Favorite resources for Windows event logs and some other documents I created:

1. Fairly comprehensive list of useful logs for an investigation Jack Voorhees pointed out

<https://www.malwarearchaeology.com/cheat-sheets>

1. If you’re interested in grabbing specific event IDs for a hunt and want to easily search the data with Pandas this is a good article on how to grab those events from a host

<https://blogs.technet.microsoft.com/ashleymcglone/2013/08/28/powershell-get-winevent-xml-madness-getting-details-from-event-logs/>

1. Document I wrote for useful event IDs and which Echo index they are located in. Also has a few links for useful articles on some of the event IDs.



1. Document I wrote for finding hidden searchable fields in Echo specific to Windows event logs



1. This is a great article Derek V. wrote up on searching event logs in Arcsight. Very useful if you can’t find what you’re looking for in Echo.

<https://cdn1-cloud.atlassian.net/wiki/spaces/TH/pages/739998/Finding+Logs+in+Arcsight>

Favorite resources for getting better acquainted with the Windows Registry:

1. Amazing blog that has other resources to check out, and lists several forms of persistence. <http://www.hexacorn.com/>
2. Article about amcache on a blog with other good forensic resources

<https://binaryforay.blogspot.com/2017/10/amcache-still-rules-everything-around.html>

Favorite resources for getting started with malware analysis:

1. Decent article with links to more for those looking to get started with malware analysis

<https://zeltser.com/mastering-4-stages-of-malware-analysis/>

1. An introduction to assembly

<https://www.youtube.com/watch?v=wLXIWKUWpSs>

1. For when you’re ready to start looking at assembly

<https://malwareunicorn.org/#/workshops>

1. IDA cheat sheet

<https://www.hex-rays.com/products/ida/support/freefiles/IDA_Pro_Shortcuts.pdf>

1. X64dbg documentation

<https://x64dbg.readthedocs.io/en/latest/commands/>

1. To find samples to practice malware analysis on

<https://zeltser.com/malware-sample-sources/>

1. Another good idea when starting RE is to practice compiling programs and disassembling them. It will help getting used to looking at assembly. Try this video on C, or go with a language that’s comfortable. Maybe talk to Andrew Orr or Adam Lesperance for more resources on this too

<https://www.youtube.com/watch?v=KJgsSFOSQv0>

https://godbolt.org/

1. Try these crackmes while building RE skills

<https://crackmes.one/>

<https://reverseengineering.stackexchange.com/questions/15774/crack-me-material>

1. Another book to read, when you want to try and crack windbg and feel confident in your skills, Practical Reverse Engineering by Bruce Dang. Windbg cheat sheet:

<https://oalabs.openanalysis.net/2019/02/18/windbg-for-malware-analysis/>

1. Yara- check out the yara docs off this page

<https://virustotal.github.io/yara/>

Favorite resources for Mac:

Jack and Megan

<https://cdn1-cloud.atlassian.net/wiki/spaces/CP/pages/511816/macOS+analysis+checklist>

<https://cdn1-cloud.atlassian.net/wiki/spaces/CP/pages/512892/Scoping+for+lateral+movement+on+macOS>

Resources for using PowerShell with Exchange

1. <https://practical365.com/powershell/>
2. <https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/exchange-online-powershell-v2/exchange-online-powershell-v2?view=exchange-ps>
3. Heikkila

Miscellaneous:

Decent book for new EAs on Safari: Digital Forensics and Incident Response by Gerard Johansen (2017)

DFRWS- great forensics conference with a few workshops- covers memory too

OSFDFCON- good conference for forensics that covers open source tools

Might be partial, but Focal Point classes

RECON- amazing Reverse Engineering conference, and a great place to make very smart contacts

Converge- Tanium conference- ask Fred Nolte or Rob Dean about this one

Favorite books to reference all the time on Safari- Windows Internals and Art of Memory Forensics

For a fun way to get more familiar with Regex: <https://regexcrossword.com/>

Not finding what you’re looking for in here, try searching #malware or #dfir. So many good blogs and articles can be found doing that.

These guys put out pretty interesting videos, mostly on ransomware, but definitely worth checkout out: <https://www.youtube.com/channel/UCykrmYP5ANJFWGWJckUJlAA>