**Field Exercise**

Check if it is an accident or an attack.

* Check wireshark record
* 🡺 (make a sample wireshark file, which we will read in for the field exercise)

If an attack, see if we can trace back the IP address of the attacker.

* (Make Wireshark record)
* Check Wireshark record to find out a suspicious IP addresses…

Is the attacker a group of persons? If so, can we find out their plan by investigating some digital evidence?

If we have a suspect identified, we can get an image of their computer and investigate the images using Access Data FTK

Deleted file? 🡺 can recover it using which tool?

(ex) Sending an image between them using an email or a SNS?

* (make a file: message file -> encryption -> steganography)
  + Screen captures are needed
    - Encryption/decryption
    - PKI Demo - <http://infoencrypt.com/>
* Solve it in a backward

Rescue

* (make a photo with the location information on)
  + Screen captures is needed
    - Output of the photo scavenger Hunt
    - <http://regex.info/exif.cgi>