Page:
Date: / /

Search and Seizure.

Pre search activities

1. Warrant preparation
2. Plan preparation
3. Preparing toolkit
4. ~~Traditional~~ equipment
5. Computer specific equipment.

On scene activities

2. Securing the premises -
3. Scene processing -
4. Locating evidence -
5. Sizing & documentation of evidence.
6. Bagging & tagging -
7. Transportation. /

1. Warrant Preparation application.
   - Intelligence gathering is critical to the development of a comprehensive warrant.
   - When available, operating systems, storage devices & hardware ~~spec~~ specifications should be ~~available~~ included in warrant application.
   - So such articulations must that searches are tailored to the particulars of that case at hand & that evidence collected within the parameters of warrant.
   - Warrant $\xrightarrow{app^n}$ specialists $\rightarrow$ Magistrate so it should include the relevant details. In addition, all equipment, media & individuals should be added.
   - No-knock warrant should be get for exigent circumstances.
   - With the vulnerability of computer data, investigators should be able to present a case to magistrate for rapid entry if the suspect has prior

knowledge of search or if he/she has technical expertise to destroy evidence.

2. Plan Preparation.
- The plans should follow 5-paragraph military order SMEAC.

Situation : clearly define who and what of investigation no of individuals & ~~equipment~~ computer types of equipment.
geographical location

Mission : what is the optimal case scenario?
What do investigators want to happen?

Execution : How will the mission accomplished

Avenues of approach & escape : Case supervisor should provide detailed maps to investigators prior to arriving the scene which include location of doors, elevator, obstacles, parking, suspect equipments etc..

Commun^n : How will investigator communicate at scene?
to dept?
Who is primary point of contact?

3 Preparing toolkit : Computer-specific equipment & materials.

i) Multiple boot disks
used to avoid self destructive programs employed by the suspect & to minimize changes to a suspect drive (e. during routine boot process, disk space is reassigned & file/data may be overwritten.

ii) FTK Images :
Programe allows for the acquisition of physical device images. creation of simultaneous multiple image from a single source.

iii) Registry Viewer.
A utility which enables user to view windows registry files & genuate reports.

iv) Password Recovery toolkit (PRTK)
- This programe provides for the discovery and identification of encrypted files.
- This programe provides locksmithing tools for a variety of popular software like microsoft. excel etc.

v) Distributed Network Attack (DNA) - 50 client
- This programe extends decryption capabilities beyond a single computer by using the distributed power of multiple computers across a network to decrypt files and recover passwords.

vi) Wipe drive - 3.0
- Programe designed to forensically wipe drives.
- It used to Remove / wipe criminal contraband or evidences fo to reuse.

- Seizure
- Legal procedure of search and seizure comes under CrPc 93.
- There is 2 teams responsible for search & seizure.
  i) Physical search team
  - Depends upon size of crime scene and multiplicity of machines will dictate no of individuals of physical team.
  - Absolute aim of this team is to identify & secure any and all potential evidence.
  - They are not responsible for collection.

  ii) Seizure team
  - They are responsible for bagging & tagging
  - Because of the fragility of evidence experienced cyber investigators should be there.
  - They are present at commencement throughout whole processing.
  - This team comprised of seasoned investigator and a Computer expert.

==

- The Investigators should read warrant ~~first~~ thoroughly with its specification & limitations prior to its execution.
- They should maintain a copy of warrant throughout investigation.
- An item which is found appears to contain criminal evidence but it is not included in warrant, its seizure should only occur if the original warrant is formally amended.

- once the determination is made that evidence may be seized & collection process initiated with imaging (duplicated byte for byte) of drives onto a clean media.
- It is essential that this process be conducted on all hard drives prior to analysis / removal with tested forensic software packages or with clean boot disks.
- Boot disks should minimally contain any & all system drivers, applicable software, virus protection & write blocking programme.
- Verification of such images should also be conducted ~~on~~ all ~~hard~~ prior to evidence removal as forensic analysis.
- Seized computers which are on should not be turned off until the scene is photographed & properly documented.
- Current state of computer & monitor should be carefully noted prior to powering down.
- Sometimes, all open documents should copying to an external storage device.