KNOW YOUR LABELS (FAQ)

Not all pedophiles are contact child sex offenders, meaning not all pedophiles will sexually offend against a child.

Not all child sex offenders are pedophiles, meaning committing a child sex offense does not mean that someone will meet the diagnostic criteria for being a pedophile.

There are more child pornography users than there are contact child sex offenders (Frei et al., 2005).

1. Child Pornography

a. Section 2256 of Title 18, United States Code, defines child pornography as any visual depiction of sexually explicit conduct involving a minor (someone under 18 years of age).
b. Visual depictions include photographs, videos, digital or computer generated images indistinguishable from an actual minor, and images created, adapted, or modified, but appear to depict an identifiable, actual minor.
c. Undeveloped film, undeveloped videotape, and electronically stored data that can be converted into a visual image of child pornography are also deemed illegal visual depictions under federal law.
d. The legal definition of sexually explicit conduct does not require that an image depict a child engaging in sexual activity.
e. Now referred to as “child sexual exploitation material” (CSEM) in the academic literature.
f. There is no evidence that the accessibility of internet child pornography has caused increases in child sexual abuse (see Wolak, Finkelhor, and Mitchell, 2011).
g. The number of individuals arrested for CP has increased in the last decade but this is likely due to the increase in law enforcement resources to investigate these crimes, including funding and new investigative tools.

2. Child Pornography Collections

a. Some child pornography users may experience a level of desensitization to mainstream pornography which results in a need to collect more extreme pornographic materials (Merdian et al., 2013; Quayle & Taylor, 2002; Quayle & Taylor, 2003).

b. Pornography users often “move through a variety of pornographies, each time assessing more extreme material” as a result of desensitization or appetite satiation, and this often leads to collecting and discovering other forms of deviant pornography (Quayle & Taylor, 2002; Quayle & Taylor, 2003; Seigfried-Spellar & Rogers, 2013; Seigfried-Spellar, 2016; Seigfried-Spellar, 2018).
c. Some child pornography users may collect sexual images of children, not because of an underlying paraphilia or sexual interest in children, but because the images are easily accessible via the Internet (Basbaum, 2010) or as part of a preference for sexually deviant content (Kettleborough & Merdian, 2017).
d. Child pornography collections often include a wide-range of images, both mainstream adult pornography and other deviant forms of pornography, such as fetish or animal pornography (Seigfried-Spellar, 2014; Seigfried-Spellar, 2016; Seigfried-Spellar, 2018).
e. Some child pornography collectors receive sexual or psychological gratification from the process of categorizing and organizing their collection categorization (see Quayle & Taylor, 2002).
f. McCarthy (2010) states that it is not the size of the child pornography collection that matters, but instead it is the proportion of adult to child pornography.
g. Contact child sex offenders are more likely to possess more child pornography in relation to adult pornography compared to non-contact offenders (i.e., child pornography users who have no history of child sex abuse; McCarthy, 2010).

3. Pedophilia

a. Not a legal or criminal term but a clinical diagnosis based on specific criteria in the Diagnostic Statistical Manual for Mental Disorders (DSM 5; 2013).
b. Diagnostic Criteria 302.2 (F65.4)
    - Over a period of at least 6 months, recurrent, intense sexually arousing fantasies, sexual urges, or behaviors involving sexual activity with a prepubescent child or children (generally age 13 years or younger).
    - The individual has acted on these sexual urges, or the sexual urges or fantasies cause marked distress or interpersonal difficulty.
    - The individual is at least age 16 years and at least 5 years older than the child or children.
c. Not considered a mental disorder but instead a paraphilic disorder involving prepubescent children.
d. The highest possible prevalence for pedophilic disorder in the male population is approximately 3–5%.
e. Female prevalence for pedophilic disorder is unknown.
f. Adult males with pedophilic disorder may indicate that they become aware of strong or preferential sexual interest in children around the time of puberty
g. To avoid the stigma associated with the word pedophilie, some pedophiles are using the term “minor-attracted person” or MAP as a label.

h. The extensive use of pornography depicting prepubescent children may be a diagnostic indicator of pedophilic disorder (see Seto et al., 2006).

MYTHS:

1. IP Addresses are Good Enough

How do you uniquely identify the suspects system for the purposes of court orders, subpoenas, and search warrants (Many of these are capture and available in the ICAC Databases of suspicious CSE activity).

IP Address (Good)

While this is a start, the IP address is not necessarily unique. This address can be changed (sometimes by the user). An ISP using DHCP could result in the same IP address be assigned to a different system(s) over a period of time.

The IP address often identifies the cable modem or external router, but doesn't identify any systems behind the cable modem or router.

MAC Address (Better)

This address is assigned to the network card of the system (ethernet or wifi). Cannot easily be changed. Every network card has a unique MAC Address.

Be careful that the MAC addresses belong to computers behind the modem or router and not the router/modem itself.

GUID (Best)

Globally Unique Identifier (GUID), is created by the P2P Client software as a way of uniquely identifying the client. The GUID uses the client and the system it is installed on to create the identifier. This number is hard to change (e.g., user would need to uninstall and then reinstall the P2P Client).

CSE material downloaded by LE found on the suspect system (BESTEST)

The positive identification of any CSE material downloaded by LE as part of the investigation, on the suspects system at the time of seizure, is important.

Comparing the located files and hashes with known CSE P2P hashes or NCMEC (Innocent Images) hashes should be done as well.

2. A User Account is Good Enough

We can show what account was being used but that doesn't necessarily tell us who was using the account - think shared accounts, hacked accounts, accounts left logged in.

Always check for malware to be able to counter or support the "malware, trojan horse" defense.

User Account

What user account was logged in during the events in question?
Where then any failed login attempts?

User Profile

Once the account is known, then the folders that make up the user's profile can be used to identify "owner" of the files. For example:

- AppData
- Cookies
- Desktop
- Documents
- Local Settings
- My Documents
- Downloads
- Pictures
- Recent
- Searches
- Videos

BUT, who was behind the Keyboard?

3. If the Account is Shared You Can't Tell Who Was Behind the Keyboard

It is thought that a forensic analysis (autopsy) of a system can only tell you the account(s) being used, but not who was sitting behind the keyboard.

- We can create behavioral profiles of users based on internet artifacts. These profiles can be used to determine the likelihood that it was Suspect-A vs Suspect-B.

Timeline & Internet Artifacts Analysis

Understanding when activities occurred in relation to the what the suspect(s) was doing or should have been doing (e.,g., at work, at school, at home).

- User patterns can be identified that can be mapped back onto patterns corresponding to the events in question.

4. Context Doesn't Matter?

Where evidence is found can be just as important as what is found! Context can be used to support or refute “intentionality” (Knowingly). It can be used to support or refute mitigating circumstances for sentencing purposes.

Location Analysis

Like saying goes, it’s all about the location.

- Where was the evidence found? Was it found in default locations (e.g., downloads folder) or is there evidence that the user created non-default storage locations (e.g., uniquely labeled folders).
- Was the evidence purposefully deleted/wiped?
- Was the evidence found in locations that the user would have access to, as opposed to hidden folders (e.g., cache, Temporary Internet Files)?
- Where was the evidence in relation to other files etc. that are important to the user (e.g., Desktop) - digital archeology.

Frequency/Pattern Analysis

How often someone interacts with a file or displays a specific behavior is very important.

- How many times was a file viewed, opened, copied?
- How many times was a website or chat room visited?
- How many times were particular search terms used?
- How many CSE images/videos were there in relation to other non CSE images/videos?