DIGITAL DEVICES

THE REALITY OF TODAY'S ENFORCEMENT is that many crimes committed in modern society have evidence regarding the crime stored in some digital format. Years ago a crime scene may have included a smoking gun, a few receipts, and a notebook of events of a particular crime. As technology develops and the Internet expands, wildlife enforcement officers are finding the expansion of communication sometimes includes evidence of a crime on local computers, digital devices, digital video cameras and the Internet. Many criminals have access to vast amounts of information on how to commit their crimes and often use Web-based social media to share the pictures of their activity. It doesn't matter if the crime is theft, deception, battery, hate crimes, wildlife or murder. Many times there is evidence of these crimes researched, stored or hidden on some digital device. It might be a cell phone used to make the call or text, a digital video camera used to scout an area, or a GPS device used to navigate the terrain. Keep in mind during your next investigation that digital evidence is all around us and knowing how to properly secure and search this evidence can make the difference between a guilty or not guilty verdict.

A typical days hunt (legal or illegal) includes most of these items: computer–to search for directions, check the weather, determine sunrise and sunset; a digital camera – to secure the images of a day's hunt and share the victory of a harvest; a vehicle or handheld GPS–to safely arrive and navigate to a hunting position; cell phones – to communicate with your hunting party or provide information as a lookout (can also substitute as a computer, GPS, camera, video camera as described above). Let's not forget a trip to the ATM and gas station for fuel, food, and soda. Most legal hunters are going to employ these devices in efforts to make their hunt more successful. They may even use these devices to assist them in returning home or calling for help.

Now turn your focus on the unlawful hunt. Imagine you were called to a location which included four young men, a vehicle, a rifle, three dead deer, and a case of beer. After securing the scene and speaking with the persons involved you may find conflicting information. Taking the opportunity to seize cell phones, cameras, and the GPS on the dash may provide valuable information. If some of the persons involved are lying about their identity (to avoid a warrant check) a search of the phone may provide intimate information about the person who owns it, including pictures and friend or family contact information. If your laws allow it, a call to the 'dad's cell' number may give you a personal insight to the owner of the phone.

Looking further at cell phone text messages may reveal prior communication and intent on committing the violation. It may also show information to outside parties who have knowledge of the illegal acts. An offender may text his girlfriend stating that they had "shot another deer", "killed a big buck", or "call Joe's butcher and tell him we are on the way". Securing the other party's phone and interviewing the other party may provide valuable information on the events. These text messages also may implicate others involved and the time the event started. A text message to "Andy" stating "I'll pick you up at 9" would likely show the location and events. Picture messages are often used to send information regarding a crime in a similar fashion as text. The added value is a photograph of the incident.

What happens after you secure the device if the offender does not give you permission to search it? Each jurisdiction is different. Here is a general outline of

how it may be done. Contact your local state's attorney and advise of the offense, criminal history, and items used. Draft a search warrant to have the devices searched and testify before a judge. Take the signed documents and contact your local crime lab or FBI office and request service on a digital device. The device is then transported to the lab for analysis. The secret service offers advice on transporting electronic devices at www.forwardedge2.com/pdf/bestpractices.pdf. The following information was taken from the guide provided by the secret service:

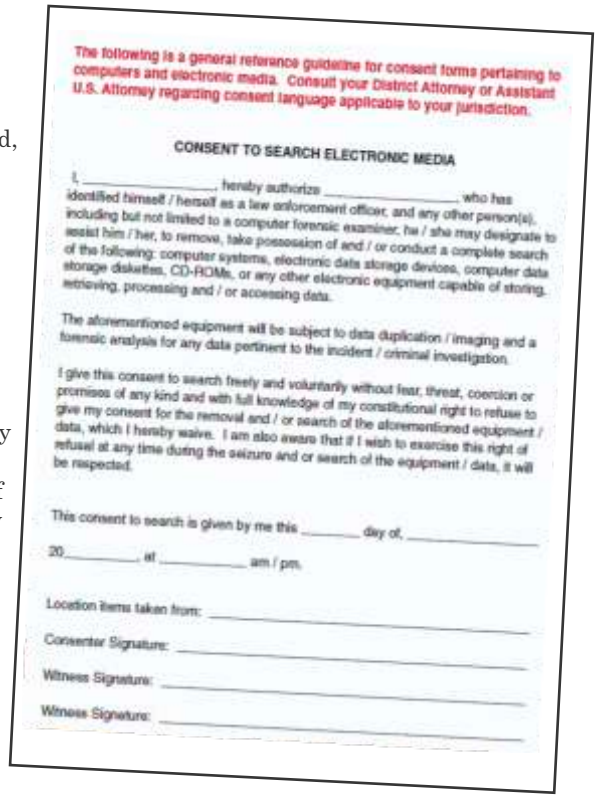
PDA, Cell Phone & Digital Camera

Personal digital assistants, cell phones and digital cameras may store data directly to internal memory or may contain removable media. The following section details the proper seizure and preservation of these devices and associated removable media.

- If the device is "off", do not turn "on".
- With PDAs or cell phones, if device is on, leave on. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display (if available).
- Label and collect all cables (to include power supply) and transport with device.
- Keep device charged.
- If device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.
- Seize additional storage media (memory sticks, compact flash, etc).
- Document all steps involved in seizure of device and components.

Let's move on to devices which may have gathered evidence along the way. If the offender's wallet is full of 20 dollar bills chances are there may be an ATM image associated with the suspect which may lead you to a time and place for your case. A stop at the local gas station reviewing the camera information usually allows you to see the suspect as he is gearing up for the hunt. The local Wal-Mart is another good place to establish evidence of a person purchasing ammunition or other supplies to commit a wildlife crime. Wisconsin Conservation Officer Youngquist was doing a poaching investigation (of a convicted felon) and found the suspect denied ever possessing the gun or ammunition. A local check of security cameras at Wal-Mart showed the suspect purchasing personal items and ammunition. If the officer is willing to spend the time looking for additional evidence many times it is found.

Here is a final note on wildlife enforce-



The following is a general reference guideline for consent forms pertaining to computers and electronic media. Consult your District Attorney or Assistant U.S. Attorney regarding consent language applicable to your jurisdiction.

CONSENT TO SEARCH ELECTRONIC MEDIA

I, _____, hereby authorize _____, who has identified himself / herself as a law enforcement officer, and any other person(s), including but not limited to a computer forensic examiner, he / she may designate to assist him / her, to remove, take possession of and / or conduct a complete search of the following: computer systems, electronic data storage devices, computer data storage diskettes, CD-ROMs, or any other electronic equipment capable of storing, retrieving, processing and / or accessing data.

The aforementioned equipment will be subject to data duplication / imaging and a forensic analysis for any data pertinent to the incident / criminal investigation.

I give this consent to search freely and voluntarily without fear, threat, coercion or promises of any kind and with full knowledge of my constitutional right to refuse to give my consent for the removal and / or search of the aforementioned equipment / data, which I hereby waive. I am also aware that if I wish to exercise this right of refusal at any time during the seizure and or search of the equipment / data, it will be respected.

This consent to search is given by me this _____ day of, _____ 20_____ at _____ am / pm.

Location items taken from: _____

Consenter Signature: _____

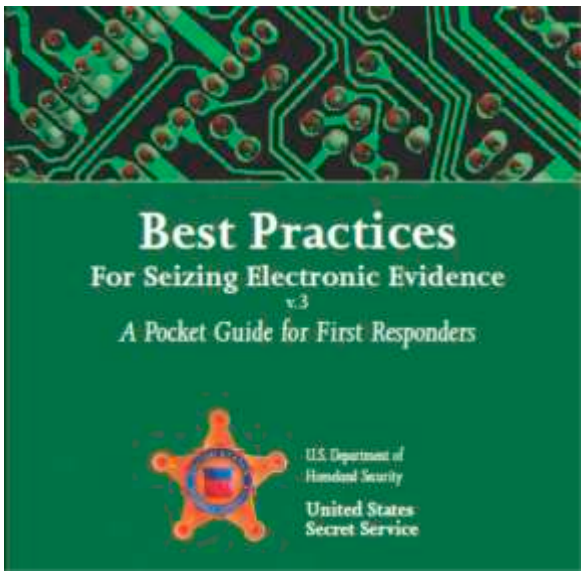
Witness Signature: _____

Witness Signature: _____

ment as many officers have had to perform death investigations. If you encounter a suicide during your tour of duty be aware that many victims share their pain using text messages, sometimes in a last ditch effort to call for help. Officers should take note of these devices and have the crime lab analyze them.

It is strongly recommended that any digital media that is secured as evidence not be placed into a personal computer or non-certified device. Also, when visiting a crime scene secure the devices and don't allow others to search or look through files as they may change. If the suspect is in custody and the defense notices files which have a date stamp after the suspect was already in jail there will be doubt as to the authenticity of these files.

Illinois recently had an on-line case where an offender was selling videos of his vehicle striking multiple deer on several occasions. The sale and profit from this illegal activity was stored on a computer, digital camera, and other electronic media. Digital media is a part of today's society and it should be considered critical during your investigations. Knowing what to look for, how to properly secure it, and decipher the contents could be the difference between a conviction or not. Technical science is not for all officers and can be daunting at times. Agencies are slowly transitioning to computer and Internet based evidence. As main stream society utilizes these items during the commission of a crime it becomes paramount for agencies to prepare its officers for the future of conservation law enforcement.



For more information or personal help in on-line investigations please feel free to contact me at info@stevenbeltran.com