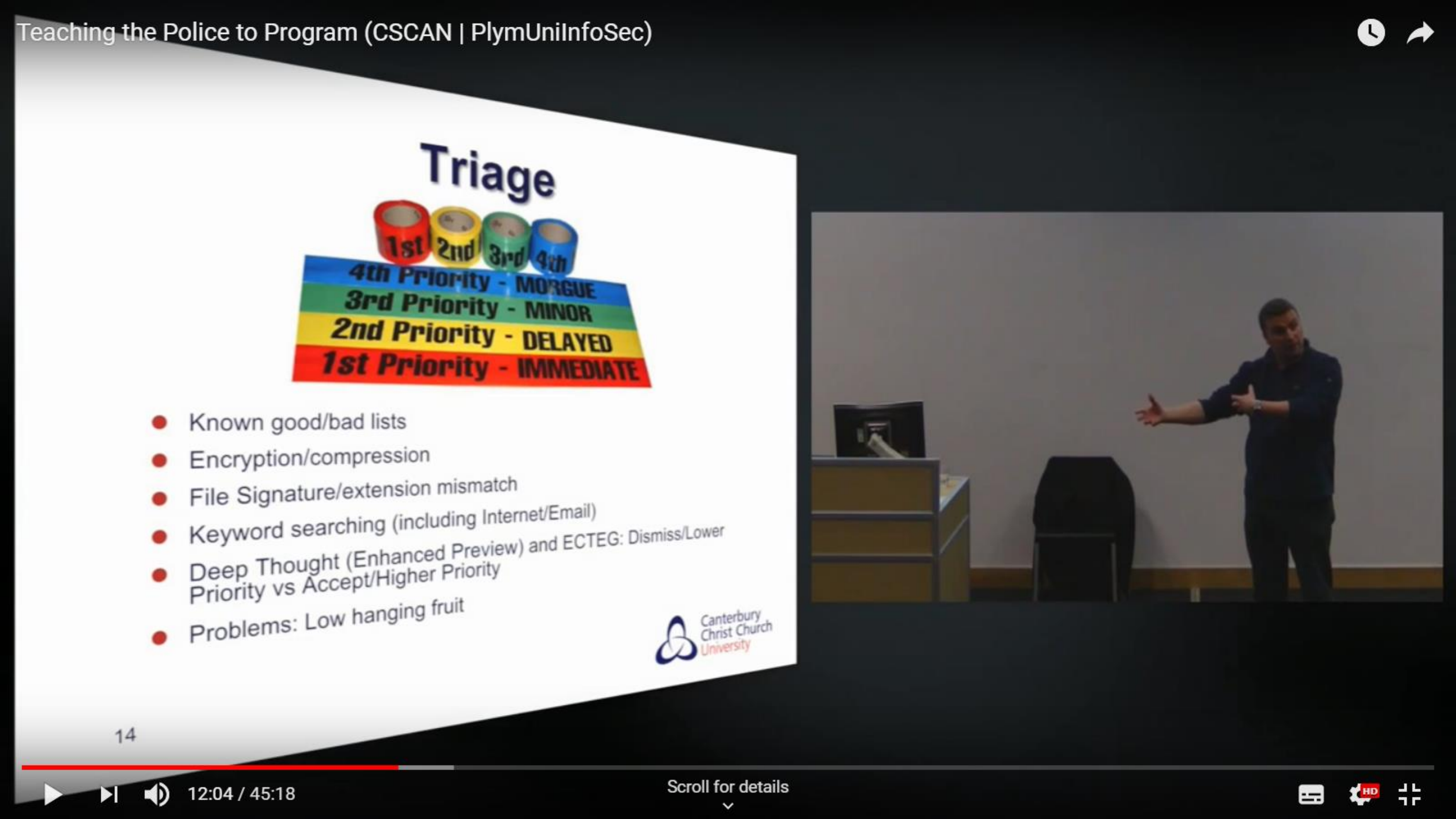
The effectiveness of policing cybercrime

Dr Paul Stephens
Director of Computing, Digital Forensics & Cybersecurity
paul.stephens@canterbury.ac.uk
http://www.canterbury.ac.uk/computing

Canterbury
Christ Church
University



Teaching the Police to Program (CSCAN | PlymUniInfoSec)

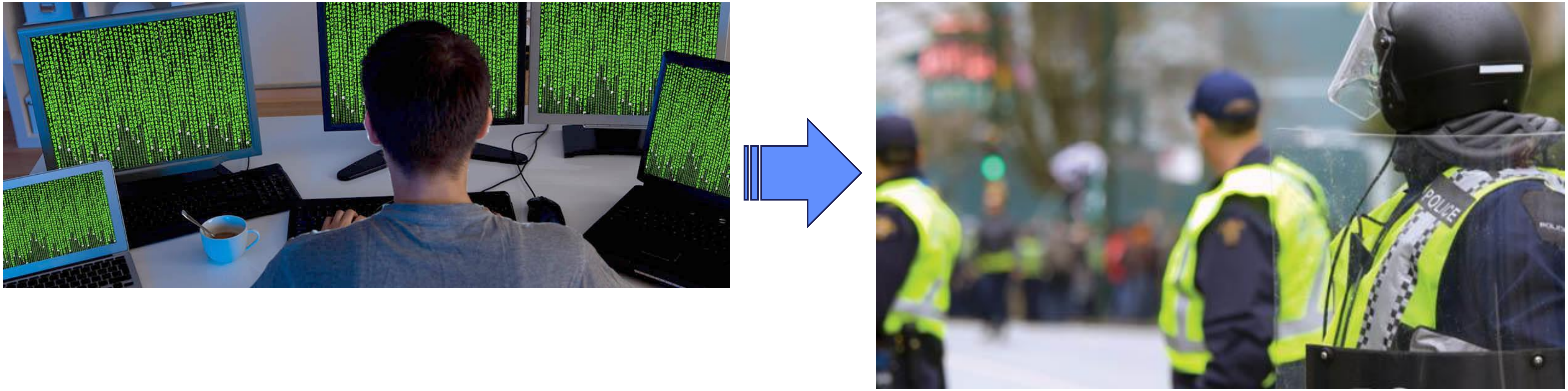
Triage

- Known good/bad lists
- Encryption/compression
- File Signature/extension mismatch
- Keyword searching (including Internet/Email)
- Deep Thought (Enhanced Preview) and ECTEG: Dismiss/Lower Priority vs Accept/Higher Priority
- Problems: Low hanging fruit

Canterbury Christ Church University

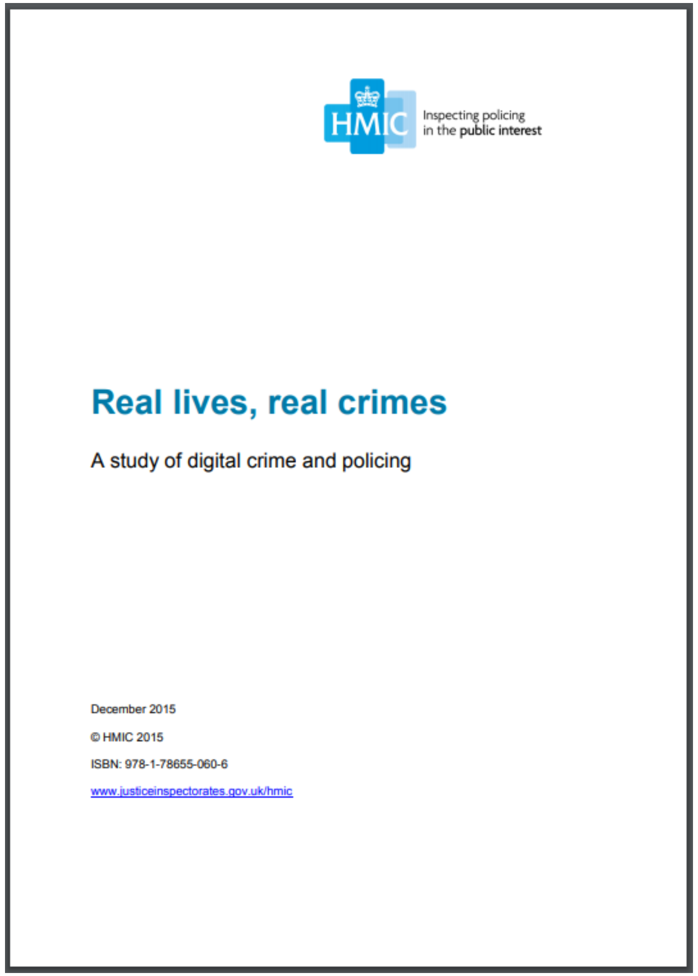
14

Focus of teaching



Canterbury
Christ Church
University

Real lives, real crimes: A study of digital crime and policing



HMIC Inspecting policing in the public interest

Real lives, real crimes

A study of digital crime and policing

December 2015

© HMIC 2015

ISBN: 978-1-78655-060-6

www.justiceinspectorates.gov.uk/hmic

- HMIC(FRS) Report
  - https://www.justiceinspectorates.gov.uk/hmicfrs/our-work/article/digital-crime-and-policing/real-lives-real-crimes-study-digital/

Daniel Blackmail victim

ABOUT

Daniel called the police because he was being blackmailed by someone whom he had met on a dating website.

43 Years old | ♂ Male | Works in finance

In his words: "I work long hours in the city centre. I often come home after a busy day and do more work from home."

Most used devices: ❶ ❷

COMMUNICATION CHANNELS

He uses his mobile 'phone often and has a work laptop which he takes home and uses for personal communications as well, mainly for email, Facebook and sometimes online chatting.

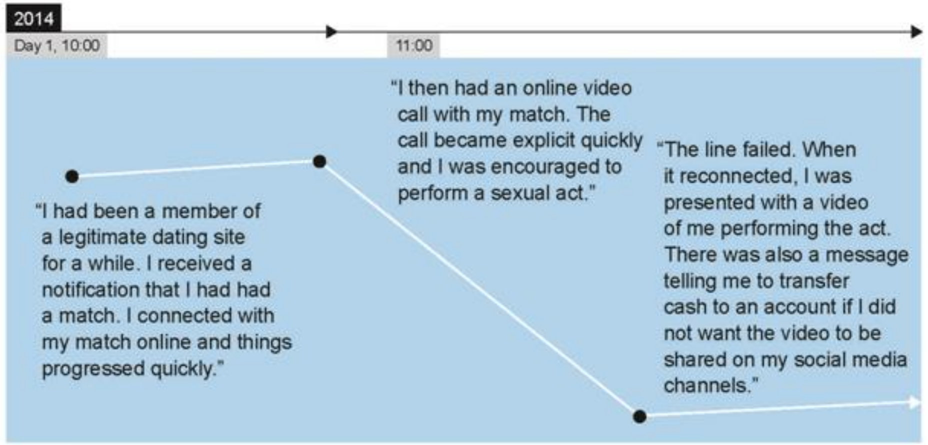
Online most for... ❶ ❷ ❸ ❹

ONLINE EXPERIENCE

He considers himself very experienced online, but still finds it hard to keep updated on the latest security measures. He is aware that there are lots of risks involved online, especially in scams through online dating sites, but he did not ever think that he would be caught out until it happened.

Level of online experience

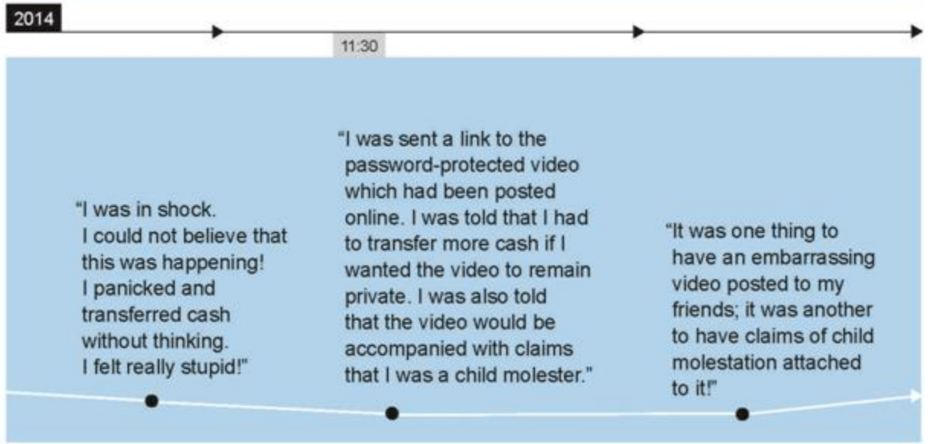
Novice — Average — ● — Expert



"I had been a member of a legitimate dating site for a while. I received a notification that I had had a match. I connected with my match online and things progressed quickly."

"I then had an online video call with my match. The call became explicit quickly and I was encouraged to perform a sexual act."

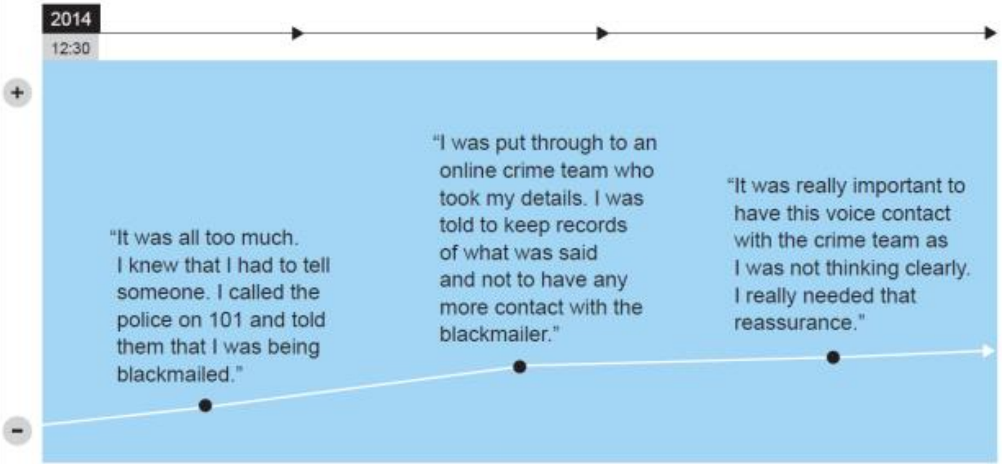
"The line failed. When it reconnected, I was presented with a video of me performing the act. There was also a message telling me to transfer cash to an account if I did not want the video to be shared on my social media channels."



"I was in shock. I could not believe that this was happening! I panicked and transferred cash without thinking. I felt really stupid!"

"I was sent a link to the password-protected video which had been posted online. I was told that I had to transfer more cash if I wanted the video to remain private. I was also told that the video would be accompanied with claims that I was a child molester."

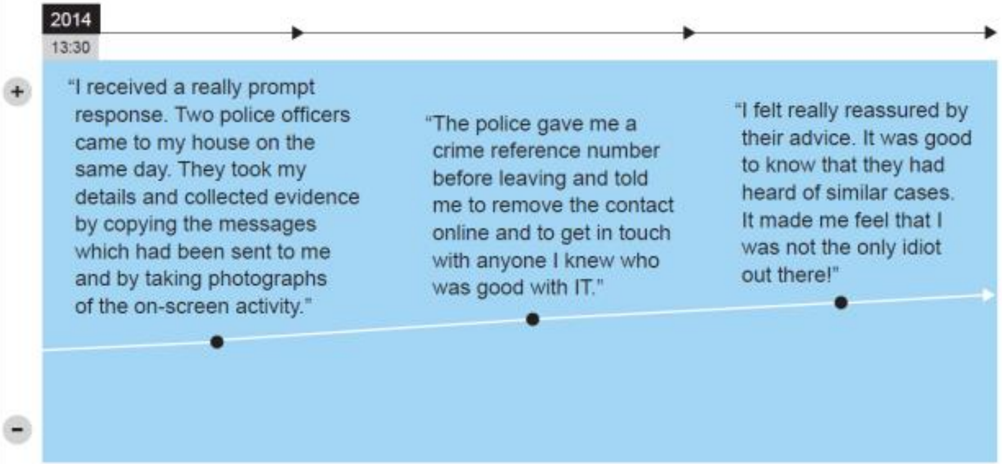
"It was one thing to have an embarrassing video posted to my friends; it was another to have claims of child molestation attached to it!"



"It was all too much. I knew that I had to tell someone. I called the police on 101 and told them that I was being blackmailed."

"I was put through to an online crime team who took my details. I was told to keep records of what was said and not to have any more contact with the blackmailer."

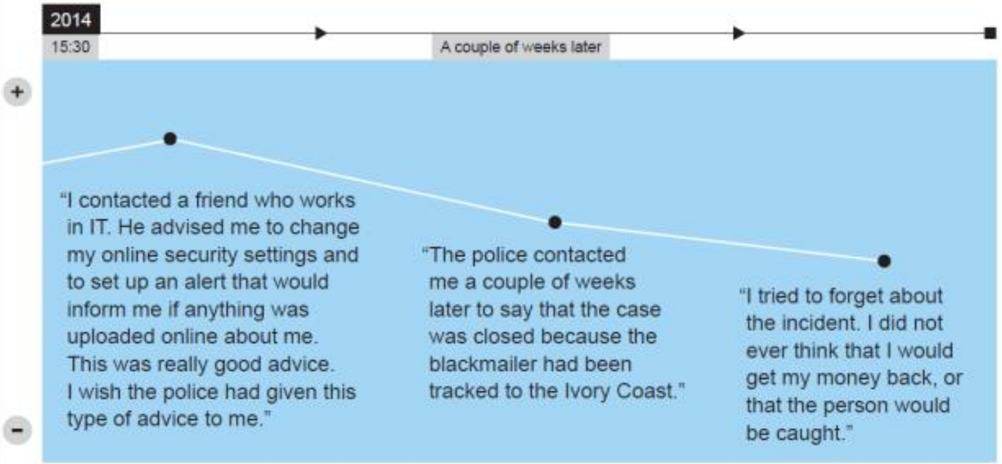
"It was really important to have this voice contact with the crime team as I was not thinking clearly. I really needed that reassurance."



"I received a really prompt response. Two police officers came to my house on the same day. They took my details and collected evidence by copying the messages which had been sent to me and by taking photographs of the on-screen activity."

"The police gave me a crime reference number before leaving and told me to remove the contact online and to get in touch with anyone I knew who was good with IT."

"I felt really reassured by their advice. It was good to know that they had heard of similar cases. It made me feel that I was not the only idiot out there!"



"I contacted a friend who works in IT. He advised me to change my online security settings and to set up an alert that would inform me if anything was uploaded online about me. This was really good advice. I wish the police had given this type of advice to me."

"The police contacted me a couple of weeks later to say that the case was closed because the blackmailer had been tracked to the Ivory Coast."

"I tried to forget about the incident. I did not ever think that I would get my money back, or that the person would be caught."

Can we continue to effectively police digital crime?

Science and Justice 57 (2017) 448–454

Contents lists available at ScienceDirect

Science and Justice

journal homepage: www.elsevier.com/locate/scijus

Review

Can we continue to effectively police digital crime?

Graeme Horsman

Department of Computing, Engineering and Technology, Faculty of Computer Science, The David Goldman Informatics Centre, St Peter's Way, Sunderland SR6 0DD, UK

ARTICLE INFO

Article history:
Received 9 February 2017
Received in revised form 5 June 2017
Accepted 7 June 2017

Keywords:
Cyber-crime
Digital forensics
Security
Crime
Research

ABSTRACT

Now approximately 30 years old, the field of digital forensics is arguably facing some of its greatest challenges to date. Whilst currently supporting law enforcement in numerous criminal cases annually, questions are beginning to emerge regarding whether it can sustain this contribution, with digital crime remaining prevalent. In his first live interview in September 2015, Head of MI5, Andrew Parker indicated that individuals are now engaging in computing acts which are beyond the control of authorities, confirming earlier remarks made by British Prime Minister David Cameron in the wake of the Charlie Hebdo attacks. Such comments cast doubt on the future effectiveness of the digital forensic discipline and its ability to effectively investigate those who implement the latest forms of technology to carry out illicit acts. This article debates the controversial question, could we be facing an era where digital crime can no longer be effectively policed?

Contents

1. Introduction

Thought of by many to be within its infancy [37,51], such statements regarding the field of digital forensics (DF) are arguably no longer accurate. These perceptions are largely due to societal and technological developments, brought into public consciousness through mounting media coverage, coinciding with increasing computer usage and volumes of digital crime [65]. Since the turn of the millennium, DF has played a major role in digital crime detection and prevention despite being in existence since the 1980's, when the first incidences of computer crime were witnessed [57]. When quantified, the field of DF is around 30 years old and is now a well-established branch of forensic science, embedded into criminal and civil legal practices worldwide where the acquisition and interpretation of digital evidence is often required. Subsequently DF evidence has featured prominently in a number of high profile investigations including those of Dr. Conrad Murray in the trial of Michael Jackson's death [5], Dr. Harold Shipman, one of the United Kingdom's (UK) most prolific serial killers [30], Lost Prophets member Iain Waktins [6] and recently convicted athlete Oscar Pistorius [8].

The discipline of DF was established in response to the increased availability and affordability of digital devices in order to tackle their potential illicit use. What followed; the commercialisation of the Internet and an unprecedented growth in technology as many services sought to migrate to the digital realm throughout the 1990s, only further

E-mail address: graeme.horsman@sunderland.ac.uk.

http://dx.doi.org/10.1016/j.scijus.2017.06.001
1355-0306/© 2017 The Chartered Society of Forensic Sciences. Published by Elsevier Ireland Ltd. All rights reserved.

- Graeme Horsman
  - https://doi.org/10.1016/j.scijus.2017.06.001

Canterbury
Christ Church
University

Could we be facing an era where digital crime can no longer be effectively policed?

- **Increasing computer usage** and **volume** of **digital crime**
  - **Conviction rates not following suit**
- **High profile cases** with **digital forensics** elements (Michael Jackson's death, Dr Harold Shipman, Iain Watkins, Oscar Pistorius)
- Case **backlogs**, cyber-**dependent**, cyber-**enabled**, **supporting** evidence
- **Privacy aware, digital natives, encryption, Deep Web, Prism Break**

Could we be facing an era where digital crime can no longer be effectively policed?

- **Locard's exchange principle not applying** so strictly to digital traces
- Detection is difficult – **time**-based, **competency**-based
- **Scale** – **Internet**, multiple **jurisdictions** and **devices**, **size** of storage media, **non-cooperation** of many countries
- Lack of **reporting** – feeling of **stupidity**, **embarrassment** factor

Conclusions of HMIC Report – Police Service

- Establish **scale** and **impact** of digital crime
  - **National** and **local** level
  - How to **respond** to it
- Create **effective leadership**, and **governance arrangements** and **strategies** at all levels to **manage the threat** digital crime poses
  - Engaging with those in **police service** and **private sector** who are able to provide **expertise**

Conclusions of HMIC Report – Chief Constables

- **Appropriate** and **continuing training** and **guidance** for all likely to deal with digital crime and its **victims**
- Officers and staff **understand the significance of online anti-social behaviour**
  - Able to **provide effective support and advice** to those that are its **victims**

Conclusions of HMIC Report – Chief Constables

- Capability to **examine digital devices appropriately**, **effectively**, and **speedily**
- Appoint **chief officer responsible** for **ensuring staff understand** which cases should be **referred to Action Fraud** and which require an **immediate response**
- **Referrals** from **National Fraud Intelligence Bureau** are dealt with **effectively**

Other responses

- **Prevention** and **awareness training** from an early age
- Improvements in **digital investigation technology, tools and techniques**
- Pushing of **responsibilities for policing** onto **companies hosting activity**
  - Facebook and **fake news**
  - Google and the **right to be forgotten**
  - Target **advertisers** rather than hosts (bad publicity)

Canterbury
Christ Church
University

Other responses

- **Legislation**, e.g., Regulation of Investigatory Powers Act **(RIPA)**
  - Criminal **offence to refuse to decrypt** encrypted data if requested as part of a **criminal investigation**
    - Penalty **two years** or **five years** for terrorism

British police are on the brink of a totally avoidable cybercrime crisis

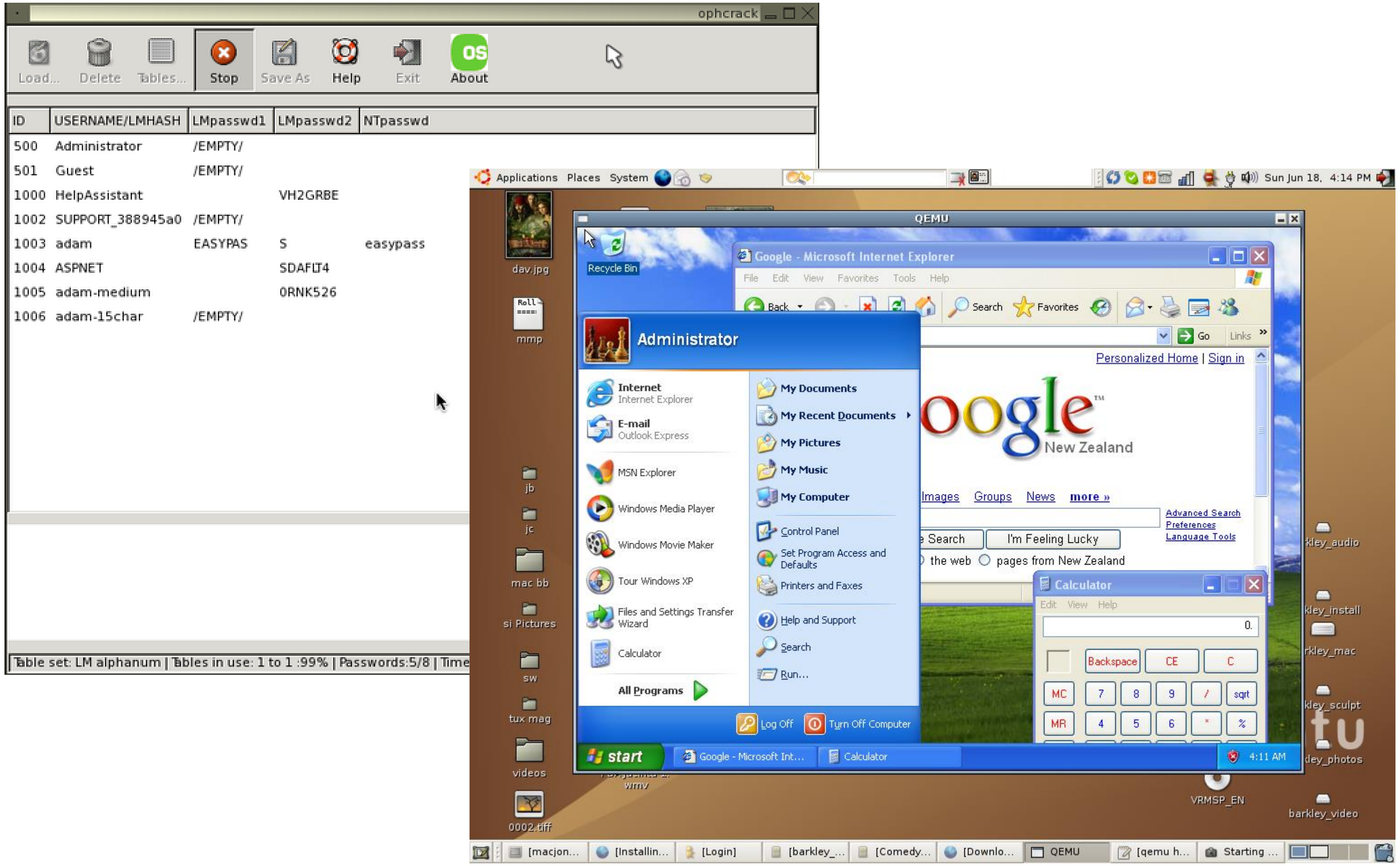
- https://www.wired.co.uk/article/british-police-cybercrime-hacking
- Legislation for ‘**offensive policing**’
- **Technology platforms** to start doing the some of the **policing**
- **More resources**…

Canterbury Christ Church University

Live Data Forensics

- How do we handle encrypted/network/volatile data?
- Critique and rewrite ACPO Guidelines?
- Automation, is it possible?
- How do we measure the effect we have on a system?

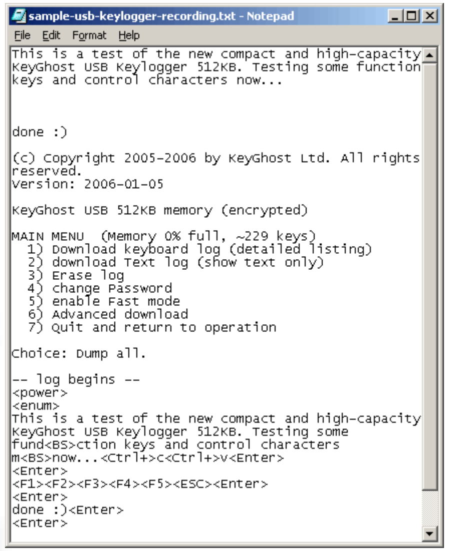
Dealing with Encryption and Complexity



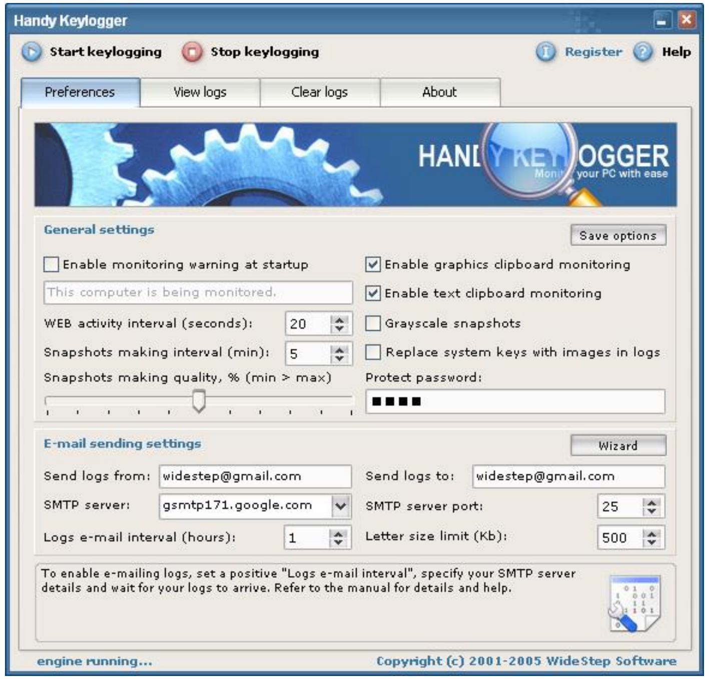
```
ID    USERNAME/LMHASH    LMpasswd1  LMpasswd2  NTpasswd
500   Administrator      /EMPTY/
501   Guest              /EMPTY/
1000  HelpAssistant                 VH2GRBE
1002  SUPPORT_388945a0   /EMPTY/
1003  adam               EASYPAS    S          easypass
1004  ASPNET                        SDAFLT4
1005  adam-medium                   0RNK526
1006  adam-15char        /EMPTY/
```

```
Table set: LM alphanum | Tables in use: 1 to 1 :99% | Passwords:5/8 | Time
```

Dealing with Better Encryption



```
This is a test of the new compact and high-capacity
KeyGhost USB Keylogger 512KB. Testing some function
keys and control characters now...



done :)

(c) Copyright 2005-2006 by KeyGhost Ltd. All rights
reserved.
Version: 2006-01-05

KeyGhost USB 512KB memory (encrypted)

MAIN MENU  (Memory 0% full, ~229 keys)
  1) Download keyboard log (detailed listing)
  2) download Text log (show text only)
  3) Erase log
  4) change Password
  5) enable Fast mode
  6) Advanced download
  7) Quit and return to operation

Choice: Dump all.

-- log begins --
<power>
<enum>
This is a test of the new compact and high-capacity
KeyGhost USB Keylogger 512KB. Testing some
fund<BS>ction keys and control characters
m<BS>now...<Ctrl+>c<Ctrl+>v<Enter>
<Enter>
<F1><F2><F3><F4><F5><ESC><Enter>
<Enter>
done :)<Enter>
<Enter>
```



General settings

☐ Enable monitoring warning at startup

This computer is being monitored.

WEB activity interval (seconds): 20

Snapshots making interval (min): 5

Snapshots making quality, % (min > max)

☑ Enable graphics clipboard monitoring

☑ Enable text clipboard monitoring

☐ Grayscale snapshots

☐ Replace system keys with images in logs

Protect password: ■■■■

E-mail sending settings

Send logs from: widestep@gmail.com

SMTP server: gsmtp171.google.com

Logs e-mail interval (hours): 1

Send logs to: widestep@gmail.com

SMTP server port: 25

Letter size limit (Kb): 500

To enable e-mailing logs, set a positive "Logs e-mail interval", specify your SMTP server details and wait for your logs to arrive. Refer to the manual for details and help.

engine running...

Copyright (c) 2001-2005 WideStep Software

Discussion, Ideas and Questions?

paul.stephens@canterbury.ac.uk

Canterbury
Christ Church
University