



SiLK and the Virtual Training Environment

**George Warnagiris
(Presenter: Markus De Shon)
FloCon 2010**



Goals

Enable remote training delivery

Modularize for maintainability

Standardize across target audiences

Transition as widely as possible

Scale best-practice training to all students

The Virtual Training Environment

Adobe Presenter-based

- Plays using standard Adobe Flash plugin

Slides

- Must be PowerPoint

Audio (MP3)

Video (if available)

Transcription or script

Virtual lab environment

- VMware images
- Virtual network
- Reuse/enhance standard system images where possible

Lessons learned so far

Distributed module development grouped by common theme is possible

- Need project lead to keep organized
- Results can be of uneven quality
- Helps identify best training developers
- Permits rapid development/update

Labs end up decoupled from lectures

Different target audiences require different data sets

Future efforts

Greater utilization of best trainer(s)

Update to keep pace with software releases

Additional tools

- iSiLK
- Visualization

Training access

VTE <https://www.vte.cert.org/>

SiLK course links <http://tools.netsa.cert.org/>



My Profile

About this Page

The list of topics and content items in this course are listed to the right. By clicking on the content item, you can retrieve information about and launch the class material.

Functions

-- User --

- [My VTE](#)
- [My Profile](#)
- [My Courses](#)
 - [Using Einstein for Network Traffic Analysis](#)
- [My Training History](#)

Course View

Using SiLK for Network Traffic Analysis

Description: Using SiLK for Network Traffic Analysis Description

Progress: (100%)

[Print Progress Report](#)

Duration: 3 Hours

Instructor:

[Course Certificate](#)

Office Hours:

[Virtual Office](#)

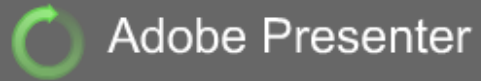
Support Forum:

[Access Forum](#)

Using SiLK for Network Traffic Analysis

- [-] Introduction to Using SiLK
 - [-] Network Flow [C]
 - [-] SiLK Beginning Flow Analysis [C]
- [-] Basic Tools
 - [-] rfilter [C]
 - [-] Counting Tools: rwcoun, rwstats, rwuniq [C]
 - [-] rwappend-rwsplit [C]
 - [-] rwfileinfo-rwglob [C]
 - [-] rwcun and rwcun [C]
 - [-] rwsort [C]
- [-] Advanced Tools
 - [-] Sets [C]
 - [-] Prefix Maps (pmaps) [C]
 - [-] Advanced SiLK Tools: Bags [C]
 - [-] Using Tuples with SiLK [C]
- [-] SiLK Summary

Details





```

silk@training932:~
login as: silk
silk@10.0.1.9's password:
Last login: Fri Apr 24 15:40:08 2009
[silk@training932 ~]$
[silk@training932 ~]$
[silk@training932 ~]$
[silk@training932 ~]$ rw
rwaddrcount      rwfileinfo      rwpackchecker   rwsetcat
rwallformats    rwfilter        rwpmapbuild     rwsetintersect
rwappend         rwflowappend   rwpmapcat       rwsetmember
rwbag            rwflowpack     rwrandomizeip   rwsettool
rwbagbuild       rwgeoip2ccmap  rwreceiver      rwsetunion
rwbagcat         rwgroup        rwresolve       rwsort
rwbagtool        rwguess        wrtd2split      rwsplit
rwcats           rwidquery      rwscan          rwstats
rwcats           rwip2cc        rwscanquery    rswapbytes
rwcats           rwmatch        rwsender        rwtotal
rwcats           rwnetmask      rwset           rwtuc
rwcats           rwp2yaf2silk  rwsetbuild     rwuniq
[silk@training932 ~]$ rw

```

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.