"SHERI'S SIDEBAR" Edition #29 4/19/2024

Happy Friday everyone.

I am back again with things I wish I had known during practice, things that have changed, interesting tidbits, and random tips for practice. Welcome back to:

SHERI'S SIDEBAR

Today let's discuss defending Alleged Possession of Child Sexual Abuse Materials/Child Pornography – THERE ARE THINGS YOU MAY NOT HAVE KNOWN WITHIN....

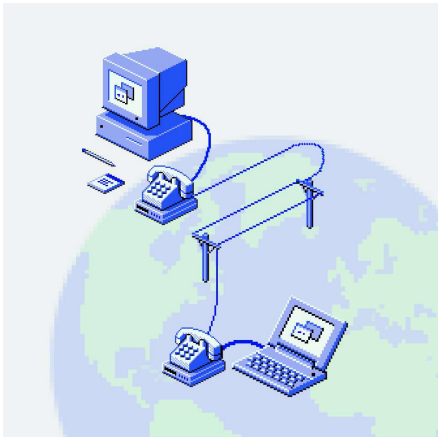
This is a long one but super helpful for Peer to Peer or Child Porn Cases! **I may have additional information if you have a case for which you need more information.

1. **Did you know when the State argues a witness is unavailable because they are on vacation or have some other event to attend to, despite there being some case law that says that is sufficient to make a witness unavailable, there is also conflicting case law?**

   For the purposes of CrR 3.3, **an "unavailable" witness is one whose testimony cannot be contrived by any means.** The word "unavailable" is not used in the social sense of having a previous engagement.
   State v. Torres, 111 Wn. App. 323, 330–31, 44 P.3d 903, 906 (2002).

   There is another case I can't recall the name of right now that also says merely because an officer is on vacation does not mean he is not available to testify. The state has to perform due diligence to determine whether the officer is still in the area where he could be subpoenaed to testify. See Edition 28 for more authority, #6.

2. **Are you aware that an IP Address alone is not sufficient PC to identify an individual or device (computer, phone, internet based device at a location) for a search warrant? (Think about those dropbox peer to peer sharing child pornography ICAC/NCMEC type cases).**

   I was thinking to myself the other day…Self, if we no longer have internet that works like this:  AND WE DON'T! WHY are we not objecting to Search Warrants that are granted solely on the basis of who pays for an IP address? Is it lack of education? Technology and I have a love/hate relationship…but let me see if I can help us out here…

   IT USED TO BE the IP address was linked to the only computer in the house, which was linked to a direct phone line, linked to the wall plug, and linked to the person paying the landline phone bill at the residence…but even then, *police could not*

prove who was sitting at the computer when say, Peer to Peer child porn was allegedly downloaded.

NOW, with wifi:

Wifi IP addresses go only to the PROPERTY. They do not even have to go *INSIDE THE RESIDENCE*. Police would have to be *inside the network or router* to determine *which individual device* on that wifi downloaded something, i.e. whose cellphone, laptop, desktop, chromebook, ipad, tablet, iPhone, Pixel, watch or whatever wifi capable device anyone within the home, *or anyone with access to the wifi* at the time may have been using.

IMPORTANT TIP:

The network or router assigns an IP address to each device, each time it logs onto the network. Some routers assign the same IP address to the same device, like a lease, for a period of time, OR until you reboot the router. Other routers randomly assign the IP address for each device everytime you login to the wifi.

That means:

1) it is not limited to the people who live there;
2) it absolutely is not limited to the person whose name is on the bill!
3) There is NO PC simply because an officer has an IP ADDRESS and a name of a person paying for wifi at a property.

Wifi IP addresses are also often not password protected, or not protected well. Remember when data packages on your cellphone were not unlimited? You could walk or pull up somewhere and catch someone's wifi unprotected and use it. THAT STILL HAPPENS, I SWEAR! I HAVE SEEN UNPROTECTED WIFI AVAILABLE when connecting to my hotspot!! OFTEN. Some people still have to pay for data and use other people's wifi.

Wifi is also easily hackable because people put 12345 as their password, **still.**

Seriously. Not to mention the devices you can buy online, or all the hackers out there that want your identifiable information and bank access to sell on the

DarkWeb. Also, unless you have the service that alerts you when a device logs on to your wifi, you do not even know that you have been hacked.

There are VPN proxy services to hide your location, or create a location change. Many sports guys know about this one! You live in an area where a certain sports tv package is not available. So you buy an VPN proxy service that shows your IP address in say Los Angeles instead of Port Angeles, so that you can get the sports packages blocked out in Port Angeles that are available in Los Angeles, because now your IP Address shows that is where you live.

MAKE OBJECTIONS – DRAFT MOTIONS TO EXCLUDE THE FRUIT OF THE POSIONOUS TREE!

3. **How many jurisdictions have Deputy Prosecutors who try to maintain criminal charges without a finding of probable cause? Did you know the U.S. Supreme Court has expressly stated a defendant's constitutional rights include the right to be free from prosecutions lacking probable cause?**

Albright v. Oliver, 510 U.S. 266, 271, 114 S.Ct. 807, 127 L.Ed.2d 114 (1994). The case cited the Fourth Amendment, which is where the police are required to have PC to arrest you.... I was thinking of the right to be free from governmental interference.

See also:

RCW 9.94A.411(2) **Decision to prosecute**.

(b) GUIDELINES/COMMENTARY:

(i) Police Investigation

A prosecuting attorney is dependent upon law enforcement agencies to conduct the necessary factual investigation which must precede the decision to prosecute. **The prosecuting attorney shall ensure that a thorough factual investigation has been conducted before a decision to prosecute is made.** In ordinary circumstances the investigation should include the following:

(A) The interviewing of all material witnesses, together with the obtaining of written statements whenever possible;

(B) The completion of necessary laboratory tests; and

(C) The obtaining, in accordance with constitutional requirements, of the suspect's version of the events.

If the initial investigation is incomplete, a prosecuting attorney should insist upon further investigation before a decision to prosecute is made, and specify what the investigation needs to include.

(ii) Exceptions

In certain situations, a prosecuting attorney may authorize filing of a criminal complaint before the investigation is complete if:

(A) Probable cause exists to believe the suspect is guilty; ***and***

(B) The suspect presents a danger to the community or is likely to flee if not apprehended; or

(C) The arrest of the suspect is necessary to complete the investigation of the crime.

In the event that the exception to the standard is applied, the prosecuting attorney shall obtain a commitment from the law enforcement agency involved to complete the investigation in a timely manner. If the subsequent investigation does not produce sufficient evidence to meet the normal charging standard, the complaint should be dismissed.

"I don't *need* probable cause!"

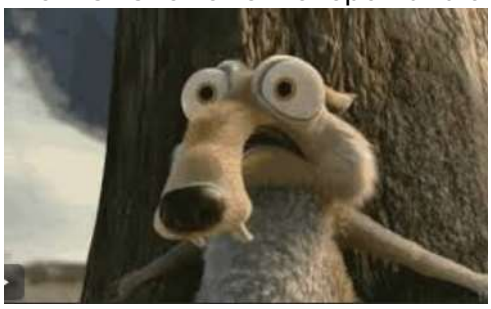
4. Do you know when you are dealing with a NCMEC case? Do you know who or what NCMEC is? Or What you should do if you are dealing with a NCMEC case?

- NCMEC – National Center for Missing and Exploited Children work with ICAC and other law enforcement agencies, dealing with child sex trafficking as one of their focus areas. NCMEC has a method of marking and tracking Child Sexual Abuse Material (CSAM), which is then used by law enforcement to seek warrants when detected by electronic service providers (ESP) that previously marked CSAM has been detected on an individual's device or in their online accounts. At times all they really have is their IP address – see #1 above. However, there are other issues as well.
    - How do they track it?
        - Peer to Peer file sharing
        - Malware
    - How do you know NCMEC or ICAC (Internet Crimes Against Children-a cross agency and jurisdiction law enforcement group) are involved?
        - Warrants will state the basis for PC as a report from an electronic provider to NCMEC.
        - It may reference a "CyberTipline Report"
        - The Affiant will likely be from the ICAC Task Force

- Why is this important to you?
    - NCMEC states that it is a nonprofit organization and resists characterization as a governmental actor for discovery and Fourth Amendment purposes.
    - **But see *U.S. v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016)(finding that NCMEC is a "governmental entity"** because service providers are required to report CSAM to NCMEC and NCMEC is required to forward those reports

to law enforcement); **see also**, NCMEC is federally funded and its two primary authorizing statutes, 18 U.S.C.§ 2258A and 42 U.S.C. § 5773(b), mandate its collaboration with federal, state and local law enforcement.

- I WORKED CLOSELY WITH ICAC ON A HANDFUL OF NCMEC CASES AS A PROSECUTOR. THINGS DURING THE INVESTIGATION SUCH AS THIS OCCUR:
    - ESP sends identified SUSPECTED matches to the tip line with OR WITHOUT reviewing the file to determine whether it is in fact a match. This is important right? To what extent can the government rely on the private search doctrine if the file sent was not in fact reviewed in the first place?
    - Basic information is also forwarded which includes an IP address, and if it is known, an email address and user name.
    - Then NCMEC may or MAY NOT also review the files to determine whether OR NOT the files actually contain CSAM! Private search doctrine reliability again.
        - DEMAND IN DISCOVERY THE CyberTipline Report!
            - This documents both the ESP actions/report and NCMEC's actions, including whether each agency did or did not review the file for CSAM.
    - NCMEC then uses the IP address to identify the geographic location where the user is likely to be located, identifies relevant law enforcement agencies, and contacts the regional ICAC task force in that area.
    - Then ICAC reviews the report and often reviews the files **<u>without a warrant</u>**.



That is possibly 3 agencies reviewing a file without a warrant. Or 2 agencies alleging private search doctrine and forwarding information they allege is CSAM WITHOUT HAVING ACTUALLY REVIEWED IT, then ICAC reviewing it WITHOUT A WARRANT so that the private search doctrine does not protect ICAC's search. Remember the 10th Circuit has held that NCMEC is a government agency. So if ESP does not validate that the file sent is actually CSAM, the private search doctrine fails. NCMEC and ICAC BOTH REQUIRE A WARRANT Under the 4th Amendment.

    - **Since WA Art. 1 Sec. 7 has stronger protections, you have great evidence for suppression/exclusion of the evidence!**

    - **It is also important to verify whether ICAC sent a preservation letter to ESP in anticipation of obtaining a search warrant later.**

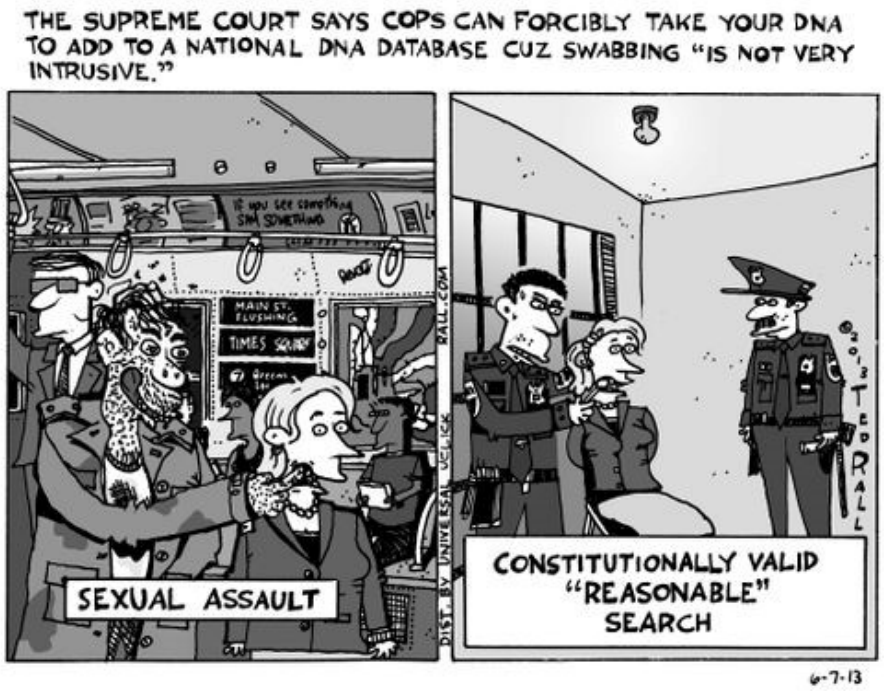
- **ICAC also at this time sends a subpoena to the internet service provider associated with the reported IP address to reveal the individual's name and physical address. With that the officer gets another search warrant for the user's account contents from the service provider…and seek out other accounts maintained by the same individual. Then getting a search warrant for the residence to obtain all electronic devices therein for CSAM.**
    - **But wait …. What about #1. How does ICAC know the IP address belongs to the individual paying the internet bill and whose residence is on that bill when multiple people can be in the house, guests can be in the house using the wifi, or people can be on or near the property also using the wifi with or without the knowledge of the people within the house???**
    - **Fight the search warrant. How is that reasonable suspicion to get YOUR INDIVIDUAL CLIENT's INFORMATION?**
    - **And how the hell does ICAC know or have any reasonable belief that ALL electronic devices therein belong to one individual?!**
        - Any attorneys have a home office?
        - Anyone use back up drives to store your old client files?
        - Anyone have jump drives with client information on them or tons of BWC video evidence stored?
        - Anyone have CSAM with a protection order as evidence for a client's case?
        - Anyone have a separate phone for your job?
        - Have any other adults in the house?
        - Have adult children in the house?
        - Anyone use your home or part of your home for Air BnB?
        - How many electronic devices are in your home right now?
            - Let's see, right now, in my house there are 19 I can think of off the top of my head. 3 belong to my private practice, 1 belongs to my current job.
            - Anyone ever had police threaten to come search your house? I have. Fortunately, as a former prosecutor I was able to make one phone call to pull in favors to get that shit called off. I have burned those bridges now by taking down those prosecutors in court when they came after me personally, but I was glad I had that favor then.
            - Because you know if the police came, <u>no matter what you said, they would take all of your protected, confidential information and go through all of your office and files regardless!</u>

- **4th Amendment & WA. Const. Art. 1 Sec. 7 Challenges:**

  - Was there PC for the device and account searches, *and for the scope of the search- was it sufficiently particularized to the indicia of ownership?*

  - Is there a suppression issue under the Fifth Amendment if either the warrant or the Police compelled the client to divulge their passcodes? TIP: Review NACDL's "Compelled Decryption Primer

  - Challenge the preservation order issued to ESP under 18 USC 2703(f). The order requires ESP to create a copy of the user's account and store it on behalf of the government…which is…an illegal seizure.



(US Supreme Court ruling DNA upon arrest, not conviction, is legal)

- How or why is it a seizure?
    - Because it deprives the user of his or her right to control their own data. The user's files are their digital papers and effects, any trespass upon their property right (via copying them to preserve them for the government) is a 4th Amendment seizure.
    - Demand Discovery for all preservation letters/orders connected to the case!

- Back to the private search doctrine.
    - Remember that the police cannot exceed the scope of viewing beyond what the private entity viewed without a warrant. US v. Jacobsen, 466 US 109 (1984).
    - If ESP never reviewed the files before reporting them, relying on the hash marks, then any subsequent review by NCMEC or ICAC or any other law enforcement agency is a warrantless search because only ESP is a private entity.
        - Remember to DEMAND the CyberTipline Report from NCMEC & Investigation notes from ICAC/Law Enforcement

- If ESP did review the files and the review by NCMEC/ICAC did not exceed that scope, consider arguing the private search doctrine does not apply in this circumstance because it was created with the physical world in mind, not the digital/electronic world of technology in which we live today – much like the public-space doctrine, the search incident to arrest doctrine, and the third party doctrine – all of which the US Supreme Court did not allow to apply to the digital device technology world when confronted with cases of technology like cellphones and computers. Therefore, there is no reason to believe the private search doctrine, created around a mailing tube in Jacobson, should govern the privacy of online accounts and communication in the technology era of remote servers and data stored in the cloud.

    - TIP: You can ask the Fourth Amendment Center at NACDL for help on these types of cases. They have sample motions and other resources.
    - I obtained most of this information at a NACDL Sex Offense Training in addition to the limited experience working with ICAC on NCMEC cases.
    - I have also taken webinar training from the Fourth Amendment Center, they are super helpful.

5. Did you know that on P2P (Peer to Peer file sharing) cases for CSAM, if the entire file is not downloaded, it cannot be viewed, it is unusable?

What does that mean, and does it help my client? YES IT HELPS, let's talk about what it means...

When you use P2P file sharing, there are groups of people who all share files, it is not a direct one person sharing one entire file to another 1 person's device. Instead, this is what happens. AND THIS IS WHAT YOU HAVE TO EXPLAIN TO THE JURY:

- Everyone sharing downloads the software
- The software uses "File hashing" NOT "matching" to find or locate things
- For example, to share a copy of the painting of the Mona Lisa,
    - The image is dissected into a grid using a mathematical algoritham
    - Each grid piece is assigned a hash value
    - Each grid piece is sent individually
    - All pieces of the grid must be received to put the painting back together for the hash values to match FOR THE FILE TO BE ABLE TO OPEN
    - Let's say the painting is put into a grid of 9 pieces
    - If you only receive 8 pieces and log off to go to work, you cannot yet open the file of the painting because the hash values won't match sufficiently to reconstruct the entire painting.
    - MAKE SENSE?
    - YOU NEED EVERYTHING WITHIN THE HASH VALUES THAT ARE MARKED TO OPEN THE FILE. THIS IS IMPORTANT

- When police or NCMEC take hashes of photos, they take them of a series of photos together, even if only 1 of 10 photos has a nude child because they are more likely to find file 1 of the nude child if they also can find 2-10, it makes the search easier.
    - Images are stored in the FBI Database even though there are innocent images within the series – MORE INNOCENT IMAGES THAN CSAM
    - There used to be 1 guy who was the sole authority of what went into the database, who determined "what is a child" – even from other cultures. One example from another culture was proven to be a 52 yoa female but his belief was this was a minor child. Other countries age of consent outside of the US is 12, 13, and age of marriage is 14.
    - Social media, the Lutheran Church and private organizations like you have seen on true crime tv shows luring people have also been involved in determining "what is a child" for the hash marking of CSAM images.
        - This means if your parents or your client's parents put the grandchild's bathtub shot on Facebook, Instagram, X/Twitter, it can be marked as CSAM if genitals or breasts (even unformed toddler age appropriate) can be seen.

        - NOTE a Torrent File is NOT a bad content file per se.
            - A torrent file means the file has been deconstructed into the pieces and parts which need to be reconstructed. The content of those pieces and parts can contain anything, good or bad.
            - The instructions come from the program software to go seek from ANYWHERE IN THE CONNECTIONS, ANY DIRECTORY THAT HAS THE PIECES, TO SEEK AND DOWNLOAD THEM FOR YOU TO RECONSTRUCT THE ENTIRE FILE on the client's computer.
            - IF one stops sharing, there are problems

- More explanation for you:
    - Google search or search software
        - You have the ability to turn on/off the ability to share while downloading
        - As soon as you have downloaded 1 piece, you can also share that same 1 piece
            - Even though you cannot open that 1 piece because you don't have the entire file. This is part of the end user licensing.

    - Torrent Exchanges
        - Pirate Bay – Men in Black 2 for example
            - It was downloaded a lot
            - You search, it starts downloading the movie
            - Click on torrent file download – be patient, the length of time depends on how many other people are sharing that movie for how long it takes to download the entire movie

        - If you want to share the p2p file, you put it on a webserver to share it
            - If you are the only 1 sharing and x is the only 1 downloading it
            - Then another person starts downloading it from the 1 person sharing it
            - A swarm is created
            - When the swarm gets too large, people will not get enough pieces to reconstruct the entire movie
            - Once 1 person does get the entire movie they become a sender too

        - So, law enforcement uses Roundup tools
            - Roundup emule
            - Roundup torrential downpour
            - Roundup ares
            - Shareazale
            - Peer spectre (not in use anymore)
            - Cps

- They look for hash values, not file names
    - Master file table:
        - File name is a label.
        - They want content – they want to find those "innocent images" which they know are attached to the 1 CSAM image
    - They go fishing
    - They fish in their local jurisdiction
    - If no fish there, they fish next door
    - ICAC deconfliction traces the IP address
        - "I detected Jones at 2am
        - OTHER JURISDICTION HANDS OFF TO THEM because it is in their jurisdiction
            - (remember the bored lea didn't find anything in HIS jurisdiction so he fished next door. He found something now he has to hand it off because he doesn't have jurisdiction to do anything about it).
            - FRANKS Motion
                - Pull the timecards of the officer – make sure the local officer isn't acting in place of the ICAC officer who does not have jurisdiction when filing the warrant
                - Watch for the silver platter doctrine (WA allows it but review Carpenter to see if you can fight it on digital grounds) and the ICAC task force

- REMEMBER the file was downloaded in parts, each file goes in **".part"**
    - The law enforcement forensic program can play it to see that it is CSAM
    - BUT THE CLIENT'S PROGRAM CANNOT PLAY IT AND COULD NEVER TELL IT WAS CSAM IF THEY DID NOT GET THE ENTIRE FILE
        - No KNOWLEDGE of the file contents, no mens rea
    - If the client started a download but did not finish it – they cannot knowingly posses
    - If the internet stopped and they don't have an entire file…
    - If the swarm fell apart and they did not get an entire file…
    - If they have piece of the file 4/454 or all the way up to 434/444 IT CANNOT BE PLAYED OR OPENED because ".part" is NOT A FILE
    - LAW ENFORCEMENT KNOWS THIS

- Ask for the LOG BITES in discovery
    - When law enforcement (LEA – law enforcement agency) downloads, they only download the suspect/client's computer files. They get a log

file with bites info which tells them whether or not the client received all the pieces!
    - It will say 4/209 or 208/209
    - Each part file has a .extension
    - ONLY IF THE DEFENDANT CLIENT IS A FORENSIC EXPERT OR HAS FORENSIC SOFTWARE CAN THEY PLAY .part files.

- Possible defenses
    - Names of the files in the LEA database in the warrant are not the same as in the client's computer – or the same on the description – they use some from another case
    - They did not see the video they only ran the hash value match
    - GO SEE THE VIDEO ON THE CLIENT'S COMPUTER – MUST SEE THE FILE DOWNLOADED for the search warrant
    - If you can't see it because it won't download and is unreadable, unusable, that is GREAT EVIDENCE FOR THE JURY
        - It proves the client only had a ".part" file and not the entire file and therefore the client had no way of knowing what was in the file.

- SW analysis
    - Application and scope
    - Were the files referenced actually viewed by the lea WHILE ON SITE?

- Knowingly Possess
    - Was the client able to play the videos – were they downloaded or are they ".part" files
    - Did the client make any statements about the actual file being fully downloaded
    - Did the client view the full downloaded file (check dates)
    - Are the image files found on google images?
        - E.g. you cannot tell if buttocks is of a child or not and the same image is on google images
        - Do a reverse search on google – figure out how to do reverse image searches if you don't know how or have your investigator do these
    - Are the files of images which are difficult to determine the age of the individual pictured

- Frank's Motion & hearing on the SW
- Attack the log bite files
- Check the forensics
    - Staleness
    - Is there a prior owner of the computer

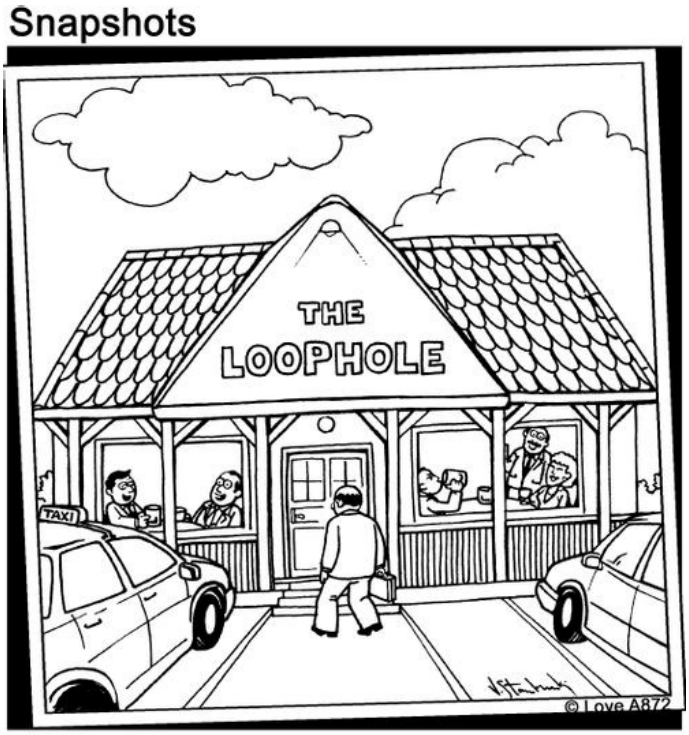
- Is it a used hard drive
- Can LEA place the client behind the keyboard/monitor?

Other Tips:

- Finding hash and historical information
- If your client lives in an apartment
  - Prior bad person's IP address could have been reassigned to your client, and now your client is in the law enforcement's database being watched and monitored for historical use
  - Search for "vice.com" non-profits use 10% use data and hand off to lea – their names are never in any report
  - Police trick computers by sending gov ad files to download fake servers in same numbers to trick you into thinking you are downloading child porn but it is fake

Have a great weekend all. Try to relax and enjoy the sun that has finally arrived after that lying little rodent and his early spring deception has ended.

Be a trail blazer I always say …



A popular hangout for attorneys.

Sheri

Sheri's Sidebar Editions are archived here: https://defensenet.org/resource-category/sheris-sidebar/