Community: Cheat Sheets

NEW - Plaso Filtering Cheat Sheet - This cheat sheet is aimed to be a reference on the filtering options available with each of the Plaso tools. Although there is some overlap in filtering options across the various tools, there are also filtering options that are unique to a specific tool. There are also filtering options that are not widely documented and are shown here. There are some lists of items, such as data types, that are not shown in their entirety. Complete Lists can be found at: https://github.com/mark-hallman/plaso_filters

Download Here

NEW - Tips for Reverse-Engineering Malicious Code - This cheat sheet outlines tips for reversing malicious Windows executables via static and dynamic code analysis with the help of a debugger and a disassembler.

Download Here

NEW - REMnux Usage Tips for Malware Analysis on Linux - This cheat sheet outlines the tools and commands for analyzing malicious software on the REMnux Linux distribution

Download Here

Yes, Please!

NEW - Cheat Sheet for Analyzing Malicious Documents - This cheat sheet presents tips for analyzing and reverse-engineering malware. It outlines the steps for performing behavioral and code-level analysis of malicious software.

Download Here

NEW - Malware Analysis and Reverse-Engineering Cheat Sheet - This cheat sheet outlines tips and tools for analyzing malicious documents, such as Microsoft Office, RTF and Adobe Acrobat (PDF) files

Download Here

NEW - SQlite Pocket Reference Guide - This guide is a supplement to the SANS FOR518: Mac Forensic Analysis and SANS FOR585: Advanced Smartphone Forensics courses as well as enhances concepts covered in other courses such as FOR500 Windows Forensics Analysis. It covers some of the core methods to extracting data from SQLite databases. Definitions, sample queries, and SQLite terminology will help you conduct manual extractions from databases of interest found on Macs, Smartphones, and PCs.

Download Here

NEW! - Eric Zimmerman's tools Cheat Sheet - SANS FOR508 Digital Forensics, Incident Response & Threat Hunting course Instructor and Former FBI Agent Eric Zimmerman has provided several open source command line tools free to the DFIR Community. These open source tools can be used in a wide variety of investigations including cross validation of tools, providing insight into technical details not exposed by other tools, and more. Eric's first Cheat Sheet contains usage for tools for lnk files, jump lists, prefetch, and other artifacts related to evidence of execution. This suite of tools allows for displaying relevant forensic data including exporting data to many commonly used formats.

To download Eric's free tools visit: https://ericzimmerman.github.io/

Download Here

Rekall Cheat Sheet - The Rekall Memory Forensic Framework is a robust memory analysis tool that supports Windows, Linux and MacOS. It has distinctly unique syntax and plugin options specific to its features and capabilities. This cheat sheet provides a quick reference for memory analysis operations in Rekall, covering

acquisition, live memory analysis and parsing plugins used in the 6-Step Investigative Process. For more information on this tool, visit rekall-forensic.com.
Download Here

SIFT Cheat Sheet - Looking to use the SIFT workstation and need to know your way around the interface? No problem, this cheat sheet will give you the basic commands to get cracking open your case using the latest cutting edge forensic tools.
Download Here

Linux Shell Survival Guide - This guide is a supplement to SANS FOR572: Advanced Network Forensics and Analysis. It covers some of what we consider the more useful Linux shell primitives and core utilities. These can be exceedingly helpful when automating analysis processes, generating output that can be copied and pasted into a report or spreadsheet document, or supporting quick-turn responses when a full tool kit is not available.
Download Here

Windows to Unix Cheat Sheet - It helps to know how to translate between windows and unix. This handy reference guide ties together many well known Unix commands with their Windows command line siblings. A great way to get Windows users familiar with the command line quickly.
Download Here

Memory Forensics Cheat Sheet - Few techniques get you to root cause faster than memory forensics. This cheat sheet walks the investigator through a six step analysis process, illuminating the most popular and powerful Volatility memory analysis plugins in each step. Memory acquisition, memory timelining, and Windows registry analysis plugins are also noted. Useful for those just starting out in memory forensics and seasoned pros looking to quickly remember Volatility plugin syntax.
Download Here

Hex and Regex Forensics Cheat Sheet - Quickly become a master of sorting through massive amounts of data quickly using this useful guide to knowing how to use simple Regex capabilities built into the SIFT workstation.
Download Here

Developing Process for Mobile Device Forensics (Det. Cynthia A. Murphy)- With the growing demand for examination of cellular phones and other mobile devices, a need has also developed for the development of process guidelines for the examination of these devices. While the specific details of the examination of each

device may differ, the adoption of consistent examination processes will assist the examiner in ensuring that the evidence extracted from each phone is well documented and that the results are repeatable and defensible.
Download Here


Figure 1: Evidence Extraction Process

SANS FOR518 Reference Sheet - This cheat sheet is used to describe the core functions and details of the HFS+ Filesystem.
Download Here

Latest Blog Posts

A few Ghidra tips for IDA users, part 1 - the decompiler/unreachable code
April 16, 2019 - 2:59 PM

A few Ghidra tips for IDA users, part 0 - automatic comments for API call p [...]
April 16, 2019 - 2:40 PM

SANS Threat Hunting and Incident Response Summit 2019 Call for Speakers – D [...]

Latest Tweets @sansforensics

Really hands-on! A piece of technical information is discus [...]
April 19, 2019 - 7:20 PM

Watch @DavidJBianco discuss the best ways to evaluate the qu [...]
April 19, 2019 - 2:20 PM

. @hexacorn Blog: Installers - Interactive Lolbins, Part 2 h [...]

Latest Papers

Evidence of Data Exfiltration via Containerised Applications on Virtual Private Servers
By Seth Enoka

Using Image Excerpts to Jumpstart Windows Forensic Analysis
By John Brown

Windows 10 as a Forensic Platform
By Ferenc Kovacs

April 08, 2019 - 7:31 PM

April 19, 2019 - 1:16 AM

"Rob has insight that few others have and that alone is worth the cost of the the course."
- Chris Spurrier, Xerox Corp

"This course is valuable to Law Enforcement professionals that conduct computer crime investigations."
- Reggie Harris, Federal Agent - DPE, OIG

"Rob Lee is a master of the subject matter. The material is presented in a way that is understandable. Rob is also charismatic enough to make the course enjoyable."
- Erik Ketlet, JP Morgan Chase