

Virginia Tech IT Security Office Incident Response Kit

November 29, 2006

Contents:

- Write-blocking Set with the following adapters
 - <http://www.forensicpc.com/proddetail.asp?prod=UWBK>
 - Parallel ATA: 3.5", 2.5", 1.8" hard drives
 - Serial ATA
 - SCSI: 50-pin, 68-pin, 80-pin
 - USB drives
 - Memory cards
 - Read / write ATA adapter for target drive
- Blank 250GB ATA (IDE) 3.5" hard drive
- Dual boot Laptop PC (Windows and Linux)
 - 2GB memory
 - Common software installed such as Office and networking tools
- Network data logger
- ATA, SATA, 2.5" hard drive to USB adapter (read / write)
- Multiple format memory card reader (read / write)
- 10/100 Ethernet tap
- Ethernet cables – short and long
- 120GB 2.5" USB drive
- 1GB USB flash drive
- USB floppy drive
- USB DVD±RW drive
- Surge Protector
- Portable printer with battery
- Hand tool kit
 - http://catalog.belkin.com/IWCatProductPage.process?Product_Id=11788
- Office Supplies
 - Incident handling forms
 - Current contacts list
 - Pens, pencils, Sharpie
 - Clipboard
 - Small notepad
 - Lab notebook
 - Printer paper
 - 9 x 12 envelopes
 - Anti-static bags
 - Evidence bags / tape
- 8-port Ethernet hub (repeater)
- AUI – 10BaseT transceiver
- Software
 - Helix CD, BackTrack CD, SANS 504 CD
 - Ghost CD, Nero CD, printer driver CD
 - Blank CDRs and DVDRs

10/100 Ethernet Tap

Parts list:

- Ethernet coupler
- Short Ethernet cable (3ft)



Network Data Logger

Parts list:

- Mainboard – Mini ITX
http://www.logicsupply.com/product_info.php/products_id/540
- Daughter board – 3 x 1Gb network card
http://www.logicsupply.com/product_info.php/products_id/495
- Compact Flash adapter
http://www.logicsupply.com/product_info.php/products_id/100
- 2.5" hard drive adapter
http://www.logicsupply.com/product_info.php/products_id/165
- AC power supply – 110W, 12V output
http://www.logicsupply.com/product_info.php/products_id/182
- ATX power supply – PicoPSU, 120W
http://www.logicsupply.com/product_info.php/products_id/505
- 8" LCD touch screen
<http://store.mp3car.com/ProductDetails.asp?ProductCode=MON%2D005>
- Aluminum enclosure – 7"x9"x2"
<http://www.mouser.com/search/refine.aspx?Ntt=563-AC-406>
- Adhesive PCB mounts (4)
<http://www.mouser.com/search/refine.aspx?Ntt=561-LAD187>

Additional items that can be found more commonly:

- 1GB DDR2 400 memory
- 2.5" hard drive – for data storage
- 1GB Compact Flash (very fast type, like the SanDisk Ultra II)
- Pelican 1200 Case

