

---

**WITNESS STATEMENT**

**(CJ Act 1967, s.9; MC Act 1980, ss5A(3)(a) and 5B, MC Rules 1981, r70)**

**Statement of** Dr. Andrew Blyth, B.Sc(Hons), M.Sc, Ph.D.

**Age of witness** Over 18. **Occupation:** University Lecturer.

**This statement (consisting of 4 pages each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have willfully stated in it anything, which I know to be false or do not believe to be true.**

**Date:** 10<sup>th</sup> January 2008

**Signed:** Dr. Andrew Blyth

---

**1. Introduction**

1.1 I (Dr. Andrew Blyth) hold a B.Sc. in Computer Science, an MSC in Computer Software and Systems Design and a PHD in Computer Science. I am head of the Information Security Research Group at the Faculty of Advanced Technology, University of Glamorgan.

1.2 The University has been asked by Richard Webber of Euro-Recycling to forensically analyze the four computer hard drives using standard forensic tools such as Encase and Access Data.

1.3 Four Computer hard-Drives were supplied to the University in various states of repair.

**Signed:** Dr. Andrew Blyth

**Date:** 11th January 2008

## **2. The Computer Hard Drives – Disk 1**

2.1 The 1<sup>st</sup> computer hard-drive (Labelled T2362006) and had been physically shredded. I was unable to recover any data from this computer hard-drive due to its extensive physical damage.

## **3. The Computer Hard Drives – Disk 2**

3.1 The 2<sup>nd</sup> computer hard-drive (Labelled S/N WMA0M 170 8919 – Wiped DOD 5220.22). This was a Western Digital Disk. That had had 2 holes punched into it.

3.2 Due to the physical damage of the computer hard drive, it was impossible to power the disk-up and thus I was unable to forensically analyse hard-drive using tools such as encase and access data.

## **4. The Computer Hard Drives – Disk 3**

4.1 The 3<sup>rd</sup> computer hard-drive (Labelled S/N K20SW7KC– Wiped Random Data). This was a Maxtor Disk. That had had 4 holes punched into it.

4.2 Due to the physical damage of the computer hard drive, it was impossible to power the disk-up and thus I was unable to forensically analyse hard-drive using tools such as encase and access data.

## **5. The Computer Hard Drives – Disk 4**

5.1 The 4<sup>th</sup> computer hard-drive (Labelled S/N A3B572BC– Wiped DOD 5220.22).

5.2 This computer hard (the 4<sup>th</sup> Disk) is physically undamaged and thus, it was possible to it power up and, to connect it via an IDE Write Blocker.

5.3 Using Encase Version 5.0. I was able to create a forensic image of the computer hard-drive. The imaging details are as follows:

Description:	Physical Disk, 12594960 Sectors, 6GB
Logical Size:	0
Physical Size:	512
Starting Extent:	0S0
Drive Type:	Fixed
File Integrity:	Completely Verified, 0 Errors
Acquisition Hash:	18a58525319ab45e7e5c03fb6f017a46

**Signed:**

Dr. Andrew Blyth

**Date:** 11th January 2008

Verify Hash: 18a58525319ab45e7e5c03fb6f017a46  
Total Size: 6,448,619,520 bytes (6GB)  
Total Sectors: 12,594,960

- 5.4 This disk had been forensically wiped. This had been achieved with a constant string of zero's (Hex 0x00) being written to the computer hard-drive. The effect of this type of data erasure is to forensically remove all evidence from the hard-drive.

**Signed:**

Dr. Andrew Blyth

**Date:** 11th January 2008