



Bridging the Divide:
Rising Awareness of Forensic Issues
amongst
Systems Administrators

Vlasti Broucek & Paul Turner
School of Information Systems
University of Tasmania

May 25 10:12:46 spike telnetd[13626]: connect from hades.porcupine.org

```
wietse  ttyp1      hades   Thu May 25 10:12 - 10:13 (00:00)
-----
hostname  -          wietse  ttyp1      0.00 secs Thu May 25 10:12
sed       -          wietse  ttyp1      0.00 secs Thu May 25 10:12
stty      -          wietse  ttyp1      0.00 secs Thu May 25 10:12
mesg      -          wietse  ttyp1      0.00 secs Thu May 25 10:12
who        -          wietse  ttyp1      0.00 secs Thu May 25 10:12
w          -          wietse  ttyp1      0.00 secs Thu May 25 10:12
ps         -          wietse  ttyp1      0.00 secs Thu May 25 10:13
ls         -          wietse  ttyp1      0.00 secs Thu May 25 10:13
w          -          wietse  ttyp1      0.00 secs Thu May 25 10:13
csh        -S         wietse  ttyp1      0.03 secs Thu May 25 10:12
telnetd   -S         root    _          0.00 secs Thu May 25 10:12
-----
wietse  ttyp1      hades   Thu May 25 10:12 - 10:13 (00:00)
```

(Farmer, D., & Venema, W. (2000). Forensic Computer Analysis: an Introduction. Reconstructing Past Events. *Dr Dobb's Journal*, 29(9), 70-75.)

Topics Covered

- ✓ Forensic Computing (FC) as an Academic Discipline
- ✓ Computer Security (CS) versus Forensic Computing
- ✓ Intrusion Detection Systems (IDS) as an Forensic Computing Tool
- ✓ Conclusion

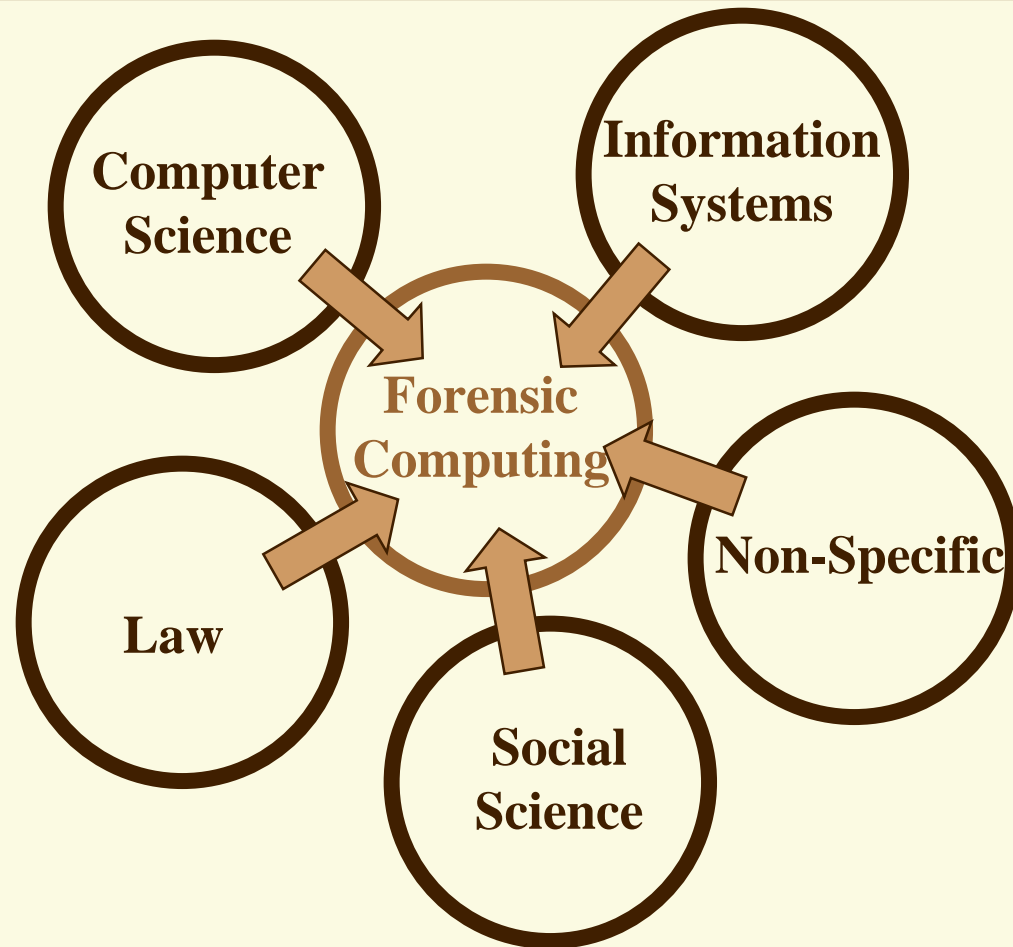
Forensic Computing - Definition

‘The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable’. (McKemmish, 1999)

‘Gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system’. (Farmer & Venema, 1999)

FC as an Academic Discipline

T
a
x
o
n
o
m
y



CS versus FC

- ✓ Myth - FC is just another name for CS
 - Example 1 - child pornography
 - Example 2 - life threatening e-mail
- ✓ Major differences
 - why
 - when
 - who
 - for whom

CS versus FC

WHY

Protects the system against attack

Does not protect the system against attack

WHEN

In or near in real time

Post mortem

CS versus FC

WHO

(Usually) computer specialist

Can be computer specialist but often not so

FOR WHOM (audience)

Restricted presentation - limited to professional audience

Evidence is nearly always presented to non-IT/IS personnel

CS versus FC

BIG PROBLEM

Can be bypassed by trusted individuals/users

The integrity of the evidence is most important

CS versus FC

- ✓ CS is one of the foundation stones of FC but unfortunately:
 - CS tools not suitable for FC
 - CS people not aware of FC issues
 - e.g. difference between scientific and legal proof
- ✓ Technology well ahead of legal systems

Intrusion Detection Systems

✓ Types

- source of information
- analysis
- response

✓ Problems

IDS - a Case Study

✓ “Rome Labs” attack

- hacker attack on Rome Air Development Center, Griffiss Air Force Base, New York, March 28, 1994

✓ Christy (1998)

- 5 days to discover the attack
- some systems left open to allow investigation
- many questions unanswered

✓ Sommer’s analysis

IDS - Technical Problems

- ✓ may not be able to collect all the data (speed limits)
- ✓ the data collected may not be sufficient
- ✓ the data collected may be flawed, erroneous or tampered with

IDS - Legal Problems

- ✓ legal admissibility of digital evidence per se
- ✓ validity, weight (legal versus scientific proof)
- ✓ legal dimensions of the forensic analysis conduct

Conclusion

- ✓ Data collection techniques to follow legal requirements
- ✓ Data collection techniques to follow privacy protection laws
- ✓ Manipulation of collected data sets
 - minimise
 - document

Conclusion

✓ Future research

- Black Box
- Privacy
- Availability

References

✓ Papers

- <http://brouk.psychol.utas.edu.au/publications.html>

✓ Contacts

- Vlasti.Broucek@utas.edu.au
- Paul.Turner@utas.edu.au

✓ Questions?