# FBI Anchorage Tips, Tricks, & Best Practices

### *Items to retain/obtain:*

- Logs – NetFlow, PCAP, Email, Windows, Firewall, etc…
- Forensic Images – see below
- Emails
- Relationships with vendors – Some vendors retain additional data for customers that then could be accessed through vendor relation channels. Have those channels ready to participate in the investigation and/or ready to assist with law enforcement request

### *Forensic Images:*

- Get familiar with open source tools such as FTK Imager
- Be able to execute tool to create memory image and disk image of identified devices
- Talk to FBI Anchorage for instructional videos on how to make a forensically sound image if necessary.
- Useful for non-law enforcement investigations and documentation

### *Tips:*

- Engage with vendors early to be able to leverage data they might have
- If this is business email compromise involving fraudulent wire transfer initiate cyber kill chain via banking institution or law enforcement agency immediately (72 hour window)
- With infected devices, best practice for evidence collection is to leave device running. Disconnect from network via methods such as (disable ports on switch, disable NIC, if virtual machine – suspend and capture memory, if all else fails – disconnect network cable). If device is running memory forensic analysis can be done, once shut down some items may be lost.

FBI Anchorage
101 East Sixth Avenue
Anchorage, AK 99501
Phone: (907) 276-4441