Incident Response Jumpkit Checklist

- ☐ Contact information (and backups)
  - IRT members
  - Other internal stakeholders
  - External stakeholders
- ☐ Pagers or cell phones (+ spare batteries and chargers)
- ☐ Laptop
  (Lots of RAM, a large hard drive and pre-loaded with forensics applications)
- ☐ Virtual machine software (e.g., Virtual Box, VMware)
- ☐ Live CDs of various types.
  - BitDefender
  - GMER
  - Kali Linux Live
  - Trend Micro RescueDisk
- ☐ DVDs or CDs with trusted, statically linked versions of programs to be used to gather evidence from systems
- ☐ Packet sniffers and protocol analyzers
- ☐ Encryption software
- ☐ Blank media (e.g., floppy disks, CD-Rs, and DVD-Rs)
- ☐ USB thumb drives (16 and 32 GB drives)
- ☐ A network hub or a tap. A tap would be better, but they cost more
- ☐ Write blocking device(s) to use when imaging hard drives or other media
- ☐ One or more external hard drives
- ☐ Tools:
  - Screwdrivers
  - Flashlight
  - Tweezers
  - Telescoping magnet
  - Multitool
  - Duct tape
- ☐ USB to serial port adapter
- ☐ Network cables (Straight and crossover or crossover adapter)

- ☐ Hard drive jumpers
- ☐ Cisco rollover cable
- ☐ Serial cable
- ☐ Female to female RJ45 connector
- ☐ Hard-bound notebooks with numbered pages
- ☐ Digital camera
- ☐ Audio recorder
- ☐ Forms:
    - Critical Log Review Form
    - Incident Questionnaire Cheatsheet
    - Incident Reporting Form
    - Incident Survey Cheatsheet
    - Chain of Custody Form
- ☐ Evidence storage bags and tags, and evidence tape (Amazon.com has these items)
- ☐ Desiccants for protecting against moisture in the bags
- ☐ Port lists (including commonly used ports and Trojan horse ports)
- ☐ Cryptographic hashes of critical files to speed the analysis, verification, and eradication of incidents
- ☐ Media, including OS boot disks and CD-ROMs, OS media, and application media
- ☐ Security patches from OS and application vendors
- ☐ Pens
- ☐ Sharpie markers

Source: Based on list from https://www.paladinsec.com/preparing-for-incident-response/