1
Introduction

The field of digital evidence, aka Forensic Computing, is unlike most other forensic sciences because the nature of the material under examination is determined, largely, by human ingenuity. Rather than looking for traces of material deposited by physical or biological entities, which tend to develop and evolve slowly, we deal with technology which is updated, enhanced and even created at an alarming rate.

Since the 1960s, the rate of development of digital technology has held true to Moore's law [32], which originally proposed that the density of transistors on a given area of silicon would double approximately every 18 months. Since the start of the 21st century, the rate has slowed slightly, but we still see a doubling in density every two years.

This means that a modern mobile phone can contain more processing power and storage capacity than the computers which NASA used to send man to the moon. In a device a fraction of the size. At a much lower price. And easier to use. With greater reliability. And a smaller power supply.

1.1 Key developments

The time when only nerds or geeks[1] were interested in computers is long gone. Advances in computer usability have led to the development of digital

[1] A geek is a nerd with social skills, and an extrovert geek looks at *your* shoes when he/she is talking to you.

Digital Forensics: Digital Evidence in Criminal Investigation Angus M. Marshall

devices which are no longer the sole preserve of the white-coated "high priests" of computing (once known as the programmers and operators), but have become accessible to everyone capable of holding a mouse or using a keyboard.

Increasing dependence on computers can, arguably, be traced back to the late 1970s and early 1980s with the development of machines such as the Apple][, Lisa and Macintosh; Sinclair ZX81 and Spectrum; Commodore Vic20, 64 and Amiga and, finally, the IBM Personal Computer [8].

The IBM PC, with its standardised low-cost hardware, simple Microsoft Disc Operating System (PC-DOS or MS-DOS) and the backing of the world's largest computer manufacturer, resulted in a host of imitators and compatible machines targeted mainly at business.

It seems that Pournelle's law[2] was perceived to be true in business. The creation of low-cost machines that allowed users to perform common computing tasks on their desktops, without having to wait for time on the company mainframe or mini-computer, led to the first steps towards pervasive computing: "computing anywhere and everywhere".

The success of these IBM-compatible PCs with Microsoft operating systems and applications created a de-facto standard, never before seen, which allowed free exchange of data and information between systems, people and organisations, thus eliminating one of the biggest barriers to information exchange.

Standardisation of software and data created opportunities for "paperless offices", where every member of staff had access to computing resources on the desktop – often linked to a local area network – connecting machines within an office or building for even greater resource sharing and efficiency.

Meanwhile, since the 1960s, work had been progressing on what we know today as the Internet [43]. This wide area network began life as an academic project designed to allow data sharing between distant sites, but in a way which allowed the network to be scaled up to include millions of machines. Again, this created a de-facto international standard for networking through the creation of an easy to use system which allowed developers to

[2] "At least one CPU per user" – Jerry Pournelle, science fiction author and BYTE columnist, 1978.

add new features without compromising the existing network. In effect, the Internet provides a global "road network" which is capable of carrying any type of traffic which can be devised.

Prior to 1989, however, the Internet was largely the preserve of the technically minded, mostly because of the huge number of incompatible applications which existed on it. Tim Berners-Lee, a British physicist working at CERN, proposed a new information management system [5] for CERN to counter the problems of information loss, damage and confusion which the organisation was suffering at the time.

The proposal defined an information sharing system which allowed disparate information systems to be linked together via a common interface based around the concept of HyperText [4].[3] In a HyperText system, the user can navigate around the text by activsting links, which jump to other pieces of text. Berners-Lee's innovation was to allow these links to reference documents and even applications external to the current document. In this way, the World Wide Web as we know it was born, with a single consistent interface to a range of different applications. Arguably, this is the single most important innovation in information systems in the 20th century. It has certainly led to the widespread adoption of Internet services as a part of everyday life.

Alongside, and slightly behind, the developments in desktop computing and internetworking, the continual shrinking of components created opportunities for smaller devices to be created. In the 1980s we saw the creation of the first analogue mobile telephony networks, with a proper launch in the UK in 1982. Although the devices in use were bulky with very limited battery life (typically a few hours), poor network coverage and susceptible to interference and eavesdropping, they were well-received and became essential tools for modern business. 1982[4] also saw the launch of the compact disc (CD) by Philips, setting a new standard for audio and data storage. The thirst for increased capacity in this convenient disc format led to the later creation of the Digital Versatile Disc (DVD) and the current battles over High-Definition disc standards.

[3] The term HyperText was coined around 1965 by Ted Nelson, but the concept is older.

[4] A very good year – it also saw the launch of the author's favourite car: the Lotus Excel.

By the 1990s, the GSM[5] [18] standard had been developed for digital mobile telephone networks, providing better quality and better use of the available networks where it was implemented. Continued improvements in technology meant that digital handsets had shrunk in size to become devices which could fit into a briefcase or pocket, with longer battery life and lower cost.

The Internet and the existence of a workable digital telecommunications network, combined with increasingly powerful low-cost devices, also created a desire to distribute more complex data in the form of music, photographs and video. Unfortunately, although the communications technologies were effective, they had not been designed with real-time high-quality audio and video in mind. As a result, it became necessary to develop compression methods such as MPEG [33] which would allow acceptable quality content to be delivered over low-bandwidth connections. The same technology is currently being used for broadcast digital television and is used to allow multiple digital channels to occupy the same bandwidth as a single analogue channel (although the analogue and digital signals cannot be present at the same time). Inadvertently, the MPEG2 standard for digital video had a major impact on the music industry through the creation of a new standard for digital audio – MP3 (MPEG2 layer 3).

The 1990s also saw some major changes in operating systems. Microsoft finally released its "Chicago" software, better known as Windows 95, setting a new baseline for the IBM-compatible world. This included networking in a format which was relatively easy to set up, and considerably easier than the previous Windows 3.11 and Windows for Workgroups systems, which had relied on support being provided by their underlying DOS. Developments of Windows 95 strengthened network and hardware support through Windows 98 and ME until the "home" platform converged with Microsoft's professional operating system (Windows NT) to create Windows XP and, at the start of the 21st century, Windows Vista.

Most recently, a new development in wired telecommunications has driven down the cost of high-performance internetworking to the point where it has become affordable for domestic users. Broadband xDSL

[5] Global System for Mobile Communications.

technology, in the form, mainly, of ADSL (Asymmetric Digital Subscriber Line), offers a high-speed digital connection using existing telephone wiring. It offers an always-on connection, for those who want it, and allows consumers to receive more complex, "richer" content, in the form of video and other media, than was previously possible using slow dial-up connections. The increased speed also means that it has become properly possible for someone to work at home as efficiently as they could in an office. The network connection to their home computer is not as fast as the one they would have in the corporate network, but the speed is sufficient for them to access core corporate services such as e-mail.

1.2 Digital devices in society

The result of 40 years of innovation, as outlined above, has been a move towards an increasingly technology-dependent society. It is rare to find anyone who does not have access to some form of computing device, be it in a vehicle (engine management in a modern car), for personal entertainment (MP3 music player, CD player, DVD player etc.), personal communications (mobile telephone), personal computing or lifestyle management (Personal Digital Assitants and smartphones).

Individuals depend on digital technology to manage their personal financial affairs, ensure that goods are in shops for them to purchase and to schedule transport and other activities efficiently. We use mobile phones to communicate, wherever we happen to be, laptop/notebook computers and PDAs to work in any location and the Internet for communications, entertainment and business 24 hours a day, 7 days a week.

From a situation where activities were generally constrained to the immediate local geographic area, we have evolved into a society which operates globally but carries out activities locally. People never actually have to meet or even speak directly to each other, but can interact via e-mail, chatrooms and online ecommerce systems. Even in the preparation of this book, there has been only one face-to-face meeting. All other discussion, negotation etc. has been carried out using online systems.

Business, industry and commerce are now almost completely dependent on digital technology as a core part of their activities. Without the systems

responsible for accepting and processing orders, controlling stock, issuing invoices and managing financial transactions, most businesses would start to suffer a cash-flow crisis within a matter of days.

Honest citizens and criminals alike have equal access to the technology, constrained only by cost and availability. Fortunately, most criminals make use of the technology for mainly legal purposes, but a few choose to use it to support their criminal activities. We shall explore some of the opportunities this creates in later chapters.

No matter how the technology is used, however, it always records some detail of what it is doing and when it is done.

1.3 Technology and culture

Although much technology evolution has been driven by the desire for lower power, higher capacity or greater efficiency, the emergence of consumer-oriented technologies such as Apple's iPod, mobile phones and similar personal devices has resulted in a merging between technology and fashion. In many cases, particularly among the younger members of society, it is no longer enough to have a device, but it is now necessary to have the "right" device. In the same way that people express their common interests and membership of a particular cultural group through clothing and make-up, design features of personal technology can be viewed as an expression of membership of such a group.

Indeed, since the technology has become so personal, possession of the correct device is perceived by some as an essential adjunct to participation in their chosen peer group. Teenagers, especially, seem to view their personal mobile phone as exactly that – a *personal* device which is guarded jealously, perhaps because it gives them a private communications channel to their peers – but only if it is the *right* make and model.

These personal technologies have also changed the way we communicate. There can be few people who have not witnessed the sight of a gang of teenagers walking down the street, heads down, silent apart from the hushed clicking as their thumbs fly across their mobile phone keypads sending and receiving SMS[6] messages.

[6] Short Message Service, aka text, aka txt.

1.4 Comment

We seem to have arrived at a time when society is dependent on technology, not so much through need as through choice. We have driven the development of more efficient, cheaper and smaller devices because they seem to make our lives easier. The cost, however, is that we have changed the way we live to such an extent that we must have such devices in order to continue living the way we want to. Those devices, like it or not, monitor almost everything we do and can store pretty accurate records about our movements and interactions. Our technological assistants, therefore, might be viewed as unsleeping witnesses.