

Tony Sammes and Brian Jenkinson

Forensic Computing

A Practitioner's Guide



Tony Sammes and Brian Jenkinson

Forensic Computing

A Practitioner's Guide



Springer

A.J. Sammes, BSc, MPhil, PhD, FRCS, CEng
Head, Department of Informatics and Simulation, Royal Military College of
Science, Cranfield University, Shrivenham, Swindon, Wiltshire SN6 8LA, UK

B.L. Jenkinson, BA, BSc (hon), MFCs
Forensic Computer Consultant, Detective Inspector (retired), former head of
Cambridgeshire Constabulary Fraud Squad, Chairman of the Forensic
Computer Group Training Committee and member of the ACPO Computer
Crime Group.

ISSN 1439-9245

ISBN 1-85233-299-9 Springer-Verlag London Berlin Heidelberg

British Library Cataloguing in Publication Data

Sammes, A. J.

Forensic Computing: a practitioner's guide. -

(Practitioner series)

1. Forensic science - Data processing. 2. Microcomputers

I. Title II. Jenkinson, B.

363.2379285416

ISBN 1852332999

Library of Congress Cataloging-in-Publication Data

Sammes, A. J.

Forensic computing: a practitioner's guide / A.J. Sammes and B. Jenkinson.

p. cm. - (Practitioner series)

Includes bibliographical references and index.

ISBN 1-85233-299-9

1. Forensic engineering--Data processing. I. Jenkinson, B., 1950- II. Title. III. Series.

TA219 .S56 2000

363.25--dc21

00-617363

Apart from any fair dealing for the purposes of research or private study or criticism or review, as
permitted under the Copyright, Designs and Patents Act 1988, this publication may only be
reproduced, stored or transmitted, in any form or by any means, with the prior permission in
writing of the publishers, or in the case of reprographic reproduction in accordance with the
terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction
outside those terms should be sent to the publishers.

© Springer-Verlag London Limited 2000

Printed in Great Britain

2nd printing 1991

3rd printing 2002

4th printing 2003

5th printing 2004

The use of registered names, trademarks etc. in this publication does not imply, even in the
absence of a specific statement, that such names are exempt from the relevant laws and regula-
tions and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the
information contained in this book and cannot accept any legal responsibility or liability for any
errors or omissions that may be made.

Typesetting: Ian Kingston Editorial Services, Nottingham UK

Printed and bound by the Alden Press Ltd., Garshead, Tyne & Wear

36/3636-543 Printed on acid-free paper: 3728 11328005

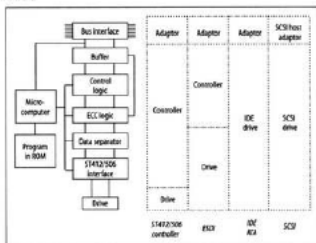


Fig. 5.15 Controllers and drives.

Integrated Drive Electronics (IDE) and AT Attachment (ATA)

The name "Integrated Drive Electronics" or "IDE" was used to signify this placement of all the controller electronics onto the drive itself, as shown in the third column of Fig. 5.15. It is a misleading use of the name (although it is still in very common use today) because other systems, such as the *Small Computer Systems Interface (SCSI)*⁴⁵, also integrate the controller electronics onto the drive, as we have indicated in the fourth column of Fig. 5.15.

A much better term is "AT Attachment" or "ATA", which defines the standard interface between the hard disk IDE system and the AT-style PC to which it is connected. The specification for this interface eventually became defined as an ANSI standard. This was done by the industry in an attempt to eliminate some of the incompatibility problems that surrounded early IDE/ATA drives. These were particularly evident when attempting to install a master and slave on the same IDE/ATA channel using drives from different manufacturers. Very often the disks would not work together.

The original ATA standard specifies:

⁴⁵ SCSI, pronounced "scuzzy", is not just a hard disk interface. It is a flexible and powerful standard (ANSI X3Y9.2) for connecting peripheral devices to computers. Up to eight intelligent devices may be connected to the SCSI bus, one of which is the SCSI host adapter which connects to the PC. SCSI drives are met much less frequently in PC systems than are IDE/ATA drives and most of the problems that are identified in the next section for the IDE/ATA interface do not apply to the SCSI interface. We therefore do not consider it further here.

Mbyte value results. With a more recent translating or extended BIOS the limitations of Logical CHS and Physical CHS geometries taken together no longer need apply since the BIOS can trade excessive cylinder size for spare head capacity⁶². If the drive supports LBA, similar translations can be performed by the BIOS between the legacy Logical CHS interface and LBA. A very modern BIOS will provide the INT 13h extensions and these entail the direct use of LBA. The BIOS will pass LBA addresses direct to the drive, provided that the drive is also able to use LBA. If the drive is not LBA capable, the BIOS will have to translate the LBA addresses into Physical CHS addresses before passing them to the drive.

Communication between the drive and the BIOS is across the IDE/ATA interface. This may use CHS addressing (sometimes known as Physical CHS) and has cylinder, head and sector per track maximum sizes of 65535, 16 and 255 respectively. This gives a theoretical maximum of 127.5 Gbyte. LBA may be used directly if the drive supports this.

Finally, for completeness, we have shown the internal interface between the controller and the disk itself. This may perform sector translation, particularly where zoned bit recording is in use. The Physical CHS addresses specified at the IDE/ATA interface are not, in such cases, an accurate representation of the physical structures inside the drive.

Summary of BIOS Translation Options

Figure 5.20 shows a summary of the translation options that may be carried out by the three different classes⁶³ of BIOS. The old BIOS class can only provide a straight through capability of Logical CHS to Physical CHS. No translation or LBA is possible.

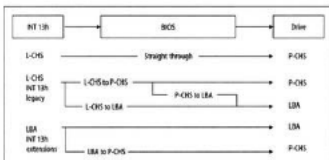


Fig. 5.20 Translation options.

⁶² This form of translation is often marked as *Large* in CMOS setup. Note that the geometry entered in setup should be the Physical CHS and not the Logical CHS. If we set *Auto-detect* the Physical CHS geometry is obtained by the BIOS querying the controller and using the returned results for its translation algorithm.

⁶³ For a more detailed treatment of BIOS types see Landis (1993a).