**Evidence handling procedures are evolving**

Evidence handling is clearly one of the most important aspects in the expanding field of computer forensics. The never-ending innovation in technologies tends to keep best practices in constant flux in effort to meet industry needs. One of the more recent shifts in evidence handling has been the shift away from simply "pulling the plug" as a first step in evidence collection to the adoption of methodologies to acquire evidence "Live" from a suspect computer.

The need for changes in digital evidence collection are being driven by the rapidly changing computing environment:

* Applications are installed from removable media such as a USB stick and are then virtualized in RAM without a trace on the hard disk
* Root kits hide within process undetected by the underlying operating system and when using local tools (binaries) ? you must analyze memory with trusted binaries
* Malware is fully RAM resident with no trace of existence on the hard disk
* Users regularly utilize covert / hidden encrypted files or partitions - areas of the hard drive to hide evidence
* Popular web browsers offer the user the ability to cover their tracks ? log files of user activity are created but deleted when the browser is closed
* Web 2.0 continues to change the landscape with web based email, blogs, wiki's and twitter extending storage of user actions / communications beyond the traditional hard disk found on the users machine.

**An Introduction to Live Digital Evidence Collection**

Effectively Live forensics provides for the collection of digital evidence in an order of collection that is actually based on the life expectancy of the evidence in question. Simply put in all likelihood perhaps the most important evidence to be gathered in digital evidence collection today and for the foreseeable future exists only in the form of the volatile data contained within the computers RAM.

Order of volatility of digital evidence

1. CPU, cache and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system / swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media

**An accepted best practice in digital evidence collection - modified to incorporate live volatile data collection.**

Stand Alone Home Computer

*For proper evidence preservation, follow these procedures in order (Do not use the computer or search for evidence)*

1. Photograph the computer and scene
2. If the computer is off do not turn it on
3. If the computer is on photograph the screen
4. Collect live data - start with RAM image (Live Response locally or remotely via F-Response) and then collect other live data "as required" such as network connection state, logged on users, currently executing processes etc.
5. If hard disk encryption detected (using a tool like Zero-View) such as full disk encryption i.e. PGP Disk ? collect "logical image" of hard disk using dd.exe, Helix - locally or remotely via F-Response
6. Unplug the power cord from the back of the tower - If the computer is a laptop and does not shut down when the cord is removed then remove the battery
7. Diagram and label all cords
8. Document all device model numbers and serial numbers
9. Disconnect all cords and devices
10. Check for HPA then image hard drives using a write blocker, Helix or a hardware imager
11. Package all components (using anti-static evidence bags)
12. Seize all additional storage media (create respective images and place original devices in anti-static evidence bags)
13. Keep all media away from magnets, radio transmitters and other potentially damaging elements  
    Collect instruction manuals, documentation and notes
14. Document all steps used in the seizure

* Note: \* If computer is x64 the author recommends collecting the image of RAM using HBGary FastDump Pro