All the gear... 
... and no idea 

Scalable, fast & forensically sound incident response using “NOOBS”

Andrew Sheldon MSc.
There are 3 BIG issues
The number of "POTENTIAL CRIME SCENES" increase every year.

Annual computer sales since 1986

Source: www.guardian.co.uk
Crime scenes keep getting BIGGER

Growth in hard disk capacity

Source: www.guardian.co.uk
There’re not enough FORENSIC ANALYSTS
The number of examinations will grow even faster.

The number of analysts will continue to grow over time.
THE SECONDARY CAUSE?

to back-room "experts"

Ratio of front-line "responders"

results in a high proportion of UNNECESSARY EXAMINATIONS
It also results in **MORE TRAVEL**

**HIGHER COSTS**

**WASTED TIME**
WHAT DOES ALL THIS MEAN
We'll KEEP getting what we've always had
If we KEEP doing what we've always done!
Too much work & too little time
Perhaps we should
EMPOWER THE FRONT LINE
To make informed decisions
There are some very good precedents

Effective at the FRONT LINE

Limited SKILLS required

Easy to DEPLOY

Supports SUSPICIONS
THE A&E ANALOGY

Not all BRAIN SURGEONS

Few SIMPLE tools

Limited TRAINING

Prioritises CASELOAD
A **formal & controlled** process for...

- Assessing risk
- Identifying targets
- Collecting data
- Filtering information
- Classifying results
- Prioritising actions
- Allocating resources

**High**
- Call in the experts

**Medium**
- Seek advice from experts

**Low**
- Perform triage or imaging
WE KNOW HOW TO APPLY THE RULES
Which help filter the RELEVENT
Prioritise RESOURCES
We must control the NOOBS with more than just a BOOT CD or thumb drive.
we have to PACKAGE THE SCIENCE
Play time ;-)

Live demos

• **Remote Forensics**
  – Respond to an incident in the USA, using Encase, via a mobile phone

• **Digital Triage**
  – Demonstrate how a NOOB can find the evidence forensically (and avoid giving you unnecessary work)
Remote Forensics Process

Case Manager in USA

Request forensic Assistance for job in New York Analyst

Authorises

Forensic Incident Management Server (FIMS)

Reviews CASE request

Downloads Credentials

Accepts CASE

Forensic Analyst in LONDON

Accesses evidence Using credentials

Evidence In USA

NOOB Does the “hands on” task

Forensic analyst Sends instructions from FIMS to NOOB

POD

NOOB

Does the “hands on” task

Forensic analyst Sends instructions from FIMS to NOOB

Remote Forensics Process
QUESTIONS?