Effective Digital Forensics Research is Investigator-Centric

Robert J. Walls  Brian Neil Levine  Marc Liberatore  Clay Shields
University of Massachusetts Amherst  Georgetown University
Digital forensics contends with the CSI-effect.
Digital forensics contends with the CSI-effect.
Digital forensics lacks a solid scientific foundation.
Digital forensics struggles with \textcolor{orange}{practical} challenges.
Digital forensics impacts people directly.
Security, privacy, & forensics?
5 principles for researchers.
Digital Forensics is Investigator-Centric
1: Forensics is Investigator-Centric

> Research is investigator driven.
1: Forensics is Investigator-Centric

> Research is investigator driven.

> Consider both goals and constraints.
1: Forensics is Investigator-Centric

> Research is investigator driven.

> Consider both goals and constraints.

> Break the rules lose the case.
1: Forensics is Investigator-Centric

> Research is investigator driven.
> Consider both goals and constraints.
> Break the rules lose the case.
> The rules change.
Forensics and law are inseparable.
2: Forensics and law are inseparable

> Law is struggling to keep up.
Forensics and law are inseparable

> Law is struggling to keep up.

> How does seizure apply to data?
2: Forensics and law are inseparable

> Law is struggling to keep up.
> How does seizure apply to data?
> Unproven techniques are risky.
Investigations are about People
3: Investigations are about people

> Focus on the person, not the machine.
3: Investigations are about people

> Focus on the person, not the machine.

> Intent is outside of security domain.
3: Investigations are about people

> Focus on the person, not the machine.
> Intent is outside of security domain.
> Crime may not violate security.
Still useful to catch the Dumb Ones
4: Still useful to catch the dumb ones

> Doesn’t have to be foolproof to be useful.
4: Still useful to catch the dumb ones

> Doesn’t have to be foolproof to be useful.

> Tech savvy criminals aren’t more dangerous.
4: Still useful to catch the dumb ones

> Doesn’t have to be foolproof to be useful.
> Tech savvy criminals aren’t more dangerous.
> 40% is still good.
Keep it Simple
5: Keep it simple

> Make it simple for investigators to use it.
5: Keep it simple

> Make it simple for investigators to use it.

> Must be within Investigator capabilities.
5: Keep it simple

> Make it simple for investigators to use it.
> Must be within Investigator capabilities.
> Often simpler non-computer solutions.
Forensics research without these principles is not forensics.
1: Forensics is Investigator-Centric.

2: Forensics and law are inseparable.

3: Investigations are about people.

4: Still useful to catch the dumb ones.

5: Keep it simple.

This work was supported in part by NSF awards CNS-1018615, CNS-0905349, and DUE-0830876, and in part by NIJ award 2008-CE-CX- K005.