



WPI

**“Everything you always
wanted to know about
digital forensics***

***But were afraid to ask”**

Robert J. Walls





Digital Forensics contends
with the CSI-Effect

Digital forensics lacks a solid
scientific foundation

Digital forensics struggles with
practical challenges

Digital forensics impacts
people directly



Security != Forensics

Security & Privacy

Security & Privacy & Forensics

5 lessons for researchers



**Digital forensics is
investigator-centric**

1

1. Digital Forensics is Investigator-Centric

- Research is investigator driven.
- Consider both goals and constraints.
- Break the rules lose the case.
- The rules change.

The background of the slide features a large, faint watermark of the University of Worcester Polytechnic Institute seal. The seal is circular with the text "UNIVERSITY OF WORCESTER POLYTECHNIC INSTITUTE" around the perimeter. In the center, there is a crest with a heart and the motto "LEHR UND KUNST" on a banner above it. The year "1865" is visible at the bottom of the seal.

**Forensics and law
are inseparable**

2

2. Forensics and law are inseparable

- Law is struggling to keep up.
- How does seizure apply to data?
- How does plain view apply?
- Forced Decryption?
- Government Hacking?
- Password Sharing?

The background of the slide features a large, faint watermark of the Worcester Polytechnic Institute seal. The seal is circular, with the text "WORCESTER POLYTECHNIC INSTITUTE" around the perimeter and "1865" at the bottom. In the center is a shield with a heart, flanked by laurel branches, and a banner above it with the words "LEHR" and "KUNST".

**Investigations are
about people**

3

3. Investigations are about people

- Focus on the person, not the machine.
- Intent is outside of security domain.
- Consider both computer and traditional crimes.
- Crime may not violate security.



**Still useful to catch
the dumb ones**

4

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.

The background of the slide features a large, faint, circular seal of Worcester Polytechnic Institute. The seal contains a shield with a book, a heart, and a laurel wreath, with the motto 'LEHR UND KUNST' above it. The text 'WORCESTER POLYTECHNIC INSTITUTE' and the year '1865' are also visible within the seal's border.

Keep it simple

5

5. Keep it simple

- Make it simple for investigators to use it.
- Must be within Investigator capabilities.
- Often simpler non-computer solutions.

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.



- 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.

Forensics research without
these principles is
not forensics

The background of the slide features a large, faint, circular seal of Worcester Polytechnic Institute. The seal contains a central shield with a book, a heart, and a laurel wreath. Above the shield is a banner with the words "LEHR" and "KUNST" separated by "UND". The outer ring of the seal reads "WORCESTER POLYTECHNIC INSTITUTE" and the year "1865" is at the bottom.

What's next?

Questions?

Robert Walls
rjwalls@wpi.edu