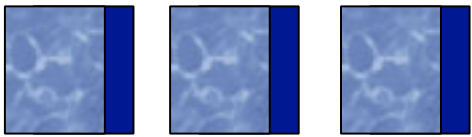
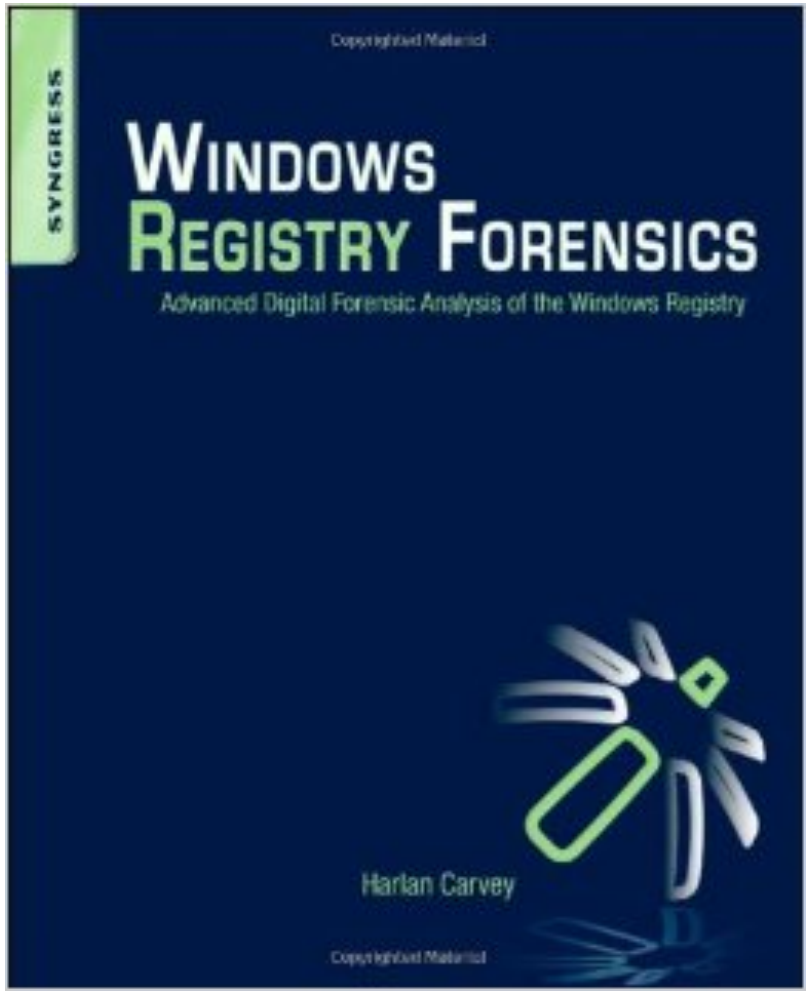
What's new in RegRipper

OSDFCon 2014

H. Carvey
keydet89@yahoo.com

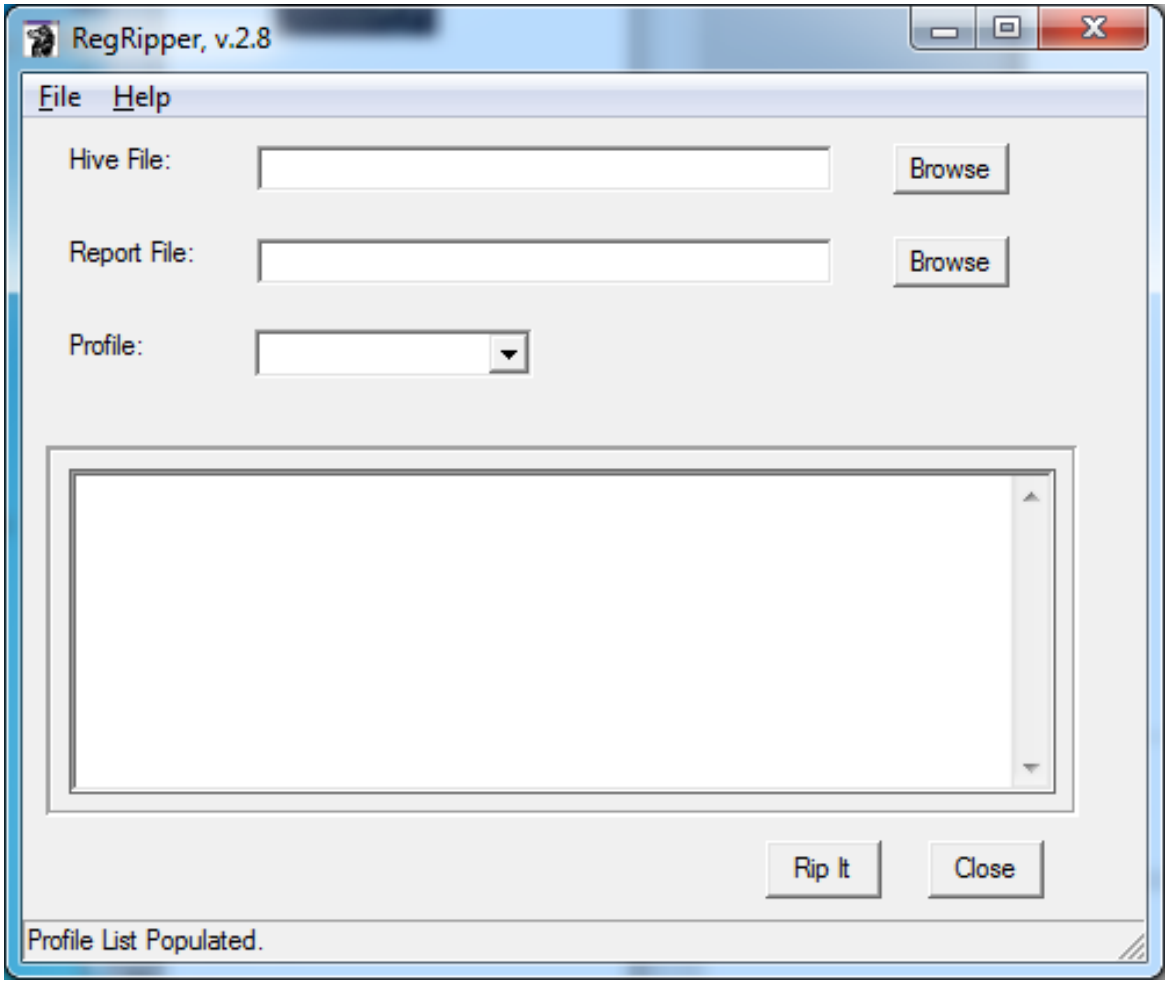


Brief Intro


SYNGRESS
WINDOWS
REGISTRY FORENSICS
Advanced Digital Forensic Analysis of the Windows Registry
Harlan Carvey

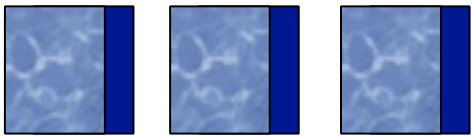
RegRipper

- GUI
- Command line
- Plugins?
- Profiles?



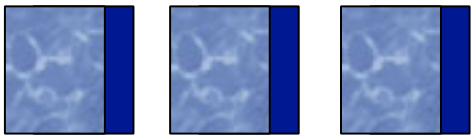
What's new

- Github - *https://github.com/keydet89*
- Contest - http://windowsir.blogspot.com/2014/10/wrf-2e-contest.html
- Plugins



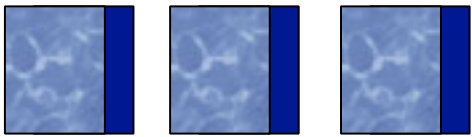
What's coming

- Consolidate plugins
  - Code to check "Run" key in Software and NTUSER.DAT hives is similar enough to have one plugin
- Output Options
  - "Regular", TLN, CSV
- "Fixing" alerts
  - Output a rating, rather than multiple alerts
- Artifact Categories



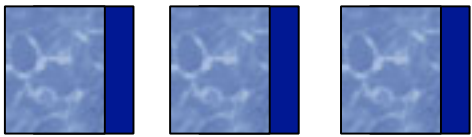
Getting the most out of RegRipper

- Do more than just run the tool
  - Goals
  - Iterative analysis process
  - Find “new” stuff
  - Verify/validate other stuff



Thanks

- Thanks to the work of:
  - Eric Zimmerman – Shellbag Explorer
  - Dan Pullega – Shellbags blog post
  - Joachim Metz – Shellbag documentation
  - Corey Harrell – All around great guy!



Questions?

keydet89@yahoo.com

http://windowsir.blogspot.com