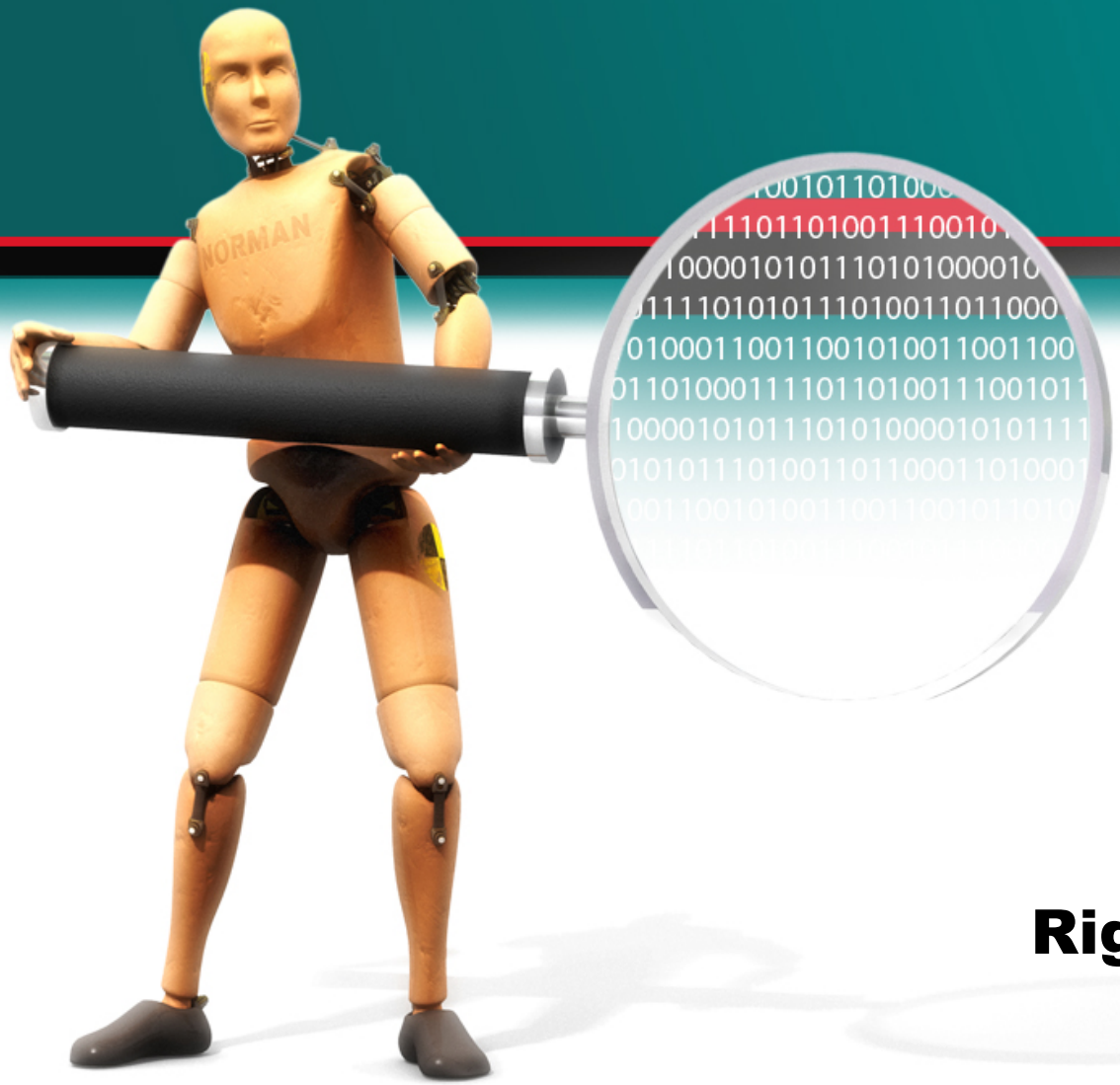
SANS: Computer Forensics Tool Panel

NORMAN®

Proactive IT security



8 September 2010

Righard J. Zwienenberg

Righard Zwienenberg

- Working for Norman Data Defense Systems
- Chief Research Officer
- Malware Analysis
- Forensics
- Law Enforcement

Why are forensic tools important

- It can work much faster and more precise than humans
- Flood of malware is increasing
- Targeted attacks
- Complexity

Where will forensic tools go to…

- **On the wire**
  - Many malware is using CiFS/SMB's to spread on networks
  - Scanning on protocol level
  - It can protect old (non-supported) networks as well as "weird" networks
- **On the phones(?)**

Questions and Answers

Righard J. Zwienenberg
Chief Research Officer
Righard.Zwienenberg@norman.com

Norman Data Defense Systems (UK) Ltd
Exchange House
494 Midsummer Boulevard
Central Milton Keynes
MK9 2EA
Tel: 08707 448044 / 01908 255990
Fax: 0870 1202901
E-mail: info@normanuk.com
http://www.norman.com/en-uk