



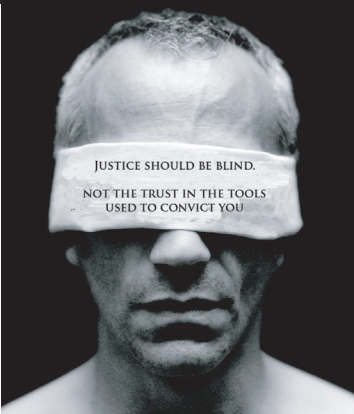
The Open
University

CSI: Malware & Cybercrime

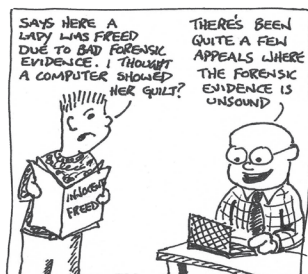
Learning to trust the tools to dissect and measure the unknown

Ian Kennedy¹, Blaine Price² and Arosha Bandara³

i.m.kennedy@open.ac.uk, b.a.price@open.ac.uk, a.k.bandara@open.ac.uk



Background & Motivation



Miscarriages of justice linked to flawed Expert evidence

Lack of scientific foundation in forensic 'junk' science

Address emerging standards introducing more science

Malware can mislead tools used in forensic examinations

Lack of statistically significant repeatability testing



Tools used
by forensic
investigators



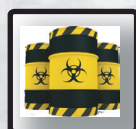
Virtual PC
Runs tool
and malware



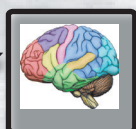
Artefacts
observed by
tools



Analysis &
reporting



350,000
samples of
real malware



Online
malware analysis
'The Oracle'



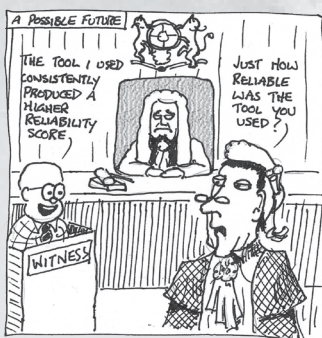
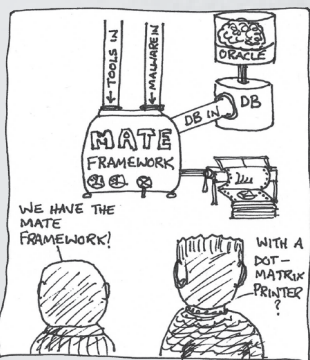
Artefacts
for each
malware sample

Malware artefacts

Individual identifiers that leave clues to their presence on a PC
Artefacts generated can change depending on the environment
Artefacts can be in observed as files & registry keys
The pattern of artefacts produced can form a footprint for the malware

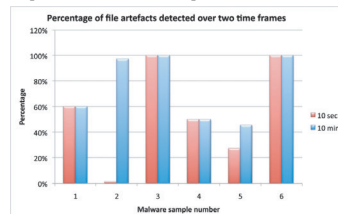
Methodology

Controlled experiments
Compare observations with those reported by 'The Oracle'
Observe footprints made by malware samples
Entire population of malware is not visible, so consider using Bayes



Malware Analysis Tool Evaluation Framework

Early results and possible impact



Early studies indicate that increasing the duration of observations raises the number of observed artefacts

Percieved benefits include:

Investigator has a more complete picture of events

Increased confidence in the use of the selected tool

Find us at our
project page

