**Module 5 Risk Management**

**5.5 Forensics**

**Strategic Intelligence/Counter-intelligence**

* Gathering of information/data regarding incident
* Nature of threat actor/source/vector
* Pull from multiple data sources (internal & external)
* Use of active logging

**Order of Volatility**

* Order for collecting evidence
* Volatile data easily/quickly lost

1. Resident computer memory
2. Caches/temporary storage
3. Physical media (USB)

* Capture data that will be lost first
* Accomplished during incident identification

**Chain of Custody**

* Provides clear record of path evidence taken from acquisition to disposal (See NIST definition)
* Any items taken must be secured to preserve its integrity (Eg. Faraday bag)
* Documentation/tracking form
* Evidence must be

1. Admissible
2. Authentic
3. Complete
4. Reliable
5. Believable

**Legal Hold**

* Preservation on all forms of relevant information when litigation reasonably anticipated
* Request to not destroy what might be relevant to legal matter

**Data Acquisition**

* Capture system image
* Network traffic & logs
* Record time offset
* System hashes
* Screenshots
* Interview witnesses

**System Image Capture**

* System image is snapshot of what exists
* Capturing image of OS in its exploited state

1. Legal
2. Helpful in revisiting issue after the fact to learn more about it

* Performed in several ways

1. Disk to disk – physical media, original to copy
2. Disk to an image file – physical to logical (VM)
3. Image file to disk – logical to physical

* Use of write-blockers on original media
* Tools – Encase, Forensics Toolkit, Native Linux command (dd)

**Network Traffic & Logs**

* Capture logs from static network systems

1. Virtual machines
2. Firewalls, IDS, VPN, routers, switches
3. Servers
4. Access
5. Security Incident & Event Management (SIEM)/Centralised logging systems

* Active network scanning (on live systems) – Wireshark

**Record Time Offset**

* Coordinating time to accurately track events
* NTP (Network Time Protocol) – synchronises time
* Time zone difference

**Take Hashes**

* Hash – unique “fingerprint” of system files/data
* Tracks integrity/any changes – hash value will change if file changes
* *National Software Reference Library (NSRL)* – to collect “known traceable software apps” through hash values & store them in a Reference Data Set (RDS) (see [www.nsrl.nist.gov](http://www.nsrl.nist.gov))

**Screenshots**

* Images on computer screen
* Tools – Alt + PrtScn buttons, Windows Snipping Tool/Snag-it
* Used as evidence

**Interview Witnesses**

* List of people contacted/asked about incident
* Who you interviewed, including names, contact information (email, phone, address) & what they saw (when, where & how)
* Should be conducted with legal &/or HR

**Documentation/Track Hours**

* Document everything
* Written narrative
* When & what was done
* Evidence
* Images
* Pictures/video
* Calculating number of man-hours & other related expenses