OMG THE KILLER IS STILL IN THE HOUSE!!!1!!11

Or: The Shift From Traditional Forensics to Live Response

NKU IMI Security Symposium
October 15, 2010

About Your Speaker

When you think of forensics...

Unplug, Image, Analyze, Repeat

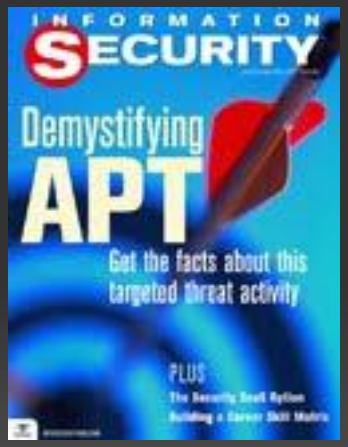
Forensics is *not* dead.

The threat landscape has changed.

They're after your data.

They're hard to find.

The new IDS…



A new buzzword appears!

Traditional forensics don't work here.

We need a new set of tools.

Monitor your environment.

Observe the attacker.

Analyze their tools & techniques.

Share what you find.

Arm yourself.

Questions?

Justin Hall
Security Architect, CBTS
justin.hall@cbts.cinbell.com