UPC Fall Conference 2013
"Computers" Breakout Session
by
Special Agent Zak Snow
Deputy District Attorney Sandi Johnson

I. Computer Definitions:
   a. IP Address
      i. Static
      ii. Dynamic
   b. ISP – Internet Service Provider
   c. Internet Browser
   d. Router
   e. Modem
   f. Hard Drive
II. Venue v. Jurisdiction
   a. Jurisdiction UCA §76-1-201
      i. A person is subject to prosecution in this state for an offense which he commits, while either within or outside the state if:
         1. The offense is committed wholly or partly within the state or attempted to commit the offense in the state
         2. An offense is committed partly within this state if either the conduct which is any element of the offense, or the result which is an element, occurs within this state.
         3. Identity Fraud is where the victim resides
   b. Venue UCA §76-1-202
      i. Criminal actions shall be tried in the county, district, or precinct where the offense is alleged to have been committed/consumated
      ii. If it cannot be readily determined, venue can be in the county in which the defendant resides
   c. Long Arm Jurisdiction for Service Providers:
      i. must have "minimum contacts" with Utah
         1. "has continuous and systematic general business contacts with [Utah]" (general jurisdiction), or
         2. "has purposely directed his activities at residents of [Utah]" (specific jurisdiction).
III. Service by State agents
   a. Preservation of Electronic Communication: 18 USC 2703(f)
      i. Once a provider of wire or electronic communication services or a remote computing service is requested to, they must preserve records or evidence for 90 days.
   b. 18 USC 2703(g) The presence of an officer shall not be required for service or execution of a <u>search warrant</u> issued in accordance with 18 USC 2701-2711
IV. How to Obtain Contents and Records
   a. Obtaining <u>Contents</u> of Electronic Communications in Electronic Storage for less than 180 days: 18 USC 2703(a)

i. Only pursuant to a federal or State search warrant

b. Obtaining Contents of Electronic Communications in Electronic Storage for more than 180 days
   i. Search Warrant
      1. Notice is NOT required to subscriber or customer
   ii. Federal or State administrative subpoena or a Federal or State grand jury or trial subpoena
      1. Notice IS required to subscriber or customer (see below)
   iii. Court Order under 18 USC 2703(d)
      1. Notice IS required to subscriber or customer
      2. Notice can be delayed 18 USC 2705
         a. Court can order delayed notification for 90 days if adverse result
         b. If using administrative subpoena, can delay for 90 days if certify adverse result
         c. Adverse Result:
            i. endangering the life or physical safety of an individual;
            ii. flight from prosecution;
            iii. destruction of or tampering with evidence;
            iv. intimidation of potential witnesses; or
            v. otherwise seriously jeopardizing an investigation or unduly delaying a trial.

c. Obtaining Records Concerning Electronic Communication Service or Remote Computing Service 18 USC 2703(c)
   i. Search Warrant
   ii. Court Order under 18 USC 2703(d)
   iii. Consent of the subscriber or customer to such disclosure;
   iv. More means, but not often used
   v. Notice is NOT required 18 USC 2703(c)(3)

d. Court Order 18 USC 2703(d)
   i. Reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are
   ii. relevant and material to an ongoing criminal investigation.
      1. Notice is required for content
      2. Notice is NOT required for records

V. State Options

a. Administrative Subpoenas
   i. UCA 77-22-2.5 Sexual offense against minor; child kidnapping; stalking
      1. Reasonable suspicion standard
      2. "Prosecutor" may issue – attorney general, county attorney, district attorney, or municipal attorney
      3. Must provide, if available, to the party subpoenaed:
         a. IP address
         b. E-mail address
         c. Telephone number, or other identifier

d. Dates & Times
4. Prosecutor must be provided with:
    a. Names & Addresses
    b. Telephone connections
    c. Length of service
    d. Records of session times and durations
    e. IP Addresses, network address, subscriber identifiers
    f. Means and sources of payment for the service, including any credit card or bank account numbers
5. Include Language for Sealing

ii. UCA 77-22a-1 Controlled Substances
1. Relevant or material to the investigation
2. "Prosecutor" may issue -- attorney general or deputy or assistant AG, county attorney or deputy, district attorney or deputy. NOTE: municipal attorney NOT authorized
3. Must notify party subpoenaed they can file a motion to quash
4. Prosecutor may subpoena witnesses, compel attendance and testimony of witness, or require production of records or other tangible records
5. Include Language for Sealing

b. Investigative Subpoenas
i. UCA 77-22-2 Any matter involving the investigation of a crime or any criminal conspiracy
1. Court issues the subpoena
2. Based upon "good cause shown"
3. "Prosecutor" means attorney general, county attorney, district attorney, or municipal attorney
4. Subpoena witnesses, compel witness' appearance and take testimony under oath, require the production of documents or any other items that are evidence or relevant to the investigation
5. Include Language for Sealing

c. Search Warrants Utah Rule of Criminal Procedure 40
i. Item in the possession of a 3rd Party (i.e. business records) Rule 40(c)
1. Magistrate must find that the evidence cannot be obtained by subpoena; or
2. If sought by a subpoena, the records would be concealed, destroyed, damaged, or altered
3. Magistrate shall direct conditions to protect 3rd party against unreasonable interference with normal business, protect confidential information, or constitutional rights

ii. Language to Include for Electronic Communication
1. Stored electronic records, including images, videos, pictures and communications of any kind from [date range], including account history and subscriber information, IP logs, stored electronic communications, MC addresses or device names of any devices

that were connected to the account, alternative e-mail addresses, account payment history to include credit card billing

iii. Language to Include for actual computer, digital media
    1. Computer Hardware
    2. Computer Software
    3. Passwords & Data Security Devices

VI. Search Warrant to Seize the Computer

VII. Executing the Computer Search Warrant

a. Secure the Scene
    i. Be aware that cameras may be attached to computer
    ii. Isolate the computers from remote access
        1. Phone/Cable modem
        2. Network cable/hub
        3. DSL Lines
    iii. Be conscious of wireless concerns

b. Secure the Computer
    i. Are there destructive programs running

c. Document the Scene
    i. Photograph the room, the back of the CPU, where all the devices are
    ii. Document the date/time displayed on the computer
    iii. Document any current activity on the monitor
    iv. Look for passwords nearby
    v. Whether computer is on/off and what is attached

d. Documenting Computer Data
    i. If the computer is OFF, do NOT turn it on
    ii. Don't look through files at the scene

e. System Shutdown
    i. Soft shutdown
    ii. Hard shutdown
        1. CPU – pull the power cord from back of CPU
        2. Laptops – pull the battery
        3. IPads, etc – airplane mode?

f. Interviews
    i. Ask for passwords for everything
        1. E-mail
        2. Word processor
        3. Internet access

VIII. Search Warrant to Search the Computer

a. Specify the files you will access
    i. Word documents
    ii. Image files/folders

b. Plain View Doctrine
    i. the agent must be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent.
        1. *Horton v. California*, 496 U.S.128, 136 (1990).
    ii. Examples:

1. Incriminating evidence on the screen
2. Photos
3. Names associated with files

iii. Key: The plain view doctrine does not authorize agents to open and view the contents of a container/folder/file/image that they are not otherwise authorized to open and review.

IX. Admissibility at Court

a. Foundation
   i. proposed exhibit is what it purports to be and is in substantially the same condition as it was at the time of the crime.
   ii. The party proffering the evidence is not required to eliminate every conceivable possibility that the evidence may have been altered.
   iii. State v. Wynia, 754 P.2d 667 (Utah Ct.App. 1988)

b. Hearsay
   i. Rule 803(6) Records of a regularly conducted activity
   ii. State v. Davie, 240 P.2d 265 (Utah 1952)

c. Self-Authenticating
   i. Rule 902(11) original or copy of a business record are self-authenticating
   ii. Must provide notice of intent to offer the record

d. Summaries
   i. Rule 1006
   ii. Can use if content is so voluminous that they cannot be conveniently examined in court
   iii. Must make originals available