NebraskaCERT CSF

Free Forensic Tools!

November 19th, 2008

By: Matt Churchill

CONTINUUM WORLDWIDE™

Categories

- Image
- Carve
- Analyze
- Memory
- Virtualization
- Live CDs
- Misc
- Resources

Image

- FTK Imager
  - http://www.accessdata.com/downloads.html
- Forensic Acquisition Utilities (FAU)
  - http://gmgsystemsinc.com/fau/
- Various DD flavors
- Various Live CDs

Carve

- WinHex
  - http://www.x-ways.net/winhex/
- PhotoRec
  - http://www.cgsecurity.org/wiki/PhotoRec
- Scalpel
  - http://www.digitalforensicssolutions.com/Scalpel/

Analyze

- ProDiscover Basic
  - http://www.techpathways.com/DesktopDefault.aspx?tabindex=9&tabid=14
- TSK & Autopsy
  - http://www.sleuthkit.org/
- PTK
  - http://ptk.dflabs.com/

Analyze

- WinHex
  - http://www.x-ways.net/winhex/
- PyFlag
  - http://www.pyflag.net/cgi-bin/moin.cgi
- SANS Forensic VM
  - Available to SANS portal members
- FTK demo (up to 5000 items)
  - http://www.accessdata.com/downloads.html

CONTINUUM WORLDWIDE™

Memory

- mdd
  - http://sourceforge.net/project/showfiles.php?group_id=228865
- win32dd
  - http://win32dd.msuiche.net/
- Volatility
  - https://www.volatilesystems.com/default/volatility
- Memoryze
  - http://www.mandiant.com/software/memoryze.htm

Virtualization

- Excellent Description:
  - http://windowsir.blogspot.com/2007/03/mounting-dd-image.html
- LiveView
  - http://liveview.sourceforge.net/
- ProDiscover
  - http://www.techpathways.com/DesktopDefault.aspx?tabindex=9&tabid=14
- VDKWin
  - http://petruska.stardock.net/Software/VMware.html

Live CDs

- Helix
  - http://www.e-fense.com/helix/
- CANE
  - http://www.caine-live.net/en/index.html
- PlainSight
  - http://www.plainsight.info/download.html
- BackTrack (will mount drives, but has forensic tools)
  - http://www.remote-exploit.org/backtrack.html

Misc

- RegRipper
  - http://regripper.net/
- Forensic CaseNotes
  - http://www.qccis.com/?section=casenotes
- NirSoft Tools
  - http://www.nirsoft.net/
- Historian
  - http://www.mandiant.com/software/webhistorian.htm
- Windows File Analyzer
  - http://www.mitec.cz/wfa.html

Resources

- http://nehtcia.org
- http://windowsir.blogspot.com
- http://forensicir.blogspot.com
- http://sansforensics.wordpress.com
- www.ForensicFocus.com
- www.E-Evidence.info
- www.google.com

Questions?

- **Matt Churchill**
  - 402.916.1825
  - matthew.churchill@continuumww.com
  - Or… mc@cops.org


CONTINUUM
WORLDWIDE℠