

# Building your own U3 launch-able Windows Forensic ToolKit

## Mocha Forensics

By: Jason Kendall  
For Sector 2010

# About Me

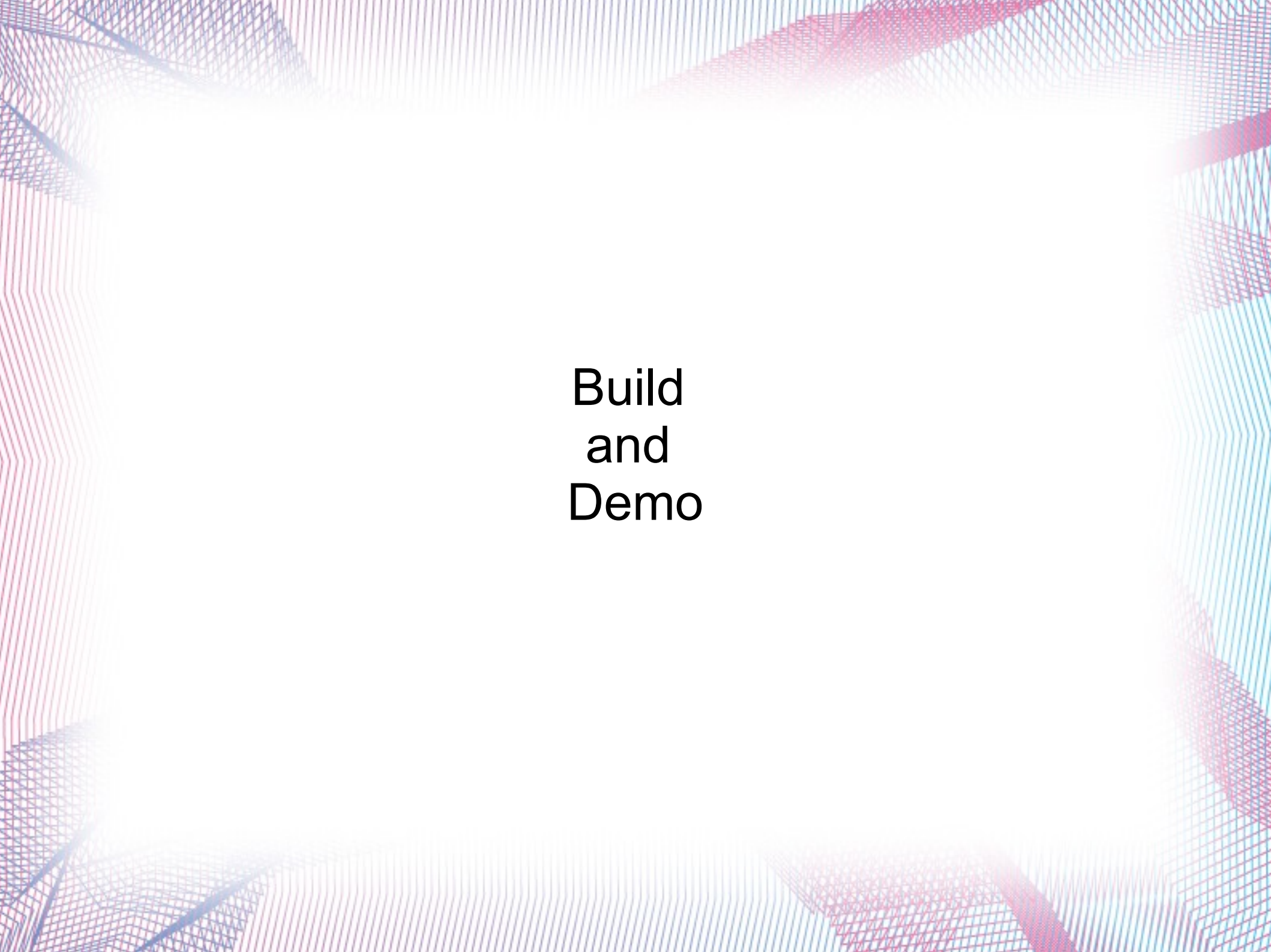
- Information Security Generalist SME
- Senior Security Analyst for a Top 5 Bank in Canada
- Looking to ride the next wave of Cyber Attacks
- Email: [jason.kendall@ostlabs.com](mailto:jason.kendall@ostlabs.com)
- Twitter: CoolAcid

# The Tool Set

- Binds tools together to be placed on a U3 auto-running USB drive to gather forensic data from a running windows system
- Uses the Windows Forensic Toolkit by Fool Moon Software & Security
- Multiple Utilities usually found with WFT
- Short URL to Project - <http://www.shurl.ca/16>

# Caveats and Next Steps

- Normal U3 Drive limitations: Must have cdrom auto-run enabled, Windows machine must not be locked
- Need to rewrite the .bat file and .vbs file as one file
- Add more options that are easy to configure
- Figure out the licensing of the extra software and see what I can re-distribute or link to

The background features a complex, abstract pattern of thin, overlapping lines in red and blue. These lines form a series of interconnected, slightly offset rectangular and square shapes, creating a 3D wireframe effect. The lines are most dense at the corners and become sparser towards the center, where the background is a plain, light color.

# Build and Demo