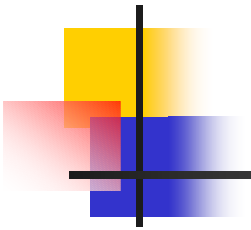
FOSS systems: Why do we not use them more ?

Les Hatton

Professor of Forensic Software Engineering,
CISM, Kingston University
L.Hatton@kingston.ac.uk

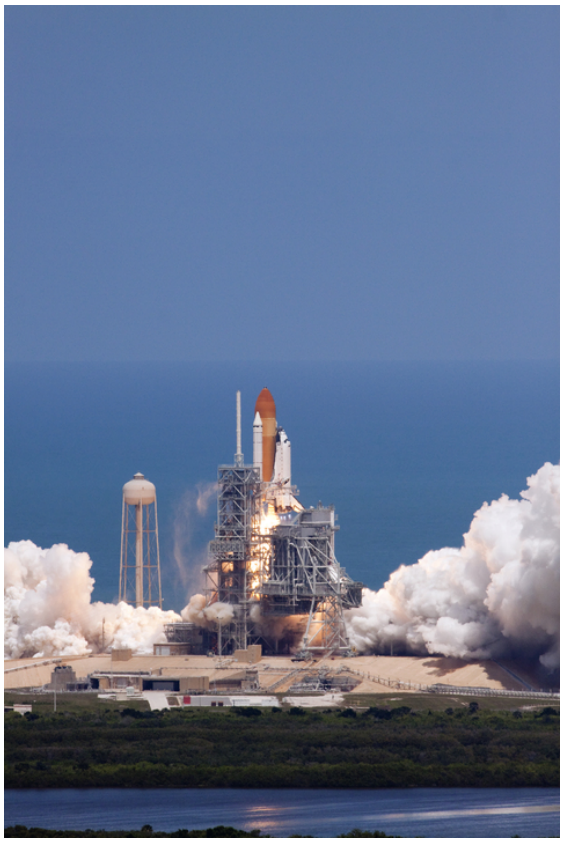
Version 1.1: 25/Oct/2010

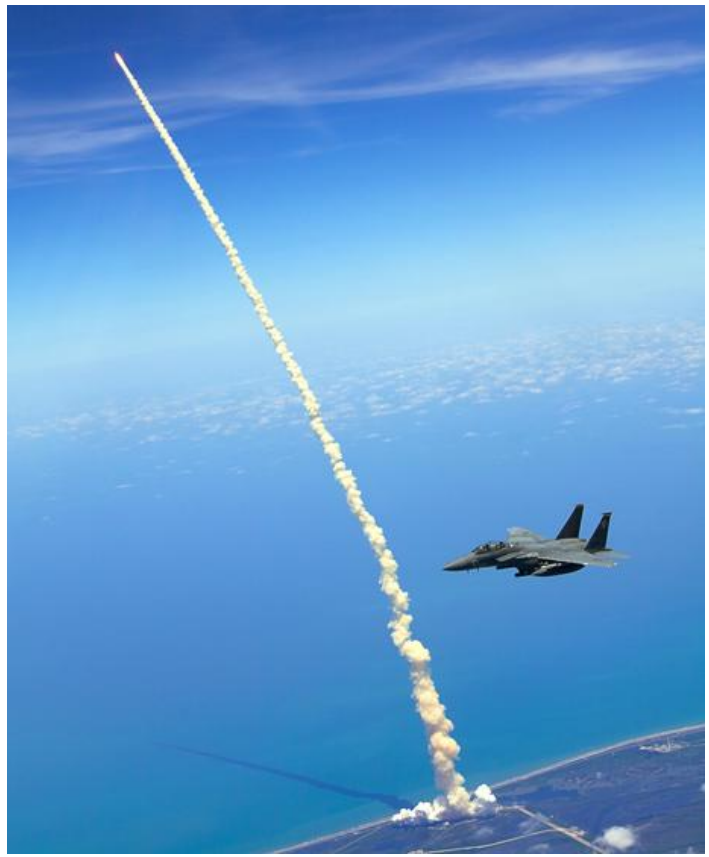
Overview



- A little about reliability
- A little about life-cycles
- A little about support
- A little about ubiquity
- And a little about security

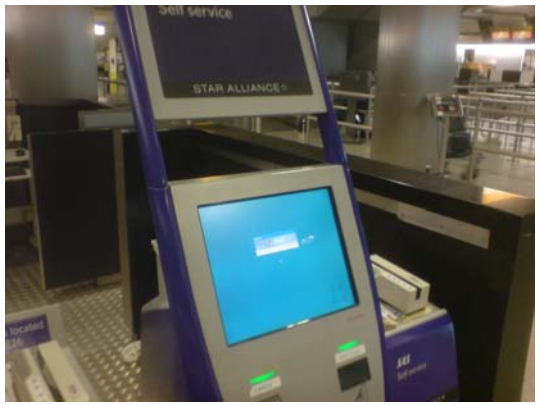
Some software is exceedingly good …
(Space Shuttle software)





… but most of it is not
(all within 90 minutes at Heathrow, 11-May-2010)

Check -in



Departures

"This system is rubbish"
(departures official)

Departures lounge

On the plane

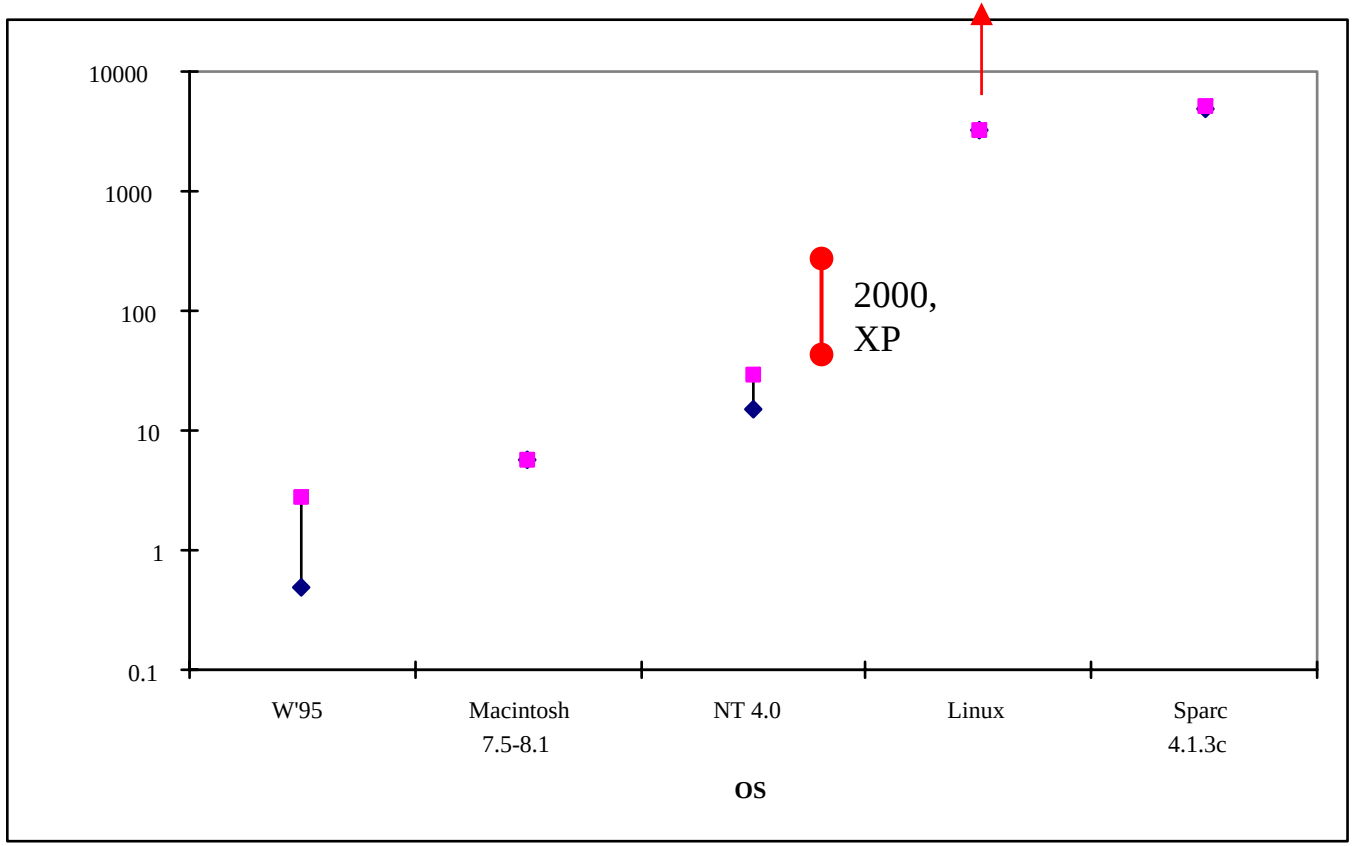
Check-in problems happen to me quite a lot

- Feb 2010, print off boarding cards online
- Departures won't let me in because they can't read it.
- SAS can't issue another boarding card because I already have one
- I generously offer to lie on the runway until they sort it out.
- SAS duty manager gives me written one if I promise "I am me".
- I point out that its lucky I'm not Bertrand Russell. This comment is wasted. Note to self: no more jokes at check-in
- Departures won't let me in because I now have two passes until they find person who refused the first one.

OS Reliability

> 50,000 hours

MVS, VMS (1980s)



> 400 years between failures reported by some users for Linux 2006-9

Mean Time Between Failures of various operating systems

OS reliability

Statistics from a primary mail and web server

- Operating System Centos 5.X
- Continuous up-time (at time of writing), 823 days.
- Mail load handled, approximately 110 million messages (99.97% junk)
- 10 web-sites served.
- Auto-patched, zero maintenance.

Hatton (2011) “e-mail forensics”.

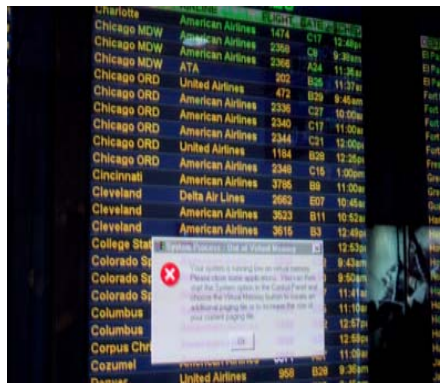
This sort of thing is surprisingly common

24.5 million XP crashes per day

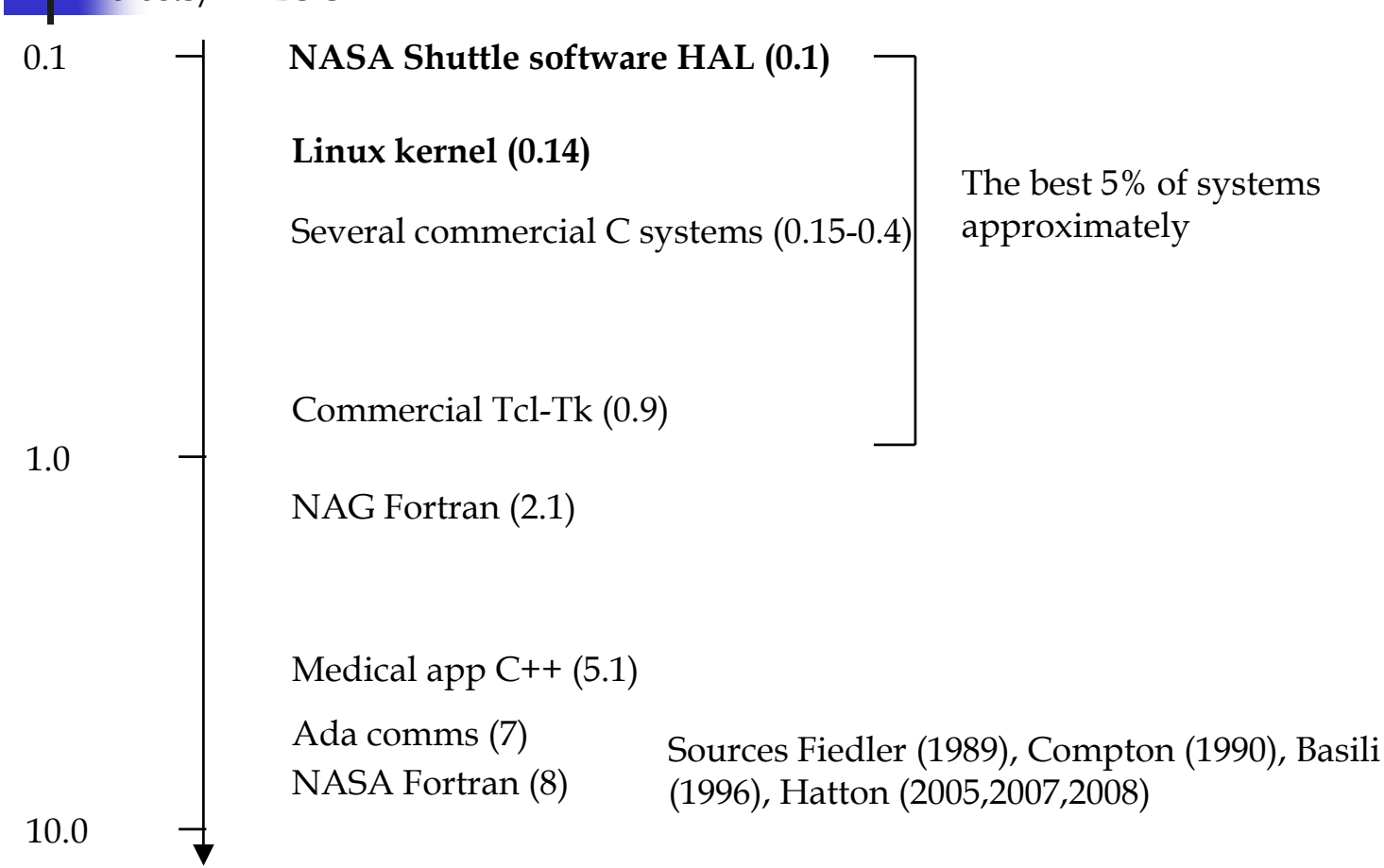
http://www.pcmag.com/article2/0,4149,1210067,00.asp

5% of Windows Computers crash more than twice a day

http://www.nytimes.com/2003/07/25/technology/25SOFT.html



A software quality scale based on defect density



“Assumption is the mother of all screw-ups” *

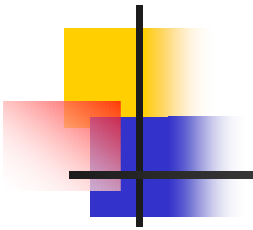
My first medical system experience, (a medical records system which each night backed itself up with the message …)

* Wethern’s law of suspended judgement

“Assumption is the mother of all screw-ups”

Unfortunately, it was delivered in the Netherlands which after suitable translation yields …

Overview



- A little about reliability
- A little about life-cycles
- A little about support
- A little about ubiquity
- And a little about security

A little about reliability

FOSS development is effectively what became *agile*.

- Engineer experience (Brooks, 1975)
- Open (“All bugs are shallow …”, Raymond (1999))
- Iterative (Release often, change little)
- Darwinian (Large-scale prototyping)
- …

Brooks (1975) “The mythical man month”, Raymond (1999) “The cathedral and the bazaar”.

A little about reliability

What we rarely do is

- Requirements
- Specification
- Design
- Implementation
- Test
- Release and leave country

This is the so-called **waterfall model**. Think of it in the sense of going over a waterfall in a barrel. You don't why you agreed to it in the first place and you can't get out until you hit the bottom which your barrel will mostly likely not survive.

It is rarely if ever successful. Top-down management controlled systems rarely are whatever "life-cycle" model you adopt. They make senior management feel good until the end. At this point, they will say engineers "need more business skills".

It is no surprise therefore that …

Many large projects are late or never appear at all or don't do what they are supposed to

- NHS "Connecting for Health"
- Child Support Agency
- Passport Office
- Benefit Office
- C-Nomis (2009) (Ministry of Justice and Home Office) – "Nobody sure how 161million pounds had been spent"
- Transport Direct cycle route planner (2009). This absorbed 2.7 million pounds but failed to replace a public site with far greater coverage and functionality (cyclestreets.net) which cost around 6,000 pounds.

The Welsh/English NHS approaches: 1. The English top-down approach.

- *Aimed to double budget* and assumed technology existed and the problem was one of procurement at the right price
- Series of wildly-ambitious billion pound contracts
- “Essential systems are late, or when deployed, do not meet expectations of clinical staff; estimates of local costs are still unreliable; and many NHS staff remain unenthusiastic.” Edward Leigh MP, Commons public accounts, 2009
- Repeatedly refused independent auditing.

The Welsh/English NHS approaches: 2. The Welsh iterative approach.

- Virtually no budget and no grandiose ambitions
- Built incrementally from Gwent GPs outwards to one hospital and so on. The glue software came from a company too small to be eligible for English contracts.
- These are not just technical issues. Dealing with politicians' unrealisable dreams like "Choose and book" helped cripple the English system.
- "Never let a politician near an IT system proposal." (I will take the rap for this quote.)

Michael Cross: http://www.guardian.co.uk/technology/2009/jan/29/computer ...

A few of the problems

11/08/2008

- Failures in new NHS computer system have meant hundreds of suspected cancer sufferers in London have their operations cancelled.
- People in contact with MRSA could not be contacted
- Many appointments lost.

http://www.bbc.co.uk/1/hi/england/7555077.htm

19/09/2006

- Failures in new NHS computer system have led to 110 ‘major incidents’ in 4 months.

http://www.dailymail.co.uk/

But you are not alone

Banks and payrolls …

- 08/07/2008. Westpac in Australia issued all payroll and direct debits twice.

  http://blogs.spectrum.ieee.org/riskfactor/2008/07/westpac_bank_glitch_causes_pro.html

- 11/08/2008. Swansea Council in Wales had to abandon a GBP 819,000 project with CAP Gemini after it increased to GBP 8,000,000 after continual problems.

  http://blogs.spectrum.ieee.org/riskfactor/2008/08/

Cars …

- 05/02/2010. Toyota Prius braking problem. (causing one second lag in application of brakes.)
- 06/02/2005. Whole string of problems, shaking Mercedes, Ford that bakes back seat passengers …

  http://www.nytimes.com/2005/02/06/automobiles/06AUTO.html
- 26/10/2004. BMW disables dynamic stability control and ABS. Two police drivers vindicated after investigation.

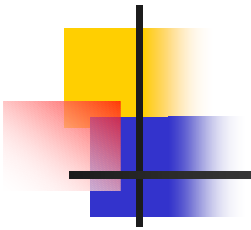
  http://www.daserste.de/plusminus/beitrag.asp?iid=254
- 14/04/2004. Ford is recalling 363,440 of its 2001-2003 Ford Escape vehicles due to software problems in power-train causing engine stalling.

  Detroit News

The author's favourite ...

- "Entire Montgomery Ward warehouse goes missing for 3 years".
  - An error in the input program lost the warehouse in Redding, California. The staff didn't like to say anything because they thought they had lost their jobs although their pay-cheques continued to arrive.

Overview



- A little about reliability
- A little about life-cycles
- A little about support
- A little about ubiquity
- And a little about security

Support

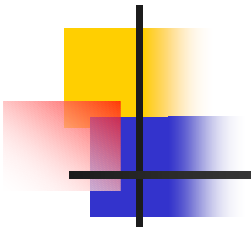
- Support is very rapidly being replaced by internet search.
- Typically for my queries, 15 minutes of searching reveals a significant answer.
- All too often, our experience of commercial support follows this pattern …

The strange case of the FAX machine and the telephone sex line

- Receive telephone bill for FAX machine containing two 20m05s calls to a telephone sex line at 4am.
- I call BT support. “Computer says” its correct
- I ‘elevate priority’ and provide FAX logs. BT says it will investigate
- Final demand received
- I call BT again. “Computer says” its correct
- Notice of removal of service arrives
- I call BT and invite them to take me to court
- BT calls me. “Computer says” its correct but they will let me off “if I don’t do it again”

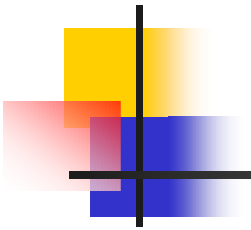
6 weeks

Overview



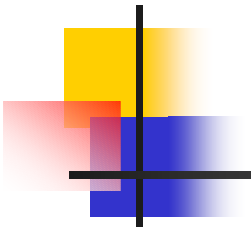
- A little about reliability
- A little about life-cycles
- A little about support
- A little about ubiquity
- And a little about security

Ubiquity



- The internet depends on FOSS
  - Open software – Apache, Firefox, MySQL, PHP, Perl and so on
  - Open protocols – Mail, TCP/IP, …
  - Open data formats – pdf, HTML, …
- This extends to medical systems
  - DICOM (mostly), …

Overview



- A little about reliability
- A little about life-cycles
- A little about support
- A little about ubiquity
- And a little about security

Knock, knock its your internet burglar …

Imagine your internet-connected PC is a house.

- Every 2 minutes somebody peers through the window
- Every 3 minutes, somebody climbs over the wall and walks round the house
- Every 80 minutes, somebody tries your doors and windows
- Every 3 hours, somebody will try to break the door down with a sledgehammer.

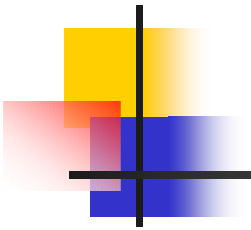
Botnets

- Thousands of PCs and PDAs controlled by remote criminal operators
  - Mariposa botnet (Spain, Mar 2010) had details of 800,000 people gleaned from 12.7 million machines.
  - Waledac (US, Feb 2010) (hundreds of thousands of PCs) used for sending hundreds of millions of spam messages each day.
  - Lethic (Jan, 2010), Mega-D (Nov 2009), Torpig (May, 2009), McColo (Nov, 2008) all taken down after efforts by security reseachers.
- About every 3 weeks the PC of a personal acquaintance is compromised.

Security breaches

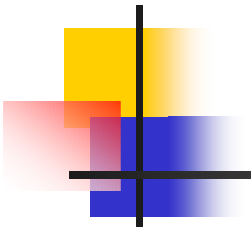
- Recorded successful computer viral attacks on NHS systems.
  - 23-Apr-2010 1100 machines, Qakbot
  - 18-Feb-2010. West Middlesex, Conficker-A
  - 10-Jul-2010. > 8,000 machines hit in last year
  - 21-Aug-2009. Whipps Cross hit
  - …

Hacking of embedded systems



- Stuxnet (27-Sep-2010)
  - The first recorded hacking of an industrial control system, (Siemens power grid infrastructure monitoring).

Security of FOSS systems



- FOSS systems seem to be standing up to attacks pretty well.
  - Open source appears to act in favour of the defender not the attacker with loop-holes typically closed very quickly and the underlying security model is conservative.

Things FOSS doesn't help: Data loss, (many, many examples)

- Organisations have an appalling record …
  - Mar 2010, Barnet council lost 9,000 children's records
  - Aug 2008, Zurich insurance lose about 600,000 records, (came to light in Mar, 2010).
  - Jan, 2010, Ladbrokes lose 4.5 million customer records.
  - Oct 2008, 25 million child benefit records lost, (this included 350 on witness protection scheme).
  - 2005-2008, HMRC reported 7 other significant data loss incidents.
  - Dec 2007, hundreds of thousands of patient records from nine NHS trusts went missing. The NHS also routinely shares patient data with local councils.
  - In 2008, the MoD lost almost as many records as the NHS.
  - Dec 2007, Department of Transport admits three major data loss incidents including those of 3 million learner drivers.
  - Aug 2008, HSBC lost an entire server with 159,000 customer records.

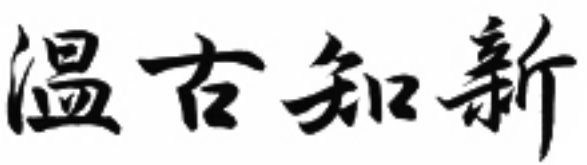
General conclusions ...

- FOSS appears to have many, many benefits
  - It's development experiences help teach us how to build commercial scaleable systems.
  - Infrastructural components like the Linux kernel are amongst the most reliable complex systems the human race has ever produced.
  - The reliability is accompanied by a much lower security threat profile.
  - The lack of formal support has little effect with modern internet search capability.

- High quality IT systems are at the heart of an efficient economy. Its time we learned some lessons.

The essence of Forensics …

"Those who cannot remember the past are condemned to repeat it". George Santayana, (1863-1952)



"On Ko Chi Shin" – "Studying the old promotes a better understanding of the new". Ancient Japanese proverb.

Notes for this talk are available at:-

http://www.leshatton.org/

Vodafone's attempt to upgrade my Mobile WiFi connection