**1. Introduction**

* For digital forensics to be an accepted science, it has to apply the scientific method.
* Follow due diligence and review all facts.
* Verification: Forensic results from the opposing team should be reviewed to verify the results.

**2. Methodology**

* There can be more than one way to approach a forensic investigation.
* Maintain consistency and accuracy:

***Do not contaminate the evidence.***

***Be objective.***

***Present the facts.***

***Give a best effort.***

* Methodology depends on the context of the case.

**3. Principles (from APCO, 2o12)**

* **Principle 1:**

No action taken by law enforcement should change data held on a computer or storage media.

* **Principle 2:**

Access to original data should be performed by a competent person who can explain their actions.

* **Principle 3:**

An audit trail or record of all processes should be created and preserved.

* **Principle 4:**

The person in charge of the investigation is responsible for adhering to the law and these principles.

**4. First Response**

* **Interviews:**

Interview co-workers, suspects, or victims. Record and date interviews.

* **Equipment:**
* response computer, dongles
* imaging devices, extension cords, camera
* paper, pen, pencil, cell phone,
* food, beverages, rags, change of clothes
* gloves, tool kit, first aid kit, network cables
* boot disks, blank CDs/DVDs
* grounding mechanism, write blockers, target drives
* flash drives, flashlight, empty bags
* tape, string, scissors, wire cutters
* magnifying glass, blanket, securing straps
* extra mouse, keyboard, suction cups

**5. Incident Response**

* **Documentation:** Use diagrams, written text, pictures, and video.
* **Inventory:** Inventory everything brought to and removed from a scene. Tag items with keyed labels.
* **Scene-specific** **considerations:** Secure the scene, photograph from multiple angles, register serial numbers and tags, secure devices for transport, look for peripheral devices, consider temperature variations during transport.
* **Imaging and previewing:** Image the RAM and hard drive, use write blockers, check BIOS settings.
* **Time:** Establish when events occurred, document managed computer clocks, modified, accessed, created, and deleted times for files.
* **Internet search history:** Determine sites visited and searches performed.
* **E-mail search:** Collect chat logs, social networking artifacts, names of users, login names, user account names, passwords, internet access types, offsite storage, installed software, security provisions, web mail, data access restrictions, instant-message screen names, destructive devices or software, social networking accounts, and other relevant information.

**6. Digital Evidence**

* Digital evidence: Reliable information that supports or refutes a hypothesis, used in scientific investigations and legal cases.