	Chardonnay	Myers	Morticia	akon	Bugs	Duc Chow
Plike	BMW 330csi	Steakhouse	Steppenwolf	Sasamie	Shinkansen	Autoselect	Bandari-Dancer
Screwtape	Scorpion	Magimix	John Brewer	Maggie the Mog	Shun	Headstrong	Kai Lung
Sally	Herbie	The Naked Chef	PunkGrrrl	Padrone	Hanoi Jane	Kiwa	Chairman Mao
Argus	Armstrong Siddeley	Eggs Benedict	Salieri	Achilleus	DimSim	SnakeCharmer	Origami
F'lar	Firebird						
Mr E	Stealth	Cordon Bleu				Pcchips	Ramen
Crazy Horse	Big Block	Short Order	Morgan Roth	Brett Reynolds	Bayahusa	Mister Mix	Sumo Hibachi
Proteus		ravioli	Oscar	DXO	Chi		
Sure	MGB	Della	Dazed	Robin	Kenjogo	Slartibartfast	Ming
Lerch	Nomad	Julia Child	Nic	Rook	yen	pippi	Eri
Toddler		Thyme	Hexagon	Perpendicular		Pampers	Messenger
Lizzard	Henry J	Waffles	Garfield	Pooch	Wakizashi	Six Pax	Dong Hu
Okuna	ElDorado	Tiramisu	Heepman	Hummingbird	Okinawasan	Gentle Giant	Saiya
Fletcher Rabbit	Spyder	Fondue	Strauss				
Earch	Escort	La Zucca	Makaymluk	Orits	Shiral	Room	
Nym	Thesis	Vinaigrette					
Chingachgook	Yugo	Sage	Red Benson	Cheesehead	Jummi		
Electron	Carrara	Grilled Lobster	Mr Swing	Broadway	Fuji	C@T.biz	Mandarin
Jol	Bentley	Truffles	Roadie	rock-n-rye	Kirishima	Omega	
Tex (Mavrick)	NisaanZ	Bill Granger	Economy	white widow	Nikkei	Insect	Chairman

17

Bebop	Probe	Epicurean	Husky	Norris	Lemon GumBall	BlueApple	Kage Zong Yin
Moe Szyslak	DeLorean	Burgermeister	Master P				
Pickleman	Model T	The Galloping Gourmet	Ozzy	The Phantom	Chop Suey	Magilla	Rickshaw
Dream Catcher	Diamante	Dill Weed	Dry Cell	Dabney	Dao Chen		
Papano Eggplant		Pudding	Puck	slim	Okiko	Abe	Hy
Muad'Dib	Vega	Crème Brulee	Hard Rock	Blaise	Dien	Analytiker	Yamoto
Paito	Boss442	Chef Jacques Pepin	Easy Rider	Clark	Zorbak	Athlon64	Sakki
The Clerk	Morris	CurryWurst	Tangerine Dream	Interceptor	Toyota	mb@ thebunker	Sallythe4th
Newnew			diskman	akai	shloko	gforce	
Bumhead	Kamatsu	Sashimi	Scott	Telkontar R.T.	Musashi		
xxxxx							
Gine orw5	Toyota	Umami	Mo	adi	Yamada Odo	Ufo	alf
Archiver		Bon appetit					
Tweety	Mini Minor				Sayuri	K9	
Soft	Cuda	Hot Pepper	Lovesick	Trip	Wii	Like that	Cass
Blackhawk42		Watermelon Wine					
Yellowhead	CarWasher	Vegetarian	Drum	Tramp	Komodo	DaBit	Sumiko
RoadKill	Hudson Hornet	Grilled Cheese	Anonymous	anonymous		Anonymous	Low Fat
Wonka	Beetle						
Box of Rocks	Safrane	Artery-clogger	Cartman	Suslik	Haneko	Volsh	Monorail Cat
Mystikal	VanquishS	Fanny Farmer	Rastaman	Brickhouse	Sakura	Gunter	Puan
Spyder							
Shella	Fender	Tournedos	Sibelius	House	Kensie	Eastern	Sapporo
Sparky							
Unforgiven							
SweetLeaf							
Vermon							
Ptluver							
Methuselah		Chocoholic	Grumpy	Von Dutch	Furumekashii	Reboot	Pegasasu
Wraith		Peaches	Metalhead	xender	Fallen	Jolly Roger	Chihiru
Hellhammer		RachelRay@ FHM.com	RaginCajun				
Caratucus			Malechai	Horus	Mikado	Jeepers	Anvil
PoTuS				Mr.Vitamin B12	Bushido	RunningMan	
silvershadow					Kemsi	twenty	Ashima
Zorro					Mata Hari		
buc						Alpha Tek	Yoshifumi
Eurydice						Perce P Cassidy	The Hermit

SPECIFIC SUBJECT LOCATION INFORMATION

13.   Daniel Castleman has been identified as a subject in this investigation. As further

described below, he is directly associated with the following nicknames used by him to communicate with other members of the child exploitation enterprise: "Chingachgook," a.k.a. "Yugo," a.k.a. "Sage," a.k.a. "Red Benson," a.k.a. "Cheesehead," a.k.a. "Jummi."

14. On or about February 28, 2006, an individual utilizing the nickname "Yugo" (Daniel Castleman) posted a message with the subject line "Mail to those who like automobiles," in the newsgroup *alt.anonymous.email*, and encrypted with the PGP keys utilized by members of the child exploitation enterprise. In the message, "Yugo" stated in part "First, I would like to thank all of you that have posted. You all have done a wonderful job. I recently suffered an injury to my person, no I'm not going to say whether it's medical or physical injury. I don't want to say for security reasons. Anyway, I have been out of commission for a couple/several months now. I have barely been able to keep up do to my condition. I don't tell all of you this for sympathy, but as a way to apologize for all of my requests. I'm not fully recovered, in fact, with the probability of more surgery and other medical care. So, please forgive me if I request more reposts in the future. The body may wither, but the pedo drive never dies."

15. On or about February 28, 2006, "Yugo" (Daniel Castleman) posted a message with the subject line "Re: Purple Neons," in the newsgroup *alt.anonymous.email*, and encrypted with the PGP keys utilized by members of the child exploitation enterprise. In the message, "Yugo" responded to a prior posting from another member of the enterprise regarding a video which was uploaded for the group referred to as "YoungVideoModels

Daphne-3." "Yugo" stated "Thanks for the Daphne 3 vid. Beautiful girl. The only thing

that would make this vid better; is having my face between her legs, etc., etc.

aaaahhhhhh!!!!! Take care and stay safe, Chingachgook aka Yugo." This posting reflects

"Yugo's" receipt of child exploitation material.

16.   On or about September 5, 2006, an individual utilizing the nickname "Sage"

(Daniel Castleman) posted a message with the subject line "Re: Mushroom Puffs," in the

newsgroup *alt.anonymous.message*, and encrypted with the PGP keys utilized by

members of the child exploitation enterprise. In the message, "Sage" responded to a prior

posting from another member of the enterprise regarding material which was uploaded for

the group. "Sage" stated "Nice, very nice. I'm glad I covered my keyboard with plastic

wrap before viewing the pics and vids. I think I have a new daughter in my fantasies.

Thanks again. Walk in peace, Sage." This posting reflects "Sage's" receipt of child

exploitation material.

17.   On or about March 10, 2007, an individual utilizing the nickname "Cheesehead"

(Daniel Castleman) posted a message with the subject line "Re: Gulf of Tonkin

Incident," in the newsgroup *alt.anonmailnet.messages*, and encrypted with the PGP keys

utilized by members of the child exploitation enterprise. In the message, "Cheesehead"

provided information regarding the download, decryption, and re-assembly of files

located in the newsgroups *alt.binaries.test.yenc* (a.b.t.yenc).

18.   On or about March 10, 2007, an individual utilizing the nickname

"Leonidas@Thermapolaye.gr (Leonidas)" (Daniel Castleman) posted a message with the subject line "Leonitus Nepetifolia" in the newsgroup *alt.binaries.test.yenc*, and encrypted with the PGP keys utilized by members of the child exploitation enterprise (this is the binary posting directly associated with the above text posting "Re: Gulf of Tonkin Incident").

19.   On or about March 14, 2007, a task force officer (TFO), acting in a covert capacity, downloaded the files identified by "Cheesehead" (Daniel Castleman) in his posting on March 10, 2007, from the newsgroup *alt.anonmailnet.messages*. Utilizing the instructions provided by "Cheesehead" and the group encryption keys, the TFO was able to successfully decrypt and re-assemble the files.

20.   A review of the re-constructed folders and associated files showed that they contained 3 video files with a combined size of approximately 1.3 GB, and 7 photo collages (i.e. numerous thumbnail images) with a combined size of approximately 1.99 MB. A review of the videos and images revealed the following depictions of child pornography:

Lolita Collection Vol 03.avi
A video (with audio - music only) (approximately 45 minutes 28 seconds) depicting a nude prepubescent female and a nude prepubescent male engaged in various sexual acts to include oral sex and sexual intercourse.

Lolita Collection Vol 05.mpg
A video (with audio - music only) (approximately 46 minutes 18 seconds) depicting two nude prepubescent females engaged in sexual acts utilizing vibrators. Also depicted in the video is a nude prepubescent male engaged in various sexual acts with a nude prepubescent female to include the use of a

vibrator, oral sex and sexual intercourse.

Lolita Collection Vol 06.mpg
A video (with audio - music only) (approximately 48 minutes 28 seconds) depicting a nude prepubescent female taking a shower. The video also depicts a nude prepubescent female and a nude prepubescent male engaged in oral sex.

The following 7 collages appear to be thumbnail snap shots extracted from the

aforementioned Lolita Collection videos; however, the only video included in this

newsgroup posting, as listed above, were Volumes 3, 5 and 6.

> Lolita Collection Vol 1.jpg
> Lolita Collection Vol 2.jpg
> Lolita Collection Vol 3.jpg
> Lolita Collection Vol 4.jpg
> Lolita Collection Vol 5.jpg
> Lolita Collection Vol 6.jpg
> Lolita Collection Vol 7.jpg

21.   On March 19, 2007, an administrative subpoena (IINI 1522) was served on

Usenetserver/UNS LLC, Abuse Department, 807 W. Morse Boulevard, Suite 101, Winter

Park, FL 32789, for user account information related to the above listed posting dated

March 10, 2007, subject line "Leonitus Nepetifolia," message identification

7Uulh.22745$r73.10103@fe24.usenetserver.com.

22.   On March 20, 2007, Usenetserver/UNS LLC, in response to the administrative

subpoena (IINI 1522) served on March 19, 2007, identified the account utilized to post

message identification 7Uulh.22745$r73.10103@fe24.usenetserver.com as being owned

by the following individual:

Username: bluegrasswater
Name: Peter Short
Address: 315 Wall Street
                                     Midland, TX 79706
Telephone: 915-658-5246
Electronic mail (e-mail):   bluegrasssmith@care2.com
Account status: Active

According to Usenetserver, the last known IP address used by bluegrasswater was

as follows:

IP address: 68.1.238.104
Date: February 14, 2007
Time: 14:34:46 Central Standard Time
Associated message ID: Xns98D78A28E3DDBOpenTest@208.49.80.60
Posted to (group):   alt.binaries.cleannews.test

23.   A check conducted via www.arin.net indicated IP addresses 68.1.238.104 was

assigned to Cox Communications, 1400 Lake Hearn Drive, Atlanta, GA 30319, business

telephone number 404-269-0100, business facsimile number 404-269-1898.

24.   On March 30, 2007, an administrative subpoena (IINI 1624) was served on Cox

Communications, 1400 Lake Hearn Drive, Atlanta, GA 30319, for information related to

IP address 68.1.238.104 assigned on February 14, 2007, 14:34:46 CST (derived from

results of IINI 1522).

25.   On April 3, 2007, Cox Communications, in response to the administrative

subpoena (IINI 1624) served on March 30, 2007, partially identified the account assigned

IP address 68.1.238.104 assigned on February 14, 2007, 14:34:46 CST (derived from

results of IINI 1522). Cox Communications advised the IP address represents a customer

from a cable system located in West Texas that was sold to the company Suddenlink

Communications.

Electronic mail (e-mail):	daniel.castleman
	wildman334
Telephone:	806-791-7668

26.   On April 25, 2007, an administrative subpoena (IINI 1760) was served on

Suddenlink Communications, 12444 Powerscourt Drive, Suite 140, St. Louis, MO 63131,

for information related to the following possible e-mail addresses:

daniel.castleman@cox.net
daniel.castleman@suddenlink.net
daniel.castleman@suddenlink.com
wildman334@cox.net
wildman334@suddenlink.net
wildman334@suddenlink.com

In addition, the above referenced administrative subpoena (IINI 1760) requested

Suddenlink Communications provide information related to IP address 68.1.238.104

assigned on February 14, 2007, 14:34:46 CST (derived from results of IINI 1522).

27.   On April 30, 2007, Suddenlink Communications, in response to the administrative

subpoena (IINI 1760) served on April 25, 2007, identified the account assigned to IP

address 68.1.238.104 assigned on February 14, 2007, 14:34:46 CST (derived from results

of IINI 1522 above):

User logins:	daniel.castleman
	wildman334
Electronic mail (e-mail):	daniel.castleman@suddenling.net

	wildman334@suddenlink.net
Name:	Daniel Castleman
Address:	2813 60th Street
	Lubbock, TX 79413
Telephone:	806-791-7668

28.   On April 25, 2007, an administrative subpoena (IINI 1761) was served on AT&T,

Inc., 208 South Akard, 10th Floor, Dallas, TX 75202, for subscriber information

associated with telephone number 806-791-7668 (derived from IINI 1624 and IINI 1760).

29.   On May 10, 2007, AT&T, Inc., in response to the administrative subpoena (IINI

1761) served on April 25, 2007, identified the subscriber for telephone number 806-791-

7668 (derived from IINI 1624 and IINI 1760):

Name:	Daniel Castleman
Address:	2813 60th Street
	Lubbock, TX 79413
Established:	October, 2004

30.   On or about March 31, 2007, an individual utilizing the nickname "Jummi"

(Daniel Castleman) posted a message with the subject line "Re: Haikus for all" in the

newsgroup *alt.japan.security.pgp*, and encrypted with the PGP keys utilized by members

of the child exploitation enterprise. In the message, "Jummi" provided information

regarding the download, decryption, and re-assembly of files located in the newsgroups

alt.binaries.test.yenc (a.b.t.yenc).

31.   On or about April 2, 2007, a TFO, acting in a covert capacity, downloaded the files

identified by "Jummi" in his posting on March 31, 2007, from the newsgroup

alt.japan.security.pgp. Utilizing the instructions provided by "Jummi" (Daniel

Castleman) and the group encryption keys, the task force officer was able to successfully

decrypt and re-assemble the files.

32.   A review of the re-constructed folders and associated files showed that they

contained 3 video files with a combined size of approximately 810 MB. A review of the

videos revealed the following depictions of child pornography:

> Open-f04.mpg
> A video (with audio - music only) (approximately 15 minutes 55 seconds)
> depicting a nude prepubescent female sitting on a couch fondling her genitals with
> her hand. An adult male, wearing underwear and a tee shirt, lies down on the
> couch and the female helps remove his underwear. The nude prepubescent female
> manually stimulates the adult male with her hand, and then performs oral sex on
> the adult male. The adult male begins to rub the girl's bare chest.

> Open-f07.mpg
> A video (with audio - music only) (approximately 21 minutes 29 seconds)
> depicting a nude adult female performing oral sex on a nude prepubescent female
> lying on a couch. The adult female and prepubescent female switch places and the
> prepubescent female begins vaginally stimulating the adult with her hands. The
> prepubescent female inserts her entire hand into the adult female's vagina. The
> adult female positions herself, on her hands and knees, over the prepubescent
> female who then orally stimulates the adult female's breasts. The prepubescent
> female performs oral sex on the adult female. Both the adult and prepubescent
> female lie together, in opposite directions, and perform oral sex on each other.

> Open-f13.mpg
> A video (with audio - music only) (approximately 11 minutes 52 seconds)
> depicting a nude prepubescent female and nude prepubescent male sitting on a
> bed. The male is fondling the female's genitals with his hand, while the female is
> stimulating the male with her hand. The female performs oral sex on the male
> while fondling herself with her hand.

33. On February 29, 2008, A Federal Search Warrant was executed on the residence of

Daniel Castleman (he was present). During the course of the search, a CD-R was located

with a homemade label on the CD-R titled, "To Taylor and her Dad From Vicky and Her Dad Hope this helps to let taylor know that it is ok for the two of you to play together like me and my dad." The following videos were located on the CD-R:

asveq01

Prepubescent female wearing a black mini skirt and thigh high stockings, with her legs over her head displaying her genitalia and anus. The camera is focused on this area and zooms in. She then takes off her nightgown top and massages her breasts.

asveq02

Prepubescent female masterbating an adult male while resting her head on his abdomen. She then performed oral sex on the adult male.

asveq03

Prepubescent female undresses in front of camera and performs oral sex on an adult male and the adult male masterbates.

asveq04

Prepubescent female performs oral sex on adult male in a bed.

34.   Also located in the residence during the search was a piece of paper listing the nicknames of the individuals posting text and binary posting in the criminal enterprise. The only individuals privy to this information would have P2P encryption keys specific to the newsgroup where this information was obtained.

One of those individuals, who advertised, transported, shipped and received child pornography in conjunction with the above named individual operated in the Northern District of Florida.

CONCLUSION

I, therefore, respectfully request that a warrant be issued authorizing the arrest of the above individual.
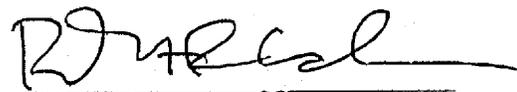
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me on 2·29-08 .

Elizabeth M. Timothy
UNITED STATES MAGISTRATE JUDGE

28