Lecture 3: Linux Data Acquisition:

4 basic steps = CAPP – Collect, Analyze, Preserve, Present

Obtain information memory: most volatile 🡪 least volatile 🡪 nonvolatile

* Memory, swap space, network status/connection, processes running, file opening, hard drive media, removable media

Aquire RAM with physical access to the system

* Memdump for linuxm unix, FreeBSD,Solaris
* Linux Memory Extractor
* Fmem

F-Response

* Dual dongle to conduct remote forensics aquision of memory and disks.
* One dongle or subject system
* One dongle for examiner system

Disk Imaging:

* Data in forensics acquisition tool stored as image file
* 3 formats – Raw format, proprietary formats, Advanced Forensics Format (AFF)
* Advantages: fast data transfer, ignore minor data errors, most popular tools read raw format
* Disadvantages: requires as much storage as original disk
* Tools might collect bad sectors

Proprietary Format:

* Features Offered: option to compress image files, split image to smaller segmented files, integrate metadata to image files
* Disadvantages: Inability to share an image between different tools, file size limitations for each segmented volume

Advanced Forensics Tools:

* Provide compressed and uncompressed image files
* No size restriction
* Provide space in image files
* Simple design with extendibility
* Open source
* Internal consistency

Best Acquisition Method:

* Static acquisitions and live acquisitions:
* Create disk to image
* Image to image
* Local disk to disk

Write Blocker:

* Software write block – prevents writing to attached disks
* Hardware write block – physically connect

Contingency Planning:

* Copy Host protected area - hardware acquisition tool to access the drive at BIOS level
* Whole disk encryption – BitLocker

CODES TO KNOW:

Lsof – list of open files, directiory. Lsof -I [ipaddress] internet connection belonging to the given ipaddress.

Find hidden disk spaces: lsof +L1.

Netcat (cryptcat) – transfer retrieved data to a forensics workstation. Setting the netcat listener on forensics workstation: nc -l 2222 > FileName. Sending infor to the workstation: who | nc 192.168.0.2 2222

Dd – data dump – read and write from media device to create raw format file

Dd if=<what-to-copy> of=<where-to-put>, dd if=/dev/df0 | nc 192.168.1.2 2222

Bs=n (bytes) – IO blocksize of n bytes. Bs=nk(kilobytes). Larger block size can decrease imaging time

Ibs=q (input block size q (bytes)),

obs=r (output block size r (bytes))

Count = s (blocks\_ - stop after transferring s inpu blocks of data

Carving out: skip=n(input), seek=n(output)

Partition table # dd if=sda.dd skip=32(start sector) count=1884128(end sector) of=sda1.dd

If=/dev/zero of=TARGET – overwrites with zeros.

If=/dev/random of TARGET – Overwrites with random data

Nc -l 8888 > /dev/hdb – listens to port 8888 and stores

If=/dev/had | nc ipaddr 8888 -w 3 – suspect machine sends data

Dcfldd – Acquiring data, enhanced dd, specify, verify acquired data with original disk, split data

Quizlet: