Some good books

Detecting lies and deceit but Aldert Virij
Confidential by John Nolan
The good news about marriage by Shaunti Feldhahn
The signal and the noise by Nate Silver
Unbroken by Laura Hlllenbrand
The cuckoo's egg by Clifford Stoll
How to write an expert witness report by James Mangaviti,…
International handbook of threat assessment edited by J Reid Meloy and Jens Hoffman

Forensic tools that I like

X-Ways Forensics – analysis of forensic images

Relatively inexpensive, dependable, easy to run from removable media. http://www.x-ways.net/forensics/

Omnipeek – forget trying to get Wireshark filters to work

Great GUI, especially helpful diagnosing problems, e.g., effects of jitter in VOIP. Quick look at environment to spot NetBIOS file sharing. https://www.savvius.com/ or if your DNS server doesn't like new domains go to http://www.wildpackets.com/

Internet Evidence Finder – extract artifacts from an image

Works on images or live connections to phones or computers. Takes hours to analyze all artifacts. Can select desired artifacts for a quick check. https://www.magnetforensics.com/

CRU Ditto –image/clone creation

Reliable hardware to image hard drives. Includes dd-rescue in latest firmware. http://info.cru-inc.com/ditto-firmware-update

CRU mouse jiggler – stopping screensaver timeouts

Prevents screensaver actuation keeping user logged in. http://www.cru-inc.com/products/wiebetech/

Key Ghost – keyloggers

For collecting passwords and investigating activity that doesn't show up on the hard drive. Caution: must comply with policy and law. Beware of non-repudiation issues and their effect on your investigation. Clunky website, good product. http://keyghost.com/

Dr. Gordon Mitchell www.eSleuth.com (888) eSleuth enquiries15@eSleuth.com

Cellebrite – for phone/tablet investigations

The standard for investigating phones. http://www.cellebrite.com/Mobile-Forensics

Grabinfo – a batch file, ask me for a free copy

A collection of common utilities that can be used to preserve data from live PCs. Gets volatile things like RAM contents, open ports, logged in users. Write Gordon for a copy. Enquiries15@esleth.com. See more about us at www.eSleuth.com or call (888) eSleuth.

X1 Social Discovery – archive social media

A better way to preserve social media than just taking screen shots.
http://www.x1.com/products/x1_social_discovery/

Windows FE – a forensically sound boot system, thanks Troy Larson and Brett Shavers!

Build from Win PE, complex process, easy boot disk usage. https://winfe.wordpress.com/

Quick View Plus – look through lots of app files fast

Makes looking at files as easy as using Windows Explorer. Important for cases with lots of data in MS Office or .pdf formats.
http://www.avantstar.com/metro/home/Products/QuickViewPlusStandardEdition

Nir Sofer's applications – do stuff that is amazing in live acquisitions

NirSoft.com has a great collection of utilities; be sure to download the command line versions too. Add what you need from these to Grabinfo.bat. http://www.nirsoft.net/

Sysinternals – small company innovation from a big company, amazing

Mark Russinovich has produced an incredible collection of Windows utilities. My favorites are Autoruns, Process Explorer, Process monitor, TCPView. https://technet.microsoft.com/en-us/sysinternals/

Dealing with threats

Find out how the threat assessment team on your campus works. Explain to them that you can help with factual information that can greatly assist in the evaluation of threats. Think about joining them.

Make sure that policy is configured to allow investigations of all machines on your network … yes, even BYOD hardware. Archive hard drives used by fired employees.

You know where to find crucial information, preserve it! Go for the volatile data.

- Live acquisitions from endpoints, servers, network
- Access control logs
- Stored video

Look up your local chapter of the Association of Threat Assessment Professionals
http://www.atapworldwide.org/?page=25

G Mitchell

Digitally signed by G Mitchell
DN: c=US, cn=G Mitchell, email=gmit@eSleuth.com
Date: 2015.09.27 05:11:44 -07'00'

Dr. Gordon Mitchell www.eSleuth.com (888) eSleuth enquiries15@eSleuth.com