A CRITICAL EVALUATION OF THE DESTRUCTIVE IMPACT OF COMPUTER VIRUSES ON FILES STORED BY PERSONAL COMPUTER USERS

Thesis submitted in fulfillment of the requirements for the Master's Diploma in Technology (Information Technology) in the School of Business Informatics at the Cape Technikon.

September 1994

Melius Weideman

ACKNOWLEDGMENTS

I would like to thank the following who played a part in this project:

- **My friend and keen computer hobbyist Arend van den Heever, for sparking my initial interest;**
- **My supervisors Mike Mullany, Steve Rossouw and Stuart Warden for valuable guidance all the way;**
- **My student, Wayne Fillis, who assisted me with the laboratory work;**
- **My dear wife Alta for managing the household and supporting me during years of hard work, and**
- **My Creator, for having given me the inclination to start and the stubbornness to finish this project.**

I herewith declare that the research done towards this qualification has been my own work, except where otherwise indicated. All references used were accurately recorded, and any opinions expressed herein are my own and not necessarily those of the Technikon.

MELIUS WEIDEMAN

SUMMARY

Computer virus programs are generally perceived to be a threat to the information stored by computer users. This research evaluated the impact computer viruses have on information stored by computer users. The emphasis was on the effects of computer viruses rather than on the detail of their operation. The main hypotheses involved the question of whether or not computer viruses do pose a threat to the information stored by computer users.

The effect of computer viruses on the information of users in industry was measured by sending a questionnaire to 388 companies country-wide. An average of 21,5% of the respondents claimed detrimental effects to information stored on disk due to computer viruses. This and other data was used to guide laboratory experiments on the actual damage done by computer viruses to stored information.

A set of test disks was prepared to represent programs and data of a typical PC user in industry. Fifteen different virus programs were used individually to infect the test disks. After each infection, all the test disks were inspected to ascertain damage to data, system and program files as well as to separate disk sectors.

The research established that:

- The damage done by computer viruses to stored information is generally limited to one file or disk area.
- Where damage to stored information did occur, it was often reversible.
- Irrational user responses to virus symptoms provide a large potential source for damage to stored information.
- The availability of master program disks (for program file restoration) and recent, validated data backup is essential to recovery from a computer virus infection.
- A user can solve most problems caused by virus infections if he has a basic understanding of disk structure, i.e. tracks, sectors, sides, the FAT, etc, and of the use of disk utility programs like Norton Utilities or PCTools.
- The fact that some of the findings of prominent virus researchers could not be verified, suggests that virus programs could be unstable.
- Claims regarding the damage inflicted by viruses must be considered to be valid only for a specific copy of the virus under discussion.

The importance of using original application software (to minimize the transfer of viruses and to enable program file restoration), regular back-ups (to enable data file restoration) and basic user awareness (infection prevention, symptoms, the use of anti-viral and utility programs, etc.) was emphasized.

The average PC user should be able to clear up a virus infection without assistance by following the given disinfection procedure. Suggestions for further study include virus origins, generations, mutations, multiple infections, and the effect of viruses on computer networks.

OPSOMMING

Daar word algemeen aanvaar dat rekenaarvirusprogramme 'n bedreiging inhou vir die inligting wat deur rekenaargebruikers gestoor word. Hierdie navorsing het die impak evalueer wat rekenaarvirusse het op inligting gestoor deur gebruikers. Die klem was op die effek van virusse eerder as op die detail van hulle werking. Die hoof hipotese het die vraag aangespreek of virusse 'n bedreiging inhou vir die inligting deur gebruikers gestoor of nie.

Die effek van rekenaarvirusse op die inligting van gebruikers in die industrie is gemeet deur 'n vraelys aan 388 firmas landwyd te stuur. 'n Gemiddelde van 21,5% van die respondente het beweer dat rekenaarvirusse nadelige resultate op hulle gestoorde inligting gehad het. Hierdie en ander data is gebruik om laboratorium eksperimente oor die werklike skade deur rekenaarvirusse aan inligting aangerig te lei.

'n Stel toetsskywe is voorberei, om die programme en data wat deur 'n tipiese PC-gebruiker in die industrie gebruik word te emuleer. Vyftien verskillende virusprogramme is afsonderlik gebruik om die toetsskywe te infekteer. Na elke infeksie is al die toetsskywe geïnspekteer vir skade aan data, stelsel- en programlêers en aan aparte skyfsektore.

Hierdie navorsing het die volgende vasgestel:

- Die skade deur rekenaarvirusse aangerig is oor die algemeen beperk tot een lêer of skyfarea.
- Waar daar wel skade aan gestoorde inligting aangerig is, was dit meestal omkeerbaar.
- Waar gebruikers irrasioneel optree as gevolg van die verskyning van virussimptome, bestaan daar groot potensiaal om skade aan gestoorde inligting aan te rig.
- Die beskikbaarheid van meester programskywe (vir programlêerherstel) en onlangse, getoetste data-rugsteun is essensieel vir die herstel na 'n rekenaar virusinfeksie.
- 'n Gebruiker kan die meeste probleme wat deur 'n virusinfeksie geskep is, oplos indien hy basiese insig het in skyfstruktuur, m.a.w. bane, sektore, kante, die lêertoekenningstabel, ens, en in die gebruik van 'n skyfnutsprogram soos Norton Utilities of PCTools.
- Die feit dat sommige van die bevindinge van prominente virusnavorsers nie bevestig kon word nie, dui op die moontlike onstabiliteit van virusprogramme.
- Bewerings oor die skade wat deur virusse aangerig word moet slegs geldig geag word vir die spesifieke kopie van die virus onder bespreking.

Die belangrikheid van die volgende punte word beklemtoon: die gebruik van oorspronklike programme (om die oordrag van virusse te minimaliseer en om programlêerherstel moontlik te maak), gereëlde rugsteun (om datalêerherstel moontlik te maak) en basiese bewustheid onder gebruikers (voorkoming van virus- infeksies, simptome, die gebruik van anti-virus en nutsprogramme, ens).

Die gemiddelde PC-gebruiker behoort 'n virusinfeksie sonder hulp te kan verwyder deur die gegewe disinfeksie prosedure te volg. Voorstelle vir verdere studie sluit in die oorsprong van virusse, generasies, mutasies, meervoudige infeksies, en die effek van virusse op netwerke.

TABLE OF CONTENTS

CHAPTER ONE ** INTRODUCTION

CHAPTER TWO ** DATA COLLECTION AND ANALYSIS: QUESTIONNAIRE

CHAPTER THREE ** DATA COLLECTION AND ANALYSIS: EXPERIMENTS

CHAPTER FIVE ** IMPLICATIONS AND RECOMMENDATIONS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE ** INTRODUCTION

1.1 BACKGROUND

This research was undertaken to investigate the potential danger that computer viruses pose to the information stored by computer users. Companies in the business community that use computers, value the data stored on their computer systems, and often base business decisions on it. Loss of part or all of this data could lead to inconvenience at best, or have disastrous consequences at worst.

A computer virus has been defined as a computer program which can make a copy of itself without the user's consent (Solomon, 1992). Pozzo stated that a computer virus can spread to other programs, and modify them to include a copy of itself (Pozzo, 1990). Computer viruses have received recent attention in both the popular and the computer media, and a tone of drama is sometimes evident in these reports. Users and readers are often left with the perception that computer viruses pose an unknown danger to the information stored on computer disks. This research investigated the risk posed by computer viruses to stored information.

As far back as the 1960's computer programmers wrote "virus" programs as a game. These programs had the ability to replicate themselves (Cullen, 1989). A program called "Creeper" was identified in 1970 (Whitmyer, 1989) and although it only printed a message on a computer's screen, it did manage to spread through nationwide networks. It was this ability of a computer program to make working copies of itself that coined the term "computer virus".

In 1975 a fiction author described how a "worm" program could spread through a computer network and multiply by itself (Brunner, 1975).

Computer researchers successfully wrote computer programs during 1982 which proved that these programs could have adverse effects, and which could in fact leave "... 100 dead machines scattered around the building" (Schoch & Hupp, 1982:176).

One author in a magazine article invited readers to send $2 in a self-addressed envelope for a copy of a set of guide-lines to write virus programs (Dewdney, 1984:15).

It was only during 1988 that a landmark article in Time Magazine alerted the general public to the existence of these programs (Elmer De-Witt, 1988). The author described how a journalist lost data stored on a diskette as a result of the action of a computer virus program.

Articles started appearing which described the results of so-called "virus infections". In one widely publicized instance, a "worm" program was released on the Internet Network, which links many research institutions in the United States of America and elsewhere (Palca, 1988; Francis, 1989; Spafford, 1989). The result was that approximately 6000 computer systems were halted, causing many wasted man-hours in an attempt to stop the spreading of the worm.

Media coverage of potential virus damage caused concern amongst users. It was claimed that the *Datacrime* virus would adversely affect many users in the USA on Friday the 13th October 1989 (Whitmyer, 1989).

The decline in the price of personal computers resulted in many more computer users having easy access to a computer system. The issue of computer viruses and their effects was no longer restricted to computer laboratories and research institutions. Many cases of "computer virus epidemics", especially at educational institutions, were noted (Radai, 1989; Van Wyk, 1989).

However, at that stage there was a lack of evidence of any serious problems caused by viruses. A data recovery expert claimed that "So far we haven't seen any problems resulting from computer viruses" (Cullen, 1989).

A study in the United States of America to identify college students' perceptions of the computer virus problem (Koo, 1991) reached the conclusion that attention should be given to both ethical and technical issues in the academic sphere. At the same time, a more concerned tone was noted in reports on computer viruses. The head of Scotland Yard's Computer Crime Unit appealed to software vendors to drop their prices. This would reduce software piracy, and as a result, the spread of computer viruses (Watkins, 1993).

A data processing manager was arrested for selling virus source code and other software tools which could assist virus programmers to produce virus programs (Evans, 1993). As a measure against virus infections, a well-known hard disk drive manufacturer attempted to build anti-virus capabilities into the electronics of their latest disk drives (Brown, 1993). The incidence of computer virus infections also appeared to increase. For example, it was claimed that approximately 50% of China's microcomputers have suffered from computer virus attacks (Jones, 1993).

1.1.1 RESEARCH OBJECTIVE

Uncertainty prevailed about the results of computer virus infections in the business sector. One author stated that "The impact of infection of computer systems in industry is less known ..." and "... it is difficult to obtain evidence of the extent to which viruses have spread in organizational settings" (Jones, 1993:192).

It was decided therefore, to determine to what degree users in the business sector have experienced problems with their stored information due to virus infections on their computers. If any problems were experienced, the environment in which they occurred would be simulated in a controlled experiment, to determine the actual effect of the virus infections. If any real risks were identified, recommendations to minimize or eliminate them would be made.

The purpose of this research is thus fourfold:

1.1.2.1 To determine what effect computer viruses have had on computerized information in the business sector.

1.1.2.2 To identify, in controlled laboratory tests, the degree of danger that some of these viruses pose to stored information.

1.1.2.3 To reach conclusions based upon the results of the laboratory tests.

1.1.2.4 To suggest a disinfection procedure for the computer user in the business sector.

1.2 VIRUS CLINIC

1.2.1 OPERATION

During 1990 the investigator received some telephonic enquiries from callers who claimed to have a computer virus-related problem. A record of these calls was not kept, but most of them were from users in the Cape Province.

In an attempt to identify those viruses that were prevalent in the Cape Province, the investigator planned and managed a "Virus Clinic" at the Cape Technikon. An advertisement was placed in a local newspaper to make this service known to the public (The Argus, 1990). It was also advertised to various departments at the Cape Technikon, as well as other Technikons and Universities. This clinic was in operation from May 1990 until March 1992.

1.2.2 RESULTS

Consultation sessions with individuals claiming virus-related problems were scheduled. The results were noted, and are summarized below.

Number of people seeking information only:	6
Number of people with virus-related problems:	21
Total number of responses:	27
Number of cases identified as actual virus infections:	12

TABLE 1-1 **CONSULTATION SESSIONS**

The 12 cases which involved actual infections were analyzed in more detail. In all cases the complainants presented more than one disk to be checked or disinfected.

Virus	Number of responses	Number of disks tested	Number of infected disks
Bouncing Ball	5	405	57
Jerusalem	1	9	4
Stoned	6	37	12

TABLE 1-2 **ACTUAL INFECTIONS**

1.2.3 SUMMARY

It was thus evident that there were computer users who had experienced computer virus-related problems in the Western Cape. Furthermore, the three viruses listed in TABLE 1-2 above appeared to be more common than the others known at the time.

1.3 SEMINARS

The investigator attended various conferences and meetings pertaining to computer viruses.

1.3.1 COMPUTER SOCIETY OF SOUTH AFRICA: WORKSHOP ON COMPUTER VIRUSES.

November 1989, Woodstock Holiday Inn, Cape Town.

At this workshop a spokesperson from Information Systems Management claimed that virus programs were commonplace in South Africa. He made no mention of any research being done on the matter. No evidence was offered to substantiate his claims about the actual incidence of viruses.

The managing director of a local computer support company identified various viruses, and warned that some of them have definite data-destroying capabilities. No research or other evidence was given or quoted to substantiate these statements.

In summary, the statements about the appearance of and danger posed by computer viruses made above were unsubstantiated. They do, however, point to a general concern about the data-destroying nature of viruses.

1.3.2 THE INSTITUTE OF INTERNAL AUDITORS' SEMINAR ON COMPUTER VIRUSES.

22 November 1989, Constantia, Cape Town.

In a discussion on computer viruses and their effects, Von Solms (1989) stressed the importance of guarding one's data. Cascarino (1989) identified various viruses and noted some preventative measures to be taken. Both speakers stressed the data-destroying capabilities of viruses, and mentioned their relevance to the computer auditor function in an organization.

Von Solms demonstrated a simple expert system which produced a brief report on the possibility that the computer memory and/or disks might be infected by specific viruses.

None of the above speakers referred to actual experiences with virus programs, nor to research conducted in the virus field. However, the concern over viruses and their possible destructive action was again evident.

At the end of the seminar, a panel discussion was held. The conclusions reached were limited to two points:

Firstly, that the computer user is ultimately responsible for his own data's safety; and secondly, that the whole computer virus issue is part of Computer Security as an overall topic, and that it should be treated as such.

1.3.3 THE ICIS CONFERENCE ON COMPUTER VIRUSES.

23 November 1989, Eskom College, Midrand, Johannesburg.

The conference leader, Solomon (1989), claimed that the popular press regularly over-dramatized virus-related events in the United Kingdom. However, 120 out of the approximately 200 delegates claimed definite evidence of virus infections at their respective companies. Since no mention was made of the actual destruction of files having taken place, either by Solomon or any one of the delegates, these claims were unsubstantiated.

Solomon demonstrated a variety of different viruses, including those known as *Denzuck*, *Jerusalem* and *Stoned*. *Denzuck* displayed its title on the monitor after booting, without any further obvious symptoms. Although it was not demonstrated, Solomon claimed that *Denzuck* could destroy data on all diskettes which are not of the 5,25-inch, 360-kb type. *Jerusalem* was shown to infect both types of DOS executable files (COM and EXE), causing them to grow in size by 1808 and 1813 bytes respectively. Without a demonstration, it was claimed to delete program files that are run on an infected system with a system date of Friday the 13th.

The *Stoned* virus displayed the message "Your PC is now Stoned!" after having booted from an infected disk some eight to 32 times (depending on the strain). Once again damage to information on 5,25-inch diskettes was claimed without a demonstration.

1.3.4 THE BSS WORKSHOP ON NETWORK SECURITY AND COMPUTER VIRUSES.

5 November 1991, Sandton, Johannesburg.

The workshop was a follow-up of Dr. Solomon's first Computer Virus Conference in the country, held in November 1989. However, this time the emphasis was on networks, back-up, and the effect of viruses on networks. The aim of this workshop was to clarify the emerging uncertainty in the data processing community about virus-related network problems. The damage viruses can cause in a stand-alone situation was also noted. According to Solomon, the press had recently been reporting on some cases of a network having been adversely affected by the presence of a computer virus.

The issue of computer data back-up and the role of viruses in back-up were discussed. The difference between Trojan Horse programs and viruses was mentioned, and the damage caused by viruses explained. It was claimed that some viruses cause trivial damage, which could take up to three minutes to rectify. Others inflicted minor damage, where up to 30 minutes would be needed to restore damaged information.

Various other categories were mentioned, and some methods of guarding against virus infections were suggested.

There is a relationship between illegally copying software and the spreading of virus programs. The problem of software piracy is one that is not easily solved. Various types of piracy exist, e.g. professional, deliberate, casual and accidental. The negative effect that exposed piracy can have on a company's reputation was discussed.

The potential problems that could be caused by the presence of viruses on a network are serious enough to warrant a special effort by both management and users alike.

1.3.5 SUMMARY

The discussions at the first conference (1.3.1 above) were general in nature, and consequently the results were considered to be too broad for further use in this research.

It was decided to ignore the statements made by the speakers at the second and third conferences (1.3.2 and 1.3.3 above), since no evidence about the data-destroying claims was given. The speaker at the last conference mentioned the damage done by viruses, and actually divided the results of various virus infections into classes of seriousness. However, no evidence of this damage was given.

From the discussions at all the conferences it could be concluded that there was concern about the safety of the computer user's data. However, there was a lack of evidence on the destructive element of viruses. As a result, the need for the undertaking of this research was confirmed.

1.4 LITERATURE REVIEW

1.4.1 POTENTIAL THREAT POSED BY VIRUS PROGRAMS

An early report (Bradford, 1988:24) refers to various rumours about viruses, including one that a virus could cause a monitor to overheat and catch fire. At that stage it was claimed that the virus issue ". . . is not anything like a big problem. It is a potential (sic!) big problem."

Another report (Joyce, 1988) lists at least ten academic and a number of American Federal government sites which had been adversely affected by virus infections. The resultant loss of productivity was also mentioned.

One of the first known viruses, the *Brain* virus, is referred to in a description of how a journalist lost "six month's worth of notes and interviews" (Elmer De-Witt, 1988:56). However, the article contains a number of inaccuracies: it refers to a disk as having "360 concentric rings of data" (p56). This statement probably refers to a 360-kb diskette, which has 40 tracks, and not 360. It also refers to Sector 0 as being on the "disk's innermost circle" (p56), while it is in fact on the outermost track.

These mistakes point to a degree of lack of insight into the technical detail of computer disk layout and viruses during the early years of computer virus reporting.

The possible threat posed to the banking industry was considered by Francis (1989:6), who came to the conclusion that "there appears to be no clear-cut answer".

A more recent report (Zajac, 1992:33) considers viruses to be "a real and potential threat to the world" and "a growing global problem". The threat posed by "stealth"-type viruses is outlined by Dvorak (1992), who also described the operation and potential damage done by other types of viruses.

Most of these references hint to the fact that a computer virus can destroy information, and therefore does pose a threat to the user. However, none of these references are specific in that they do not describe exactly what the final result of the virus infection was, how the data was destroyed or what percentage of data on the disk was at risk.

1.4.2 DAMAGE DONE BY VIRUS PROGRAMS

The literature does refer (although sparsely) to the damage done by viruses to users' information (Denning, 1988; Highland, 1989; Radai, 1989). However, it is not generally clear what the actual results of some types of computer virus infections are or what damage they could inflict on stored information.

In an early report on the *Stoned* virus, contradictory claims about the damage done by this virus were made. It was noted that "there was no loss of data", but at the same time "files that had part or all of the data on this track were unreadable" (Highland, 1989:11).

An early instance of the *Jerusalem* virus, and the fact that it would erase all files on a certain date, is discussed by Denning (1988:236). This author also claims that "An eastern medical centre lost nearly 40% of its records to a malicious program."

Highland (1992) describes how damage can be done to sensitive data by attempts to disinfect infected computer systems, rather than by the virus program itself. He states that one way to minimize the threat of computer viruses, is by making use of anti-virus software.

1.4.3 SUMMARY

Information about viruses is becoming more freely available. However, the absence of any material which could guide users in commerce as to exactly what damage they could expect from a computer virus is evident. This fact served as further motivation for this research.

1.5 HYPOTHESES

It became clear that the main focus of the research should be the potential danger that computer viruses pose to the information stored by computer users. As a result the following main hypotheses were formulated for this research:

1.5.1 Computer viruses never pose danger to the stored information of a PC user.

1.5.2 Computer viruses can sometimes pose danger to the stored information of a PC user.

1.5.3 Computer viruses will always pose danger to the stored information of a PC user.

It was considered necessary to expand these hypotheses to make it possible to test them. Some features of the operation of computer viruses were identified. Each one of these features served as a basis for formulating one or more sub-hypotheses. These sub-hypotheses would subsequently be tested. The results would serve to substantiate or refute the main hypotheses stated above. Since the sub-hypotheses were bound to be more specific, disk formats had to be identified. The disk formats chosen for the sub-hypotheses were 5,25-inch 360-kb, 3,5-inch 1,44-Mb, and a 32-Mb hard disk. The 5,25 inch 360-kb type appeared prior to the others, and has been the major storage medium for many PC users. The 3,5-inch format is rapidly gaining popularity, indicated by a sharp drop in price (from R25 per diskette in 1989 to approximately R4 per disk at the time of writing).

It is thus assumed that most users were using one of these two diskette formats. Finally, the usage of hard disk drives has also become virtually essential, hence its inclusion in the test disk set. The technical details about the test disks are given in Appendix C.

The computer viruses discussed in the current literature are claimed first to install themselves into the RAM and then on to the magnetic disk(s) of the computer being infected (Highland, 1989; Radai, 1989). While this research was being conducted, however, the first reports appeared that some viruses do not install themselves into RAM before attempting to infect other files. Since many known viruses do become resident before infecting files and/or disks, the following sub-hypotheses are formulated:

H_{1a}: Each of the viruses being considered can reproduce itself into **RAM**.

H_{1b}: Each of the viruses being considered can reproduce itself on to a **diskette** of the 5,25-inch, 360-kb type.

H_{1c}: Each of the viruses being considered can reproduce itself on to a **diskette** of the 3,5-inch, 1,44-Mb type.

H_{1d}: Each of the viruses being considered can reproduce itself on to a non-removable **hard disk**.

The information found on a magnetic disk can be classified as follows: a system file or area (put there by the operating system), a program file (copied onto the disk by the user) or a data file (created by the user on the disk).

Furthermore, the smallest addressable unit of disk space is one disk sector. If these four types of areas (which together make up all the disk space on a disk) are considered, all the areas which a virus program could occupy are covered.

Since the major objective of this research was to determine whether or not computer virus infections pose a threat to the stored information of the PC user, the damage that could be done by them is of importance.

Thus the following sub-hypotheses were formulated:

H_{2a}: Each of the viruses being considered can destroy or detrimentally affect user **data files** on a magnetic disk.

H_{2b}: Each of the viruses being considered can destroy or detrimentally affect user **program files** on a magnetic disk.

H_{2c}: Each of the viruses being considered can destroy or detrimentally affect **system files** on a magnetic disk.

H_{2d}: Each of the viruses being considered can destroy or detrimentally affect **disk sectors** which do not logically belong together as a file.

1.6 FIELD RESEARCH

To obtain a measure of the situation in commerce and industry regarding computer viruses, a questionnaire was compiled. It was sent to 388 organizations country-wide, including commercial businesses, educational institutions, research institutions and industrial concerns.

The results of this questionnaire are summarized in Chapter Two, and were used to guide the subsequent laboratory experiments.

1.7 LABORATORY EXPERIMENTS

Follow-up studies were undertaken to determine actual results of certain virus infections, with respect to the damage (if any) caused to stored information.

A sample of computer viruses had to be identified for use in the laboratory experiment. Some of the factors used in the selection of this sample are: the results of the field research, and the virus clinic results. The environment of a typical PC user was simulated, and virus infections were introduced on uninfected disks. The infected disks were then inspected and the damage done to files, sectors and system areas was noted in Chapter Three.

1.8 CONCLUSIONS AND IMPLICATIONS

Conclusions were then drawn from these results in Chapter Four. Finally the implications of these results were considered, and appropriate recommendations were made to prevent damage or limit loss due to virus actions in Chapter Five.

1.9 LIMITATIONS

Since MSDOS or PCDOS, as opposed to other operating systems, was marketed as the operating system of choice with the first Personal Computers, it has become the most used platform for millions of PC users world-wide. However, it offered no security or memory protection, and programmers can write DOS-based programs which can perform potentially malicious functions. These include programs by-passing the operating system and writing directly to disk or memory.

DOS-based programs can also install themselves into memory while allowing other programs to execute (so-called Terminate and Stay Resident programs). This situation prompted many software vendors to market anti-virus programs which could combat virus infections on DOS-based computers.

Few cases of malicious programs which run under an operating system other than DOS are known. One author claims a ratio of approximately one to 50 of existing Macintosh viruses compared to viruses on the DOS platform (Daly, 1993). Some current anti-virus programs cater for over 4500 different virus programs - all of them operate under DOS.

A large number of DOS-based anti-virus programs are available. One virus researcher in the United States of America had to use 75 different persons from 55 organizations to test different DOS anti-virus programs for inclusion in a book (Highland, 1993:6).

It is thus clear that computer virus programs are more commonly found under DOS than on other operating systems. Since this research concentrated on the average user, as defined in Appendix A, only DOS viruses were considered. Some cases of viruses affecting networks in some way or another are known (Palca, 1988; Francis, 1989; Spafford, 1989). However, this research attempts to define the implications of virus infections on the data of a single user. Since DOS has been chosen as operating system, this precludes any research on viruses affecting computer network operating systems which are not DOS-based.

1.9.1 VIRUS AND ANTI-VIRUS PROGRAMS

Since anti-virus programs are updated regularly (for example, both Dr Solomon's Anti-Virus Toolkit and McAfee's Scan provide a new version every month), a choice had to be made to standardize on specific versions of the programs used in this research. These versions are listed in Chapter Three.

It should also be noted that some viruses are known to have many derivatives or strains, each owing to program errors in the original code and/or further tampering by prospective virus writers. To ensure valid conclusions within a reasonable time, the investigator used the specific copy of a given virus in his possession as a reference and did not consider more than one copy or mutation of the same virus.

CHAPTER TWO ** DATA COLLECTION AND ANALYSIS: QUESTIONNAIRE

2.1 INTRODUCTION

The prevailing situation with respect to computer viruses in commerce and industry was probed by means of a questionnaire. The feedback from this field study was used to steer the remainder of the research in the right direction.

The questionnaire was compiled and a pilot run done with a Cape Technikon Higher Diploma class of 40 students to obtain feedback about its accuracy and validity. These students had all spent at least three years in obtaining a National Diploma in Computer Data Processing or a B.Sc degree in Computer Science or an equivalent qualification. Furthermore, at the time of this research they were all employed in the computer industry, and familiarity with computers was therefore assumed.

The interpretation of the questions was also tested. The results obtained were used to make adjustments to both the questionnaire layout and questions. A copy of the questionnaire in its final format is included in Appendix D. The questionnaire was distributed to 388 recipients at various companies across South Africa. None of the students who took part in the pilot run received one of the 388 questionnaires.

The following graph depicts the distribution of the questionnaires sent out and those that were returned.

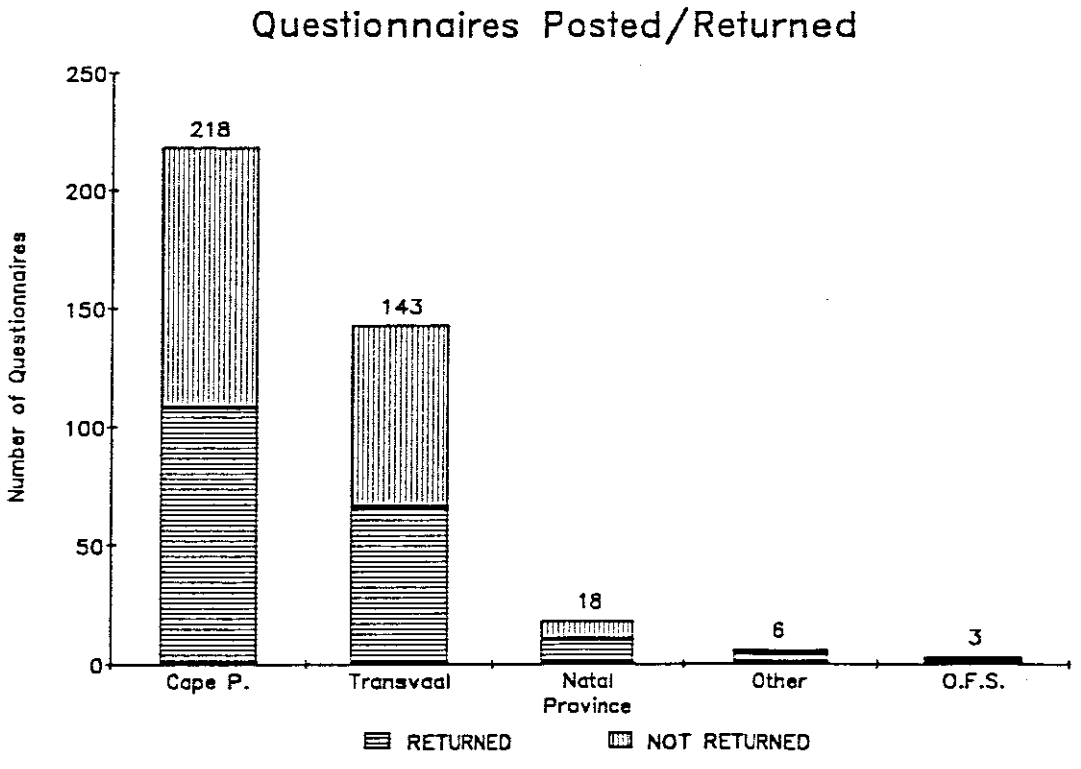

FIGURE 2-1 **QUESTIONNAIRES POSTED AND RETURNED PER PROVINCE**

To ensure relevant results, it was necessary to select only organizations which use computer systems in their business.

Of these questionnaires, 56,2% (218 out of 388) were sent to companies in the Cape Province. The reasons for this are as follows:

- Some of the addresses were those of companies employing Cape Technikon students, which are companies almost exclusively in the Cape Province.

- Other addresses were those of colleagues in the computer industry, most of which are situated in the Cape Province.

- The remaining addresses were obtained from the Computer Society of South Africa address list. This list contained addresses of companies across the country.

The return date was three weeks after the date on which the questionnaires had been posted. A one-month grace period was allowed after the return date, after which the contents of the returned questionnaires were summarized. A total of 190 questionnaires was returned, which is a yield of 49,0% (190 out of 388).

2.2 RESULTS AND DISCUSSION

2.2.1 COMPANY PROFILE

Question 1 of the questionnaire reads: **"What type of business is your company involved in?"**. This question was included to determine the areas of the business and academic world to which the results would be most applicable.

The data obtained with this question is summarized in Fig 2-2. Some respondents marked more than one block for this question (for instance a respondent at a University could have marked Educational and Research). Hence the total obtained when adding the numbers in Fig 2-2 (285) is higher than the number of returned questionnaires (190).

The topic of this research is an investigation of the damage that viruses can cause to users' files. Therefore the exact environment in which the respondents of this field research were involved is not of paramount importance. However, the types of activity in which the respondents are involved are analyzed in order to determine areas most at risk.

The first six categories (Computers/related, Education, Manufacturing, Sales, Research and Banking) account for 54,0% (154 out of 285) of the returns. Both the business and the academic communities were thus involved. It can be assumed that the results of the research are especially relevant to these six types of institution.

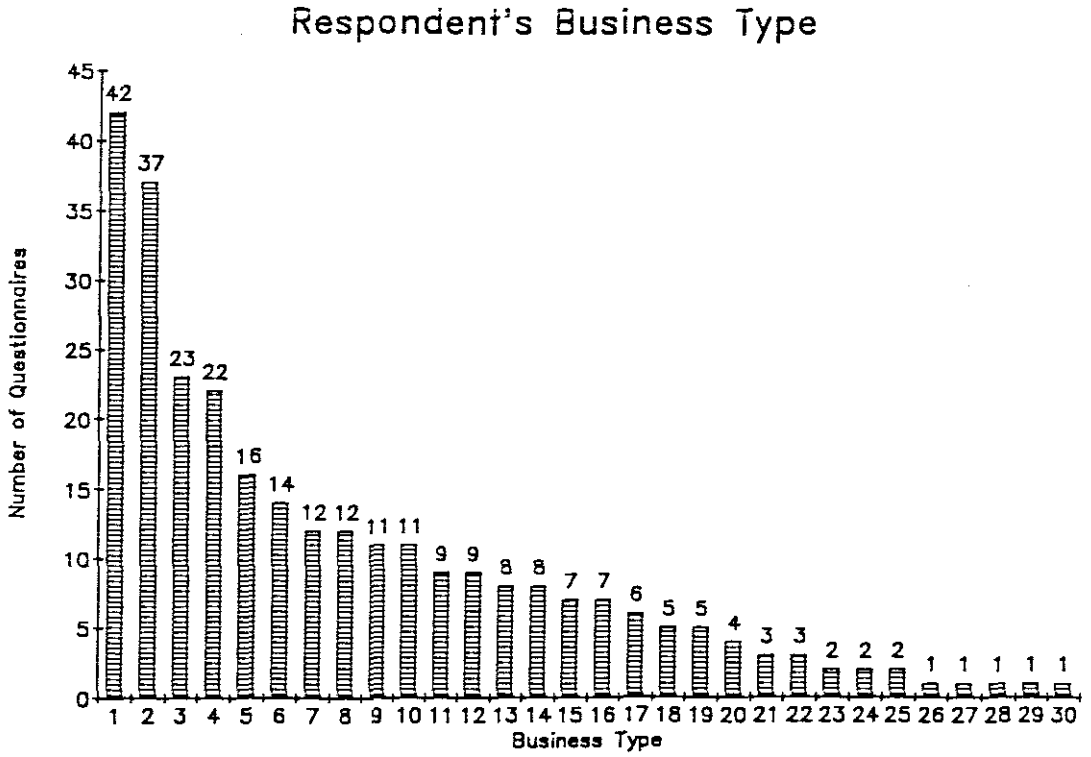

FIGURE 2-2 **RESPONDENT'S BUSINESS TYPE**

Business Type key:

1 Computers/related
2 Education
3 Manufacturing
4 Sales
5 Research
6 Banking
7 Building
8 Medical
9 Food/Liquor

10 Insurance
11 Farming/related
12 Government
13 Engineering
14 Municipal
15 Clothing
16 Energy
17 Mining
18 Entertainment
19 Transport

20 Printing
21 Chemical
22 Marketing
23 Accounting & Auditing
24 Broadcasting
25 Publishing
26 Car Rental
27 Horse-racing
28 Packaging
29 Politics
30 Welfare

2.2.2 COMPANY SIZE

Question 2 of the Questionnaire reads: **"Please indicate the number of personal computers being used in your company, ..."**. This question was included to determine the size of the company, in terms of PC users. The data obtained with this question is summarized in Fig 2-3.

A total of 47,9% of the respondents (91 out of 190) were using more than 100 Personal Computers, and 84,2% (160 out of 190) more than 10.

These figures indicate that a large percentage of the companies which responded had a significant number of PC's in use.

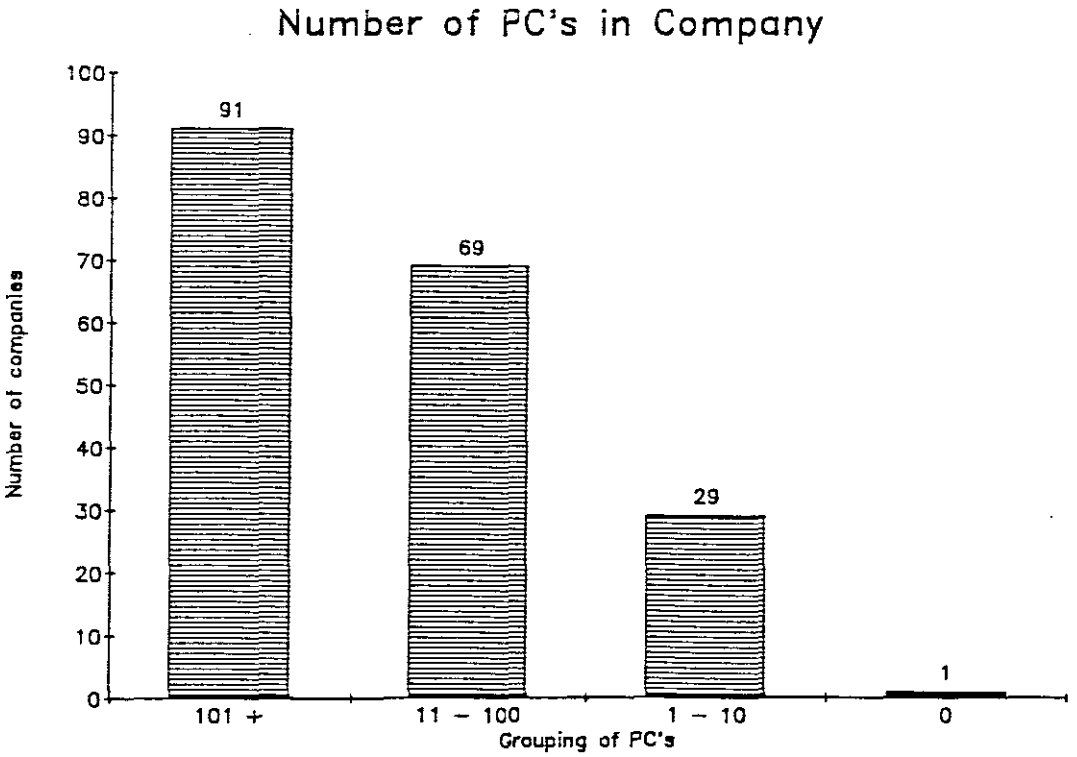

FIGURE 2-3 **NUMBER OF PC'S USED IN COMPANY**

2.2.3 COMPANY'S USAGE OF DOS

As defined in Chapter One, this research focuses only on DOS viruses. It was therefore considered important to determine whether or not the respondent's company did make use of a version of DOS.

Question 3 of the Questionnaire reads: **"Is a version of PCDOS or MSDOS being used as operating system on any one of these personal computers? If you have answered NO or UNSURE to question three above, kindly ignore the remainder of the questionnaire ..."**.

This question was included to ensure that the rest of the questionnaire would not be answered by a respondent whose company does not use DOS at all. The data obtained with this question is summarized in Fig 2-4.

A total of 187 out of 190 (98,4%) of the respondents answered affirmatively. Since it was decided to consider only DOS-based viruses during this research, the answers to the remaining questions are relevant to the focus of this research. Only the 187 responses which were positive will be considered from this point onwards.

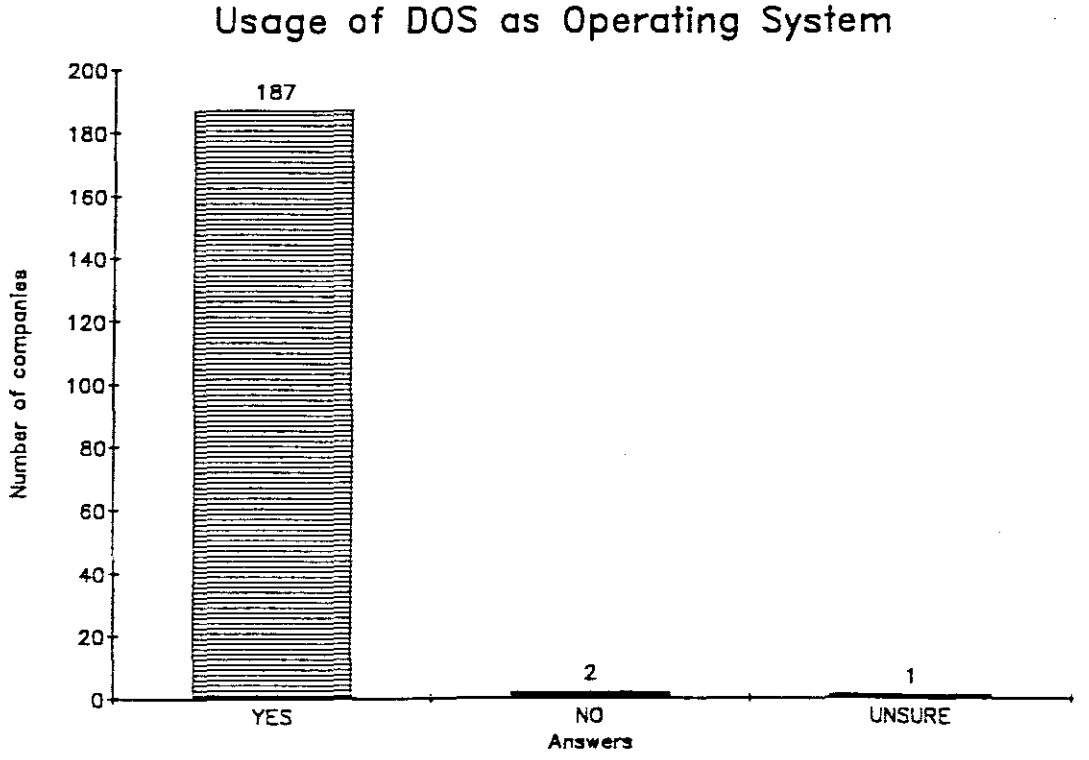

FIGURE 2-4 **PRESENCE OF DOS**

2.2.4 APPLICATION OF PC'S IN COMPANY

Question 4 of the Questionnaire reads: **"What are the personal computers in your company being used for? ..."**. This question was included to determine what the average user environment was in which virus infections took place.

Any one respondent could list more than one application of the computers in his company. Therefore the total obtained was more than 187. These results were to be used to simulate the environment of the average user during the laboratory experiments. The data obtained with this question is summarized in Fig 2-5.

A total of 60,6% (422 out of 696) of the responses indicated the use of Packages (word processing, spreadsheets and databases), Programming and Accounting applications.

The test disks to be used during the laboratory experiments were to be prepared in such a way that they would contain packages, programming tools and accounting applications so as to reflect this fact.

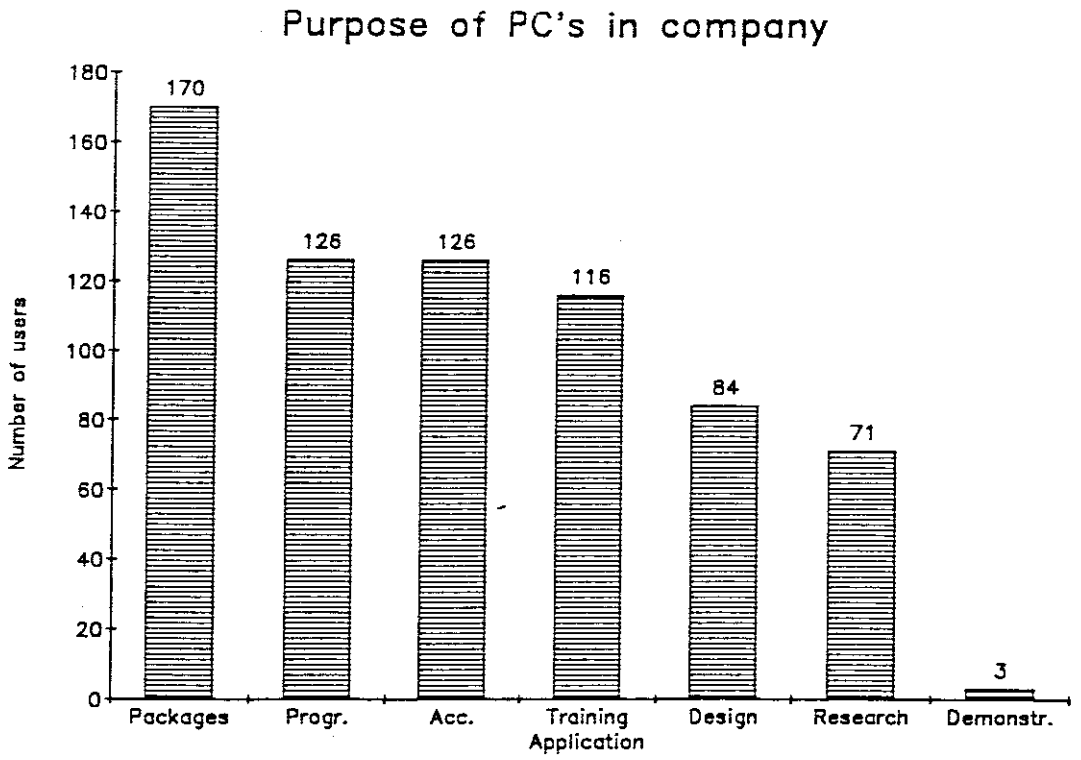

FIGURE 2-5 **PURPOSE OF PC'S IN COMPANY**

2.2.5 NUMBER OF USERS PER PC

Question 5 of the Questionnaire reads: **"Does more than one person use any one personal computer during a typical working day?"**. This question was included to test the presumption that multiple users per computer increase the risk of infection. The data obtained with this question is summarized in Fig 2-6.

A total of 86,6% (162 out of 187) respondents indicated that more than one person did use a particular computer during a typical working day.

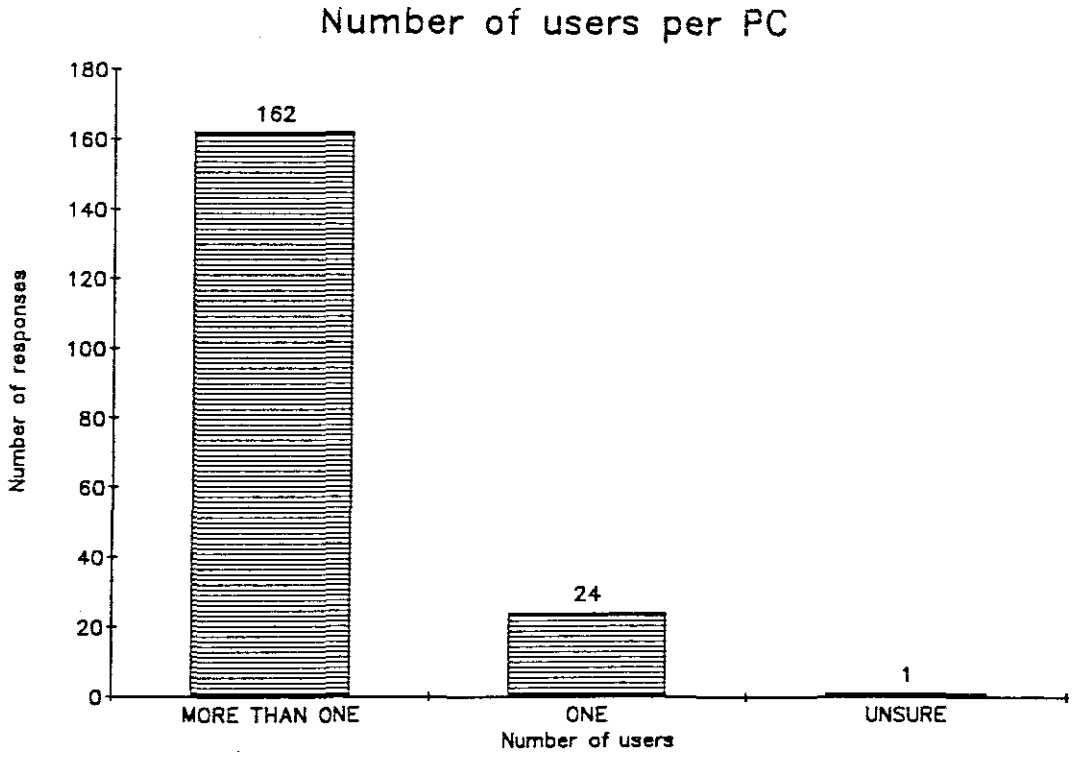

FIGURE 2-6 **NUMBER OF USERS PER PC**

2.2.6 INCIDENCE OF VIRUS INFECTIONS

Question 6 of the Questionnaire reads: **"How many personal computers in your company have had a computer virus infection that you are aware of?"**. This question was included to determine the seriousness of the problem in terms of number of infections per company. The data obtained with this question is summarized in Fig 2-7.

The results indicate that 92,5% (173 out of 187) of the respondents have had at least one virus infection at their work-place.

This high percentage of infections could be ascribed to the high number of respondents (162 out of 187) who confirmed that multiple users make use of one computer (See 2.2.5 above).

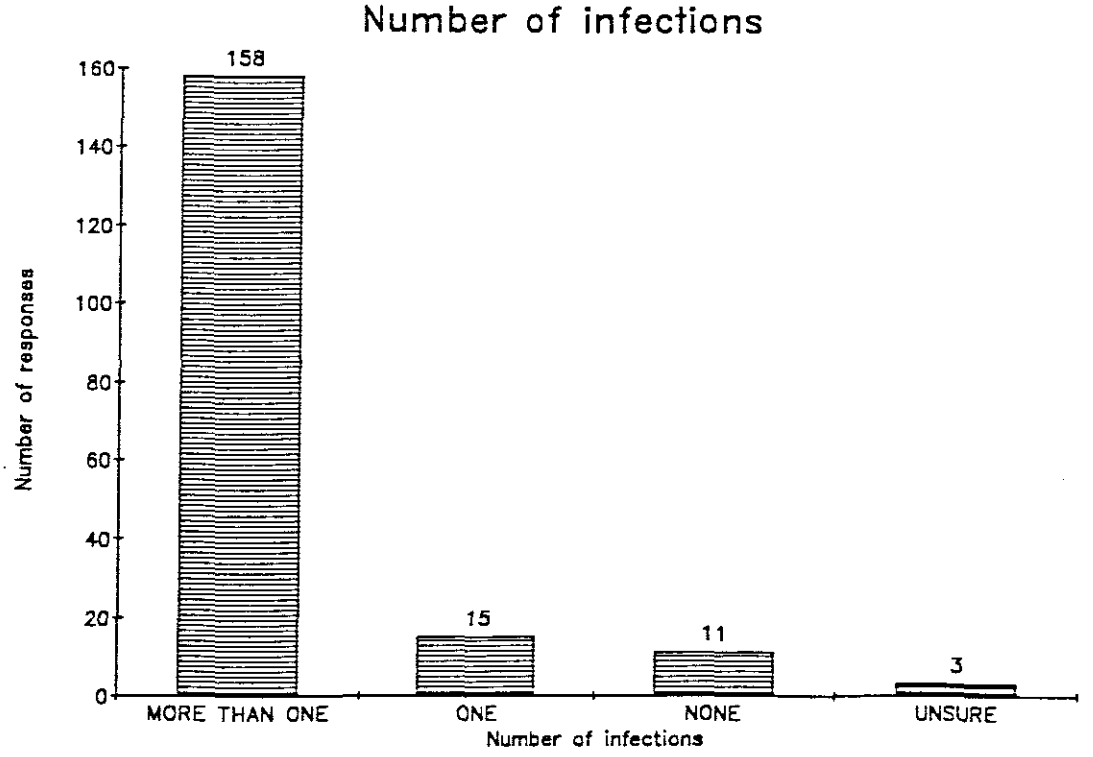

FIGURE 2-7 **NUMBER OF VIRUS INFECTIONS**

2.2.7 BASIS OF INFECTION CLAIM

Question 7 of the Questionnaire reads: **"How do you know that (an) infection(s) did actually take place?"**. This question was included to determine the basis on which the respondent answered the previous question. The data obtained with this question is summarized in Fig 2-8.

From his experience with the Virus Clinic, telephonic enquiries and on-site virushunts done in commerce and industry, the investigator found that many claims of virus infections were false. Often users claimed to have a virus related problem, based on symptoms of another problem on their computer.

In other cases the complainant's ignorance caused him to blame the symptom of a problem which he did not understand on a virus infection. Hence it was considered necessary to require the respondent to supply a motivation for his claims.

Only 39,4% (149 out of 378) of the reasons given were based on the output of an anti-virus program. A further 25,9% (98 out of 378) of the reasons were based on the observation of some well-known virus symptom. Taken together then, 65,3% (247 out of 378) of the responses were based on acceptable motivations. The remaining motivations were considered to be too vague for further consideration. Another 10,8% (41 out of 378) of the 65,3% of responses were considered invalid. Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing.

Examples of such unconvincing motivations are: "Data became corrupt (i.e. data files); . . . hard drive was gone (could not boot up); Autocad would not operate correctly on return from repairs ±18 months ago; . . . Files were corrupt".

Thus, a total of 61,1% (206 out of 337) of the claims was taken to be valid.

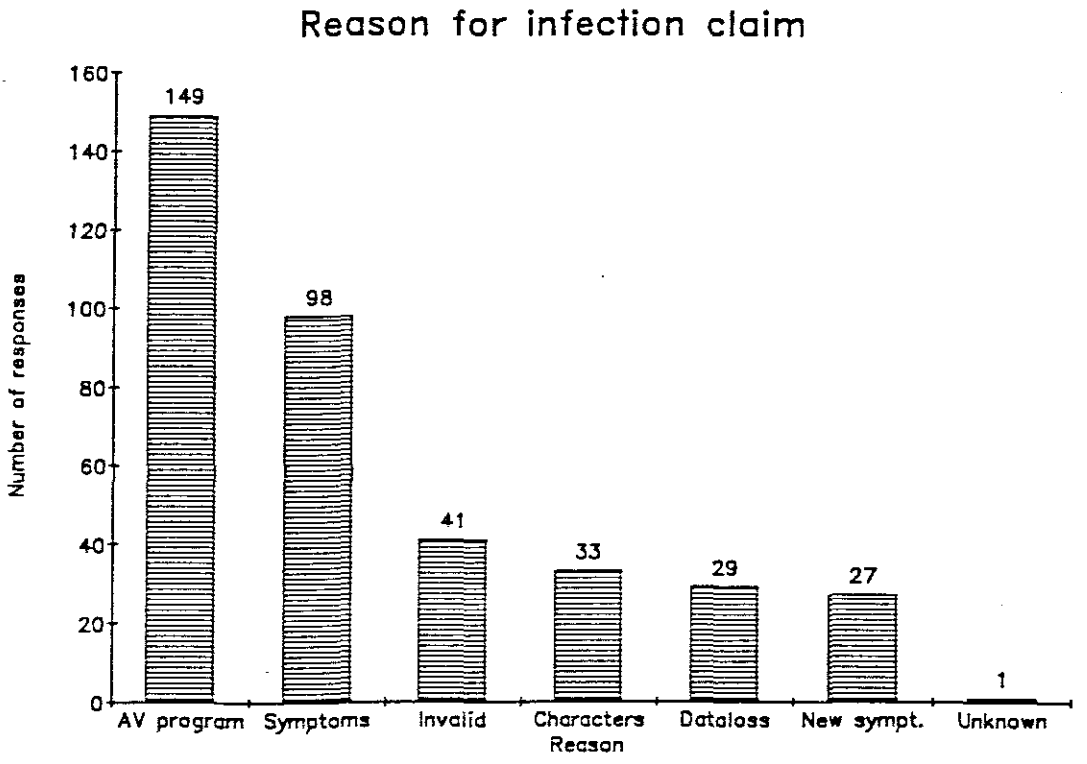

FIGURE 2-8 **REASON FOR INFECTION CLAIM**

2.2.8 DISTRIBUTION OF INFECTIONS

Question 9 of the Questionnaire reads: **"Which virus(es) caused the infection(s)?"**. This question was included to determine which virus programs appeared to be most common in commerce and industry. The most commonly found programs were to be included in the sample used during the laboratory experiments. The data obtained with this question is summarized in Fig 2-9.

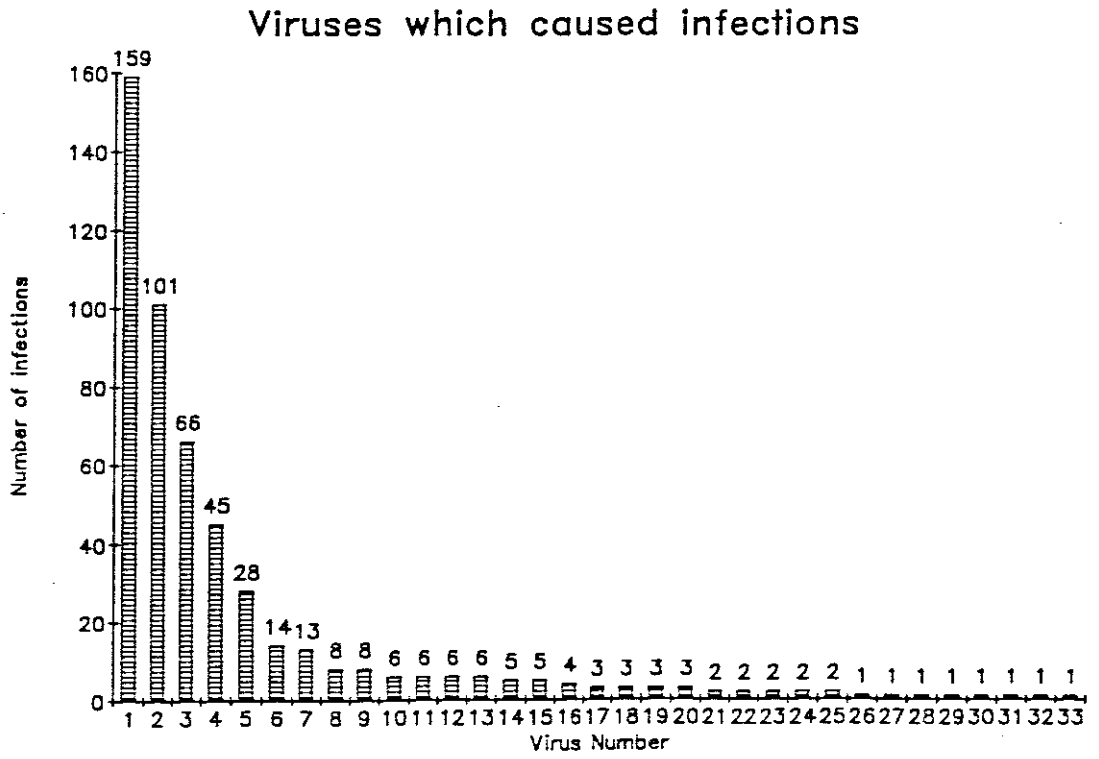

FIGURE 2-9 **VIRUS WHICH CAUSED THE INFECTION**

The virus numbers used in the graph are listed below with the virus it represents.

1	*Stoned*	18	*Anti-Cad*
2	*Bouncing Ball*	19	*Ogre*
3	*Michelangelo*	20	*Vienna*
4	*Jerusalem*	21	*Agiplan*
5	*Plastique*	22	*Azusa*
6	*Sunday*	23	*Green Caterpillar*
7	*NoInt*		
8	*Brain*	24	*Keypress*
9	*Cascade*	25	*Pretoria*
10	*Dark Avenger*	26	*DirII*
11	*Telefonica*	27	*Form*
12	*Unknown*	28	*HongKong*
13	*Durban*	29	*Liberty*
14	*Frodo*	30	*No of the Beast*
15	*Yankee*		
16	*Exebug*	31	*Suriv-1*
17	*Aids*	32	*Tenpast3*
		33	*Vacsina*

It is clear from the results that certain viruses appear to be more common than others. This fact was to be considered in the determination of the sample of virus programs to be used in the laboratory experiment. The viruses which caused most of the infections would be included in the sample.

2.2.9 INSTALLATION OF VIRUS INTO RAM

Question 12 of the Questionnaire reads: **"Did the virus install itself into the main memory (RAM) of the infected computer?".** This question was included to test hypothesis H_{1a}. The data obtained with this question is summarized in Fig 2-10.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 72,7% (136 out of 187) of the infections did involve the installation of the virus program in RAM.

However, 46 of these answers were regarded as invalid. Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing. Examples of such unconvincing motivations are:

"It was found on most of the back-up disks; *Stoned* occurred and therefore seeing this as a bootvirus the virus infected the bootsector (sic!); Whenever the machine was used and eg (sic!) Lotus started a character would disappear and reappear; All the BSV will load into RAM on an infected computer; It will be in RAM everytime (sic!) you boot off an infected hard drive; Mostly boot/partition sector viruses place themselves in ram (sic!) on bootup".

The "INVALID" answers were therefore subtracted from the "YES" answers to obtain a total of 90 reliable "YES" answers. The new percentage is now 48,1% (90 out of 187).

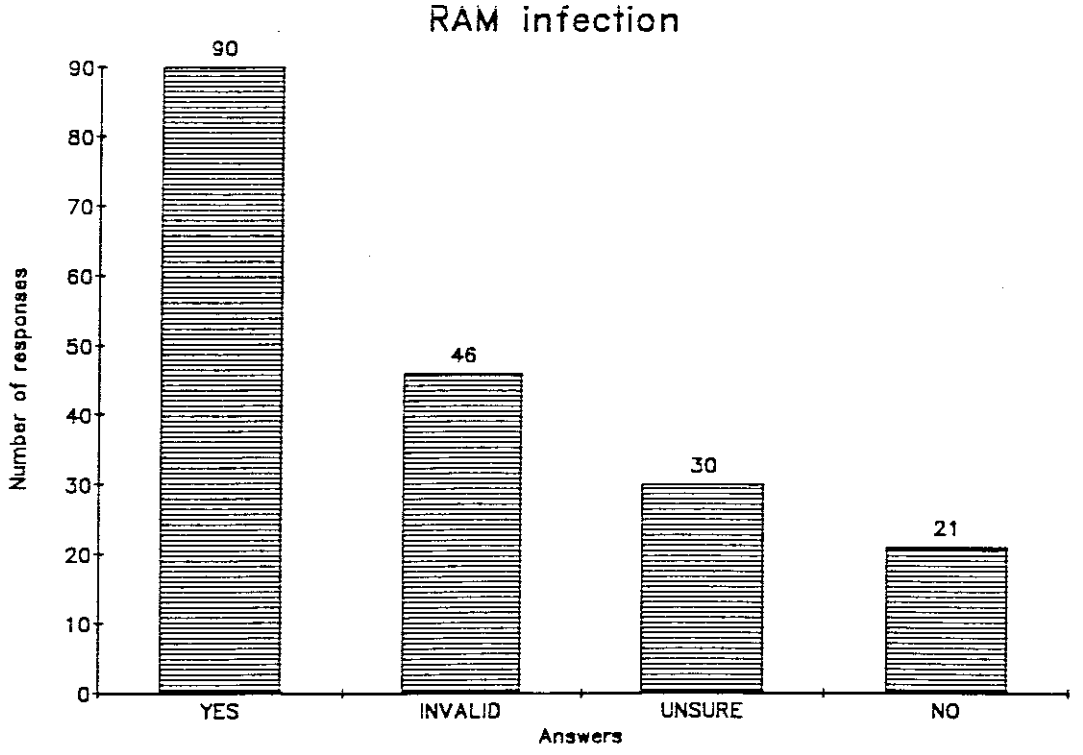

FIGURE 2-10 **INSTALLATION IN RAM**

2.2.10 INSTALLATION OF VIRUS ONTO DISKETTE (5,25-inch)

Question 13 of the Questionnaire reads: **"Did the virus install itself onto a diskette of the 5,25-inch 360-kb type?"**. This question was included to test hypothesis H_{1b}. The data obtained with this question is summarized in Fig 2-11.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 81,8% (153 out of 187) of the infections did involve the installation of the virus program onto a 5,25-inch diskette.

However, 43 of these "YES" answers were regarded as invalid. Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing. Examples of such unconvincing motivations are:

"Because the virus is memory resident any attempt to access a (sic!) external medium like a floppy infects the medium; *Stoned*, & *Italian* will infect any floppy accessed once virus is active; All PC's in use have these diskette drives. There is no other outside input to the equipment; It was transferred to the diskette while files was backup (sic!); By the nature of the virus & antiviral software".

The "INVALID" answers were therefore subtracted from the "YES" answers to obtain a total of 110 reliable "YES" answers. The new percentage is now 58,8% (110 out of 187).

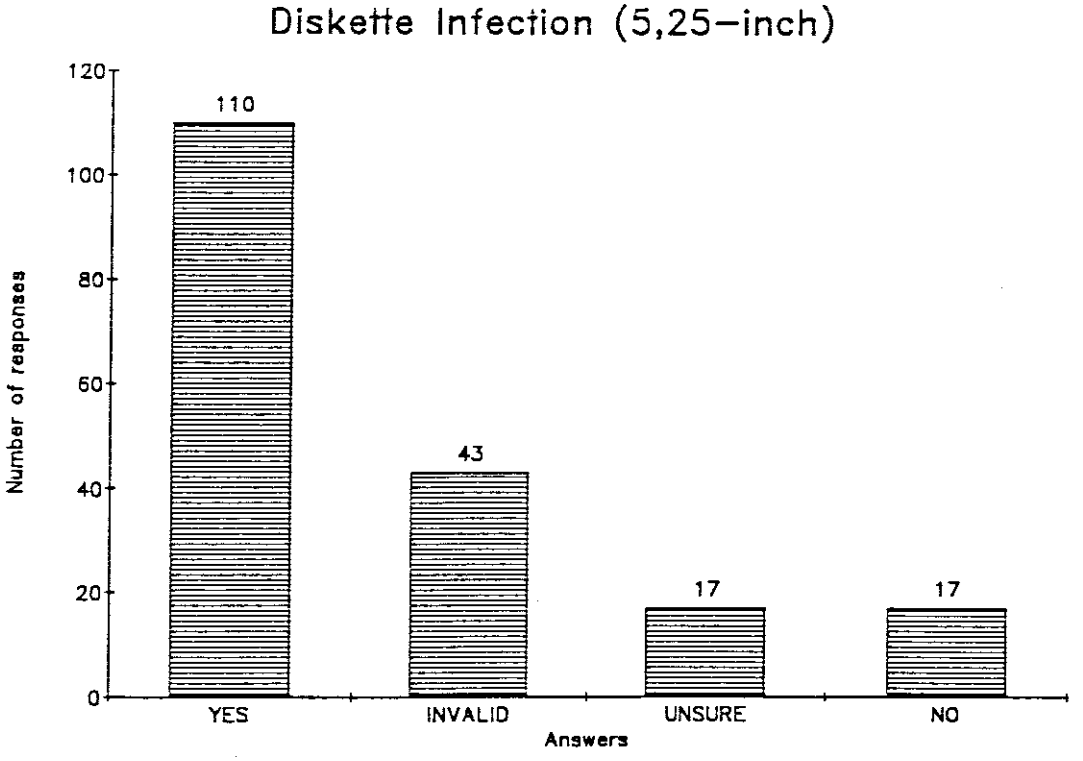

FIGURE 2-11 **DISKETTE INFECTION (5,25-inch)**

2.2.11 INSTALLATION OF VIRUS ONTO DISKETTE (3,5-inch)

Question 14 of the Questionnaire reads: **"Did the virus install itself onto a diskette of the 3,5-inch 1,44-Mb type?"**. This question was included to test hypothesis H_{1c}. The data obtained with this question is summarized in Fig 2-12.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 42,2% (79 out of 187) of the infections did not involve the installation of the virus program onto a 3,5-inch diskette. A further 42,2% (79 out of 187) did claim that infection took place.

However, 25 of these "YES" answers were regarded as invalid. Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all.

Secondly, some motivations were unconvincing. An example of such an unconvincing motivation is:

"While doing backups".

The "INVALID" answers were therefore subtracted from the "YES" answers to obtain a total of 54 reliable "YES" answers. The new percentage is now 28,9% (54 out of 187).

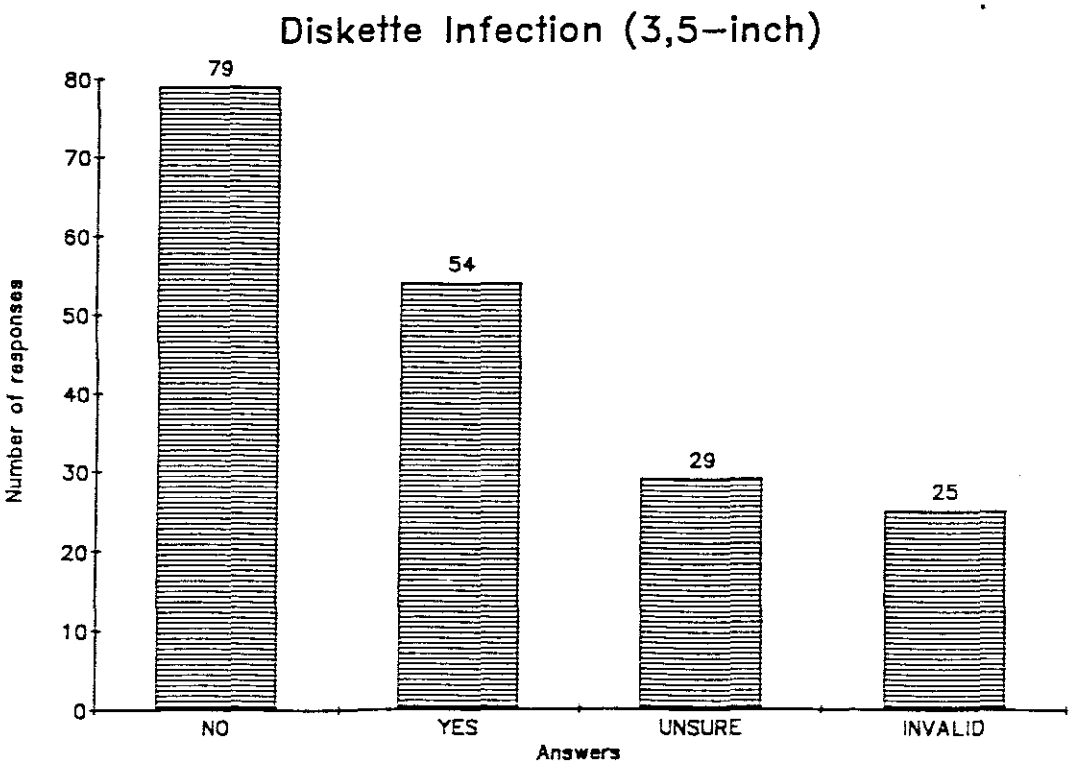

FIGURE 2-12 **DISKETTE INFECTION (3,5-inch)**

2.2.12 INSTALLATION OF VIRUS ONTO THE HARD DRIVE

Question 15 of the Questionnaire reads: **"Did the virus install itself onto the non-removable hard disk drive?"**. This question was included to test hypothesis H_{1d}. The data obtained with this question is summarized in Fig 2-13.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 62% (116 out of 187) of the infections did involve the installation of the virus program onto a hard disk drive. However, 48 of these "YES" answers were regarded as invalid.

Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing. Examples of such unconvincing motivations are:

"Once BSV installed (sic!) (from infected boot floppy) will infect any disk accessed; Wrote itself to partition table; Don't remember".

The "INVALID" answers were therefore subtracted from the "YES" answers to obtain a total of 116 reliable "YES" answers. The new percentage is now 62,0% (116 out of 187).

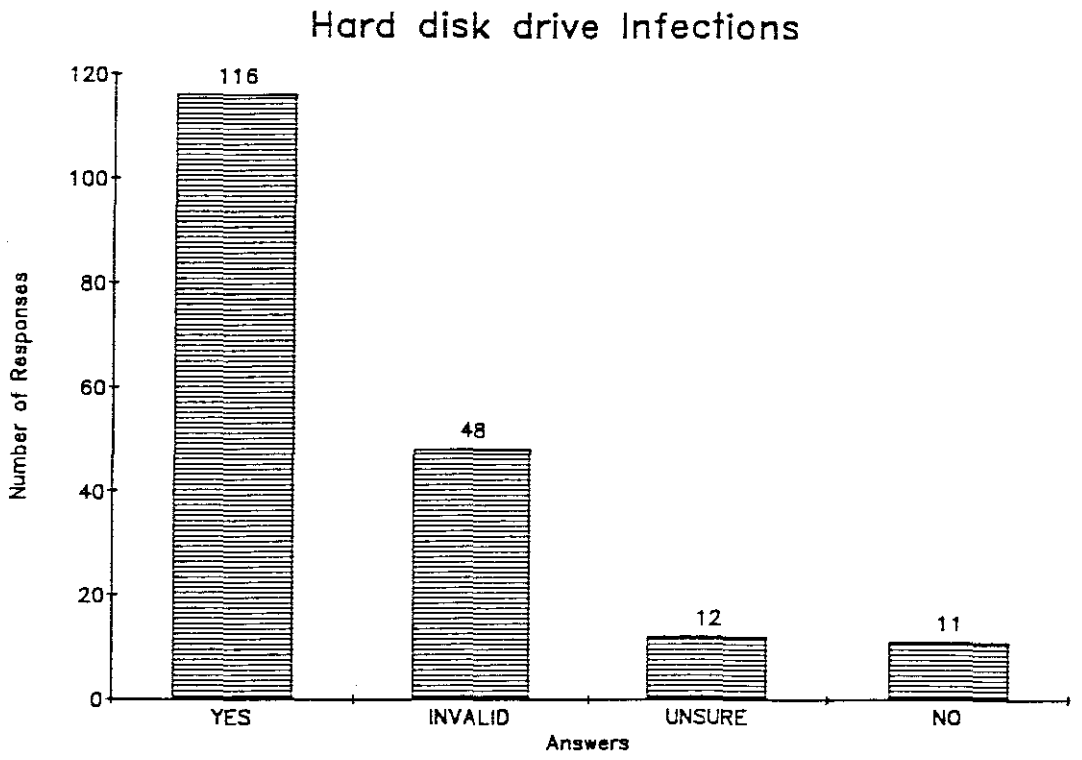

FIGURE 2-13 **HARD DISK DRIVE INFECTION**

2.2.13 *EFFECT OF VIRUS ON DATA FILES*

Question 16 of the Questionnaire reads: **"Did the virus destroy or detrimentally affect any <u>data</u> files on any disk? (e.g. word processor documents, database files, spreadsheets, program source code, etc.)"** This question was included to test hypothesis H_{2a}. The data obtained with this question is summarized in Fig 2-14.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 37,4% (70 out of 187) of the infections did affect data files detrimentally.

However, 26 of these "YES" answers were regarded as invalid. Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing. Examples of such unconvincing motivations are:

"Bootable disk was not bootable any more; In one instance a Lotus data file was corrupted on hard disk.. ; Once, *Stoned* caused corruption of FAT when activated during a disk optimization . . .; Not all PC's had data destroyed; Data files corrupt; Hard disk could not boot up and had to be reformatted; Indexes & data files corrupted".

If the number of "INVALID" responses are subtracted from the "YES" responses, 23,5% (44 out of 187) of the respondents claimed damage to data files, based on acceptable motivations.

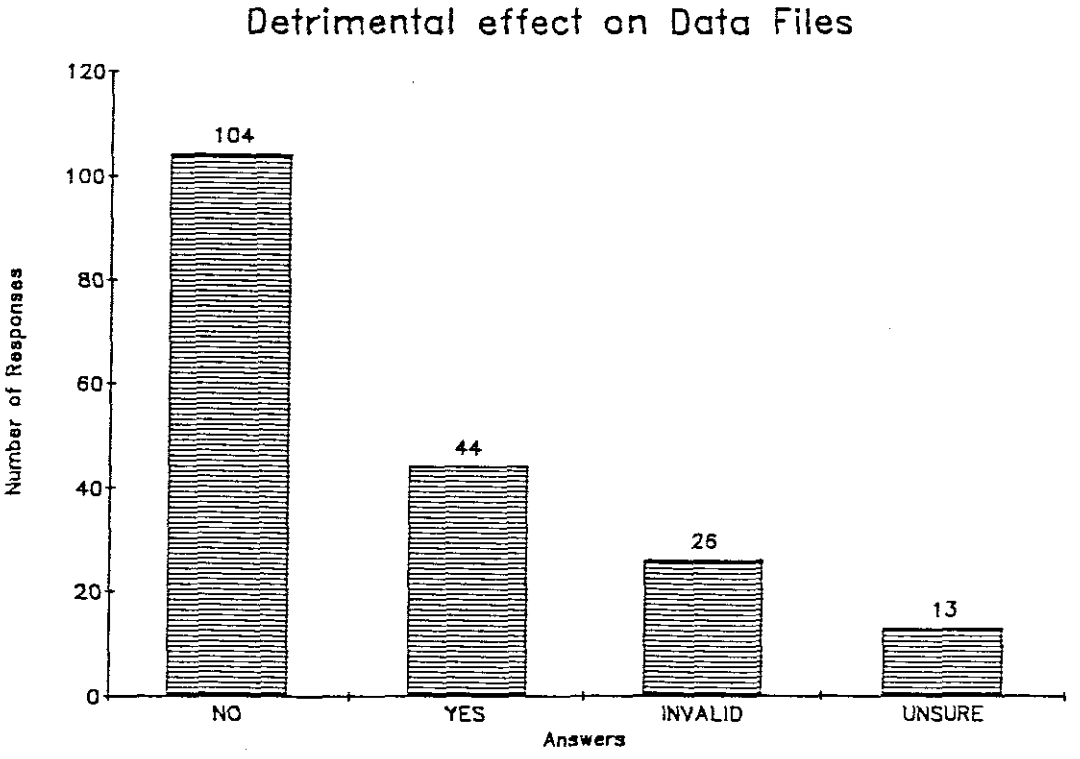

FIGURE 2-14 **EFFECT ON DATA FILES**

2.2.14 EFFECT OF VIRUS ON PROGRAM FILES

Question 17 of the Questionnaire reads: **"Did the virus destroy or detrimentally affect any program files on any disk? (e.g. word processor programs, financial programs, editors, utilities, games, etc)."** This question was included to test hypothesis H_{2b}. The data obtained with this question is summarized in Fig 2-15.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 35,8% (67 out of 187) of the infections did affect program files detrimentally.

However, 19 of these "YES" answers were regarded as invalid. Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing. One example of such an unconvincing motivation is:

"Anticad corrupted some EXE files"

If the number of invalid responses are subtracted from the "YES" responses, 25,7% (48 out of 187) of the respondents claimed damage to program files, based on acceptable motivations.

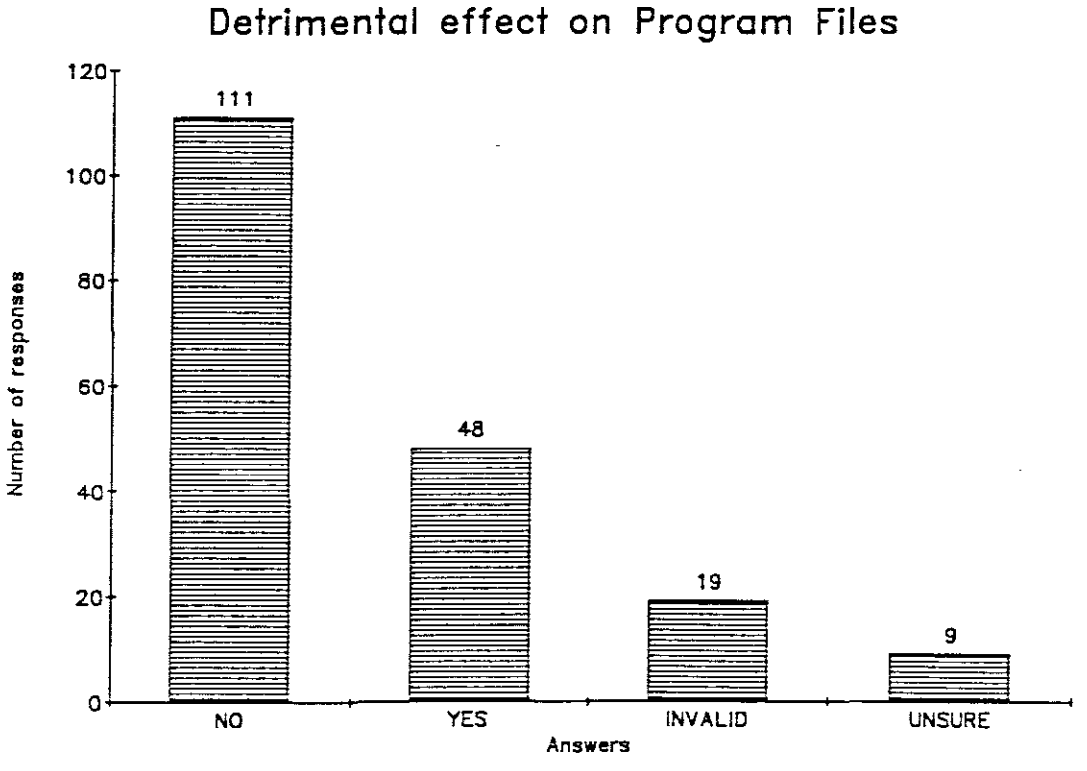

FIGURE 2-15 **EFFECT ON PROGRAM FILES**

2.2.15 EFFECT OF VIRUS ON SYSTEM FILES

Question 18 of the Questionnaire reads: **"Did the virus destroy or detrimentally affect any system files on any disk? (Specifically the three DOS system files: COMMAND.COM, MSDOS.SYS, and IO.SYS)"**. This question was included to test hypothesis H_{2C}. The data obtained with this question is summarized in Fig 2-16.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 40,1% (75 out of 187) of the infections did affect system files detrimentally. However, 31 of these "YES" answers were regarded as invalid.

Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing. Examples of such unconvincing motivations are:

"Boot sector was corrupted; *Italian* A was hidden behind the *Stoned* virus on the boot sector . . .; Command.com. (Difference in size of file)".

If the number of invalid responses are subtracted from the "YES" responses, 23,5% (44 out of 187) of the respondents claimed damage to system files, based on acceptable motivations.

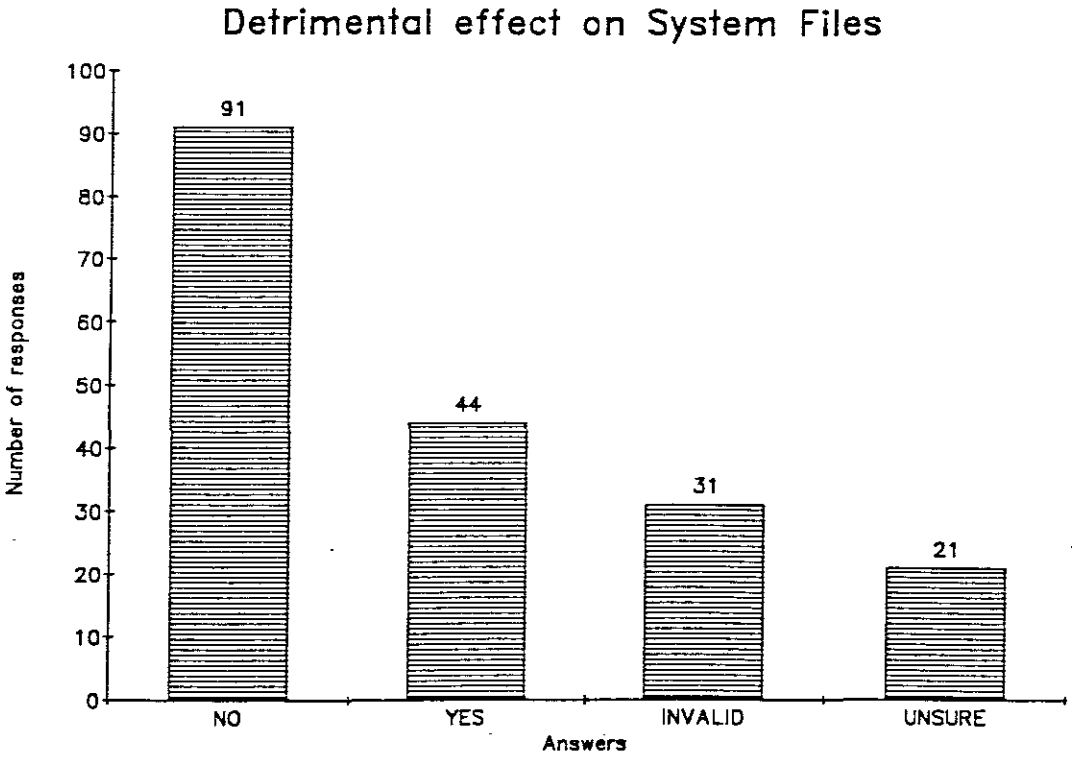

FIGURE 2-16 **EFFECT ON SYSTEM FILES**

2.2.16 EFFECT OF VIRUS ON SEPARATE SECTORS

Question 19 of the Questionnaire reads: **"Did the virus destroy or detrimentally affect any separate disk sectors which do not belong together as a file?"** This question was included to test hypothesis H_{2d}. The data obtained with this question is summarized in Fig 2-17.

If the respondent answered "YES" to this question, he was asked to motivate the answer. According to the respondents, a total of 20,3% (38 out of 187) of the infections did affect separate sectors detrimentally. However, 13 of these "YES" answers were regarded as invalid.

Two reasons exist for these responses being considered invalid: firstly, in some cases a "Yes" answer was given with no motivation at all. Secondly, some motivations were unconvincing. One example of such an unconvincing motivation is:

"Affected the FAT".

If the number of invalid responses are subtracted from the "YES" responses, 13,4% (25 out of 187) of the respondents claimed damage to system files, based on acceptable motivations.

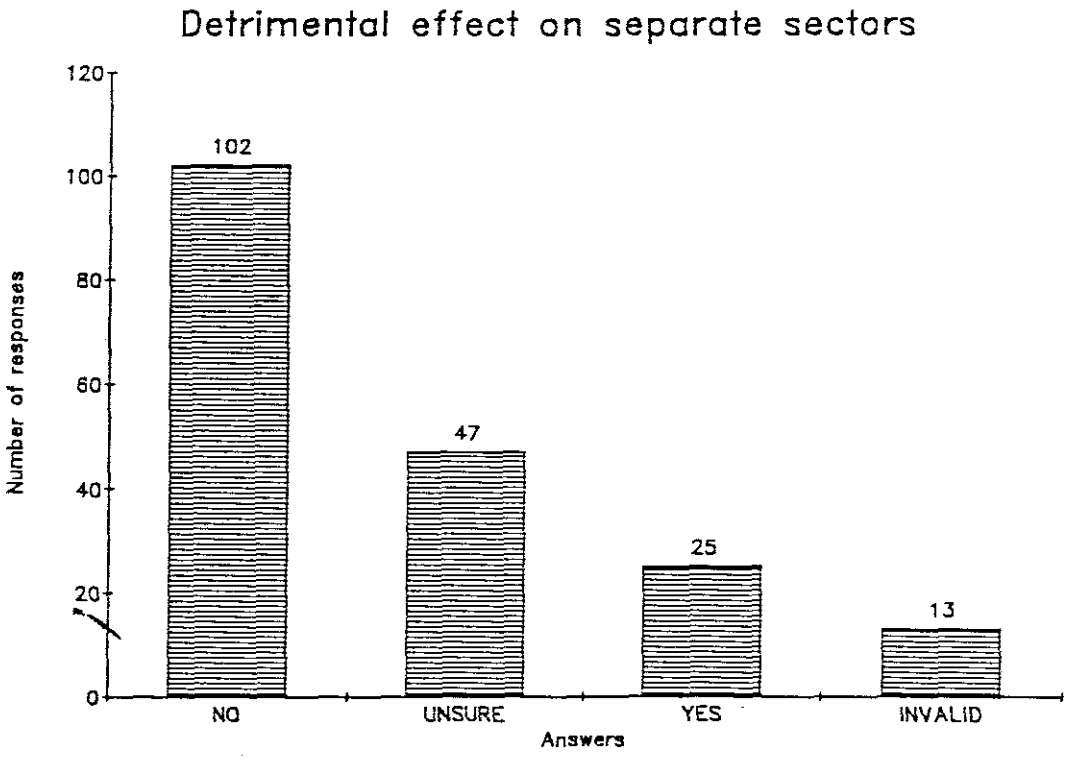

FIGURE 2-17 **EFFECT ON SEPARATE SECTORS**

2.3 SUMMARY OF THE EFFECTS OF VIRUSES

The survey focused on the effects of viruses as perceived by users rather than the detail of their operation.

The respondents claiming damage to data files, program files, system files and separate sectors were respectively 23,5%, 25,7%, 23,5% and 13,4% of the total submitted. The average of these four claims is 21,5%.

In order for a computer virus to affect data adversely on a computer user's magnetic disc, it has to affect at least one of the four areas mentioned above. Therefore an average of 21,5% of the respondents to this questionnaire claimed detrimental effects to one or more of these areas.

Of the participants of this field research 21,5% experienced detrimental effects with respect to their information stored on disk as a result of computer virus programs. However, no assumptions could be made about the possible result these effects could have had on the information stored on computer by a company.
In a large company, the loss of 21,5% of its computer-based information could have a serious effect on the running of the business.

It was thus considered necessary to determine in a controlled environment what damage virus programs do to information stored on magnetic disks.

CHAPTER THREE ** DATA COLLECTION AND ANALYSIS: EXPERIMENTS

3.1 INTRODUCTION

To determine accurately whether virus infections cause damage to stored information, various programs to be used in the laboratory experiments as well as the virus programs themselves had to be identified and obtained. Furthermore, the disks that would be infected and inspected had to be prepared.

3.2 INSPECTION PROGRAMS

Three programs were selected to be used as tools for this research: one to inspect disks at a bit level (a disk editor), one to manage disks generally (a disk utility program) and one to identify and remove viral infections (an anti-viral program).

Norton Utilities Version 6.0 and PCTools Version 6.0 were selected as disk editor and disk utility programs respectively. These two programs were ranked 3rd and 4th respectively in the "Top Ten Sellers" list (Anon (b), 1990:63).

They are generally accepted to be of the most complete utility programs available, it being recommended that "... one or more of these ... utilities should be the cornerstone of your DOS utilities software shelf." (Anon (b), 1990:182).

Dr. Solomon's Anti-Virus Toolkit Version 6.55 was used as an anti-viral program. During a review of anti-viral software, this package was highly recommended (Anon, 1991:10,11). This program is supported locally, a feature considered important should problems arise during the research. It is also updated on a monthly basis, indicating that its authors are involved in ongoing research. The regular updating allowed the investigator to choose the latest version available at the time of carrying out the research.

3.3 VIRUS PROGRAMS

The results of the questionnaire and other factors (as indicated below) were used to determine which virus programs should be included in the sample to be used during the laboratory test. Since the first computer virus appeared, the world has seen a rapid increase in the number of viruses detected. For example, Dr. Solomon's Anti-virus Toolkit Version 6.55 (released October 1993) caters for 3362 known viruses. Some of these viruses are listed below.

Aids, Aircop, Alabama, Anthrax, Ashar, Azusa, Bouncing Ball, Brain, Burger, Cascade, Casper, Cookie, Dark Avenger, Datacrime, dBase, Denzuck, Dir, Disk Killer, Durban, Fish, Flip, Friday 13th, Frodo, Fu Manchu, Icelandic, Jerusalem, Joker, Joshi, Kamikazi, Keypress, Lehigh, Liberty, Michelangelo, Mirror, Murphy, MusicBug, NoInt, Nomenklatura, Oropax, Perfume, Plastique, Pretoria, Proud, Saddam, Stoned, Sunday, Suriv, Taiwan, Tiny, Typo, USSR, Vacsina, Vienna, Whale, Yankee Doodle and *Zero Bug.*

The decision on which viruses were to be included in the sample, was based on the following considerations.

3.3.1 INITIAL ENQUIRIES

The telephonic enquiries received by the investigator involved the possible infection by one or more viruses.

Callers believed that an infection had occurred based on reports they received from known anti-viral software having been run on disks suspected of being infected. Thus the following viruses were included in the sample on the strength of these discussions: *Aircop, Frodo* and *Pretoria.*

3.3.2 REPORTED INFECTIONS

Since this research was aimed at the average computer user, it was considered necessary to include in the test sample those viruses which caused most of their infections.

The first 13 viruses listed in the summary of the answers to Question 9 caused respectively the highest number, second highest number up to the thirteenth highest number of infections (Figure 2-9). Taken together, they accounted for 91,3% (460 out of 504) of the total number of infections. The thirteenth one was labeled "unknown", and was not considered in the figures above. It was therefore decided to include the following 12 virus programs in the laboratory experiment sample :

> *Stoned, Bouncing Ball, Michelangelo, Jerusalem, Plastique, Sunday, NoInt, Brain, Cascade, Dark Avenger, Telefonica,* and *Durban.*

3.3.3 VIRUS CLINIC

The three virus programs which were identified by the Virus Clinic results (*Stoned, Bouncing Ball* and *Jerusalem*), appear amongst the four most common virus programs identified by the field survey. These two sets of results tend to indicate that these specific virus programs are more commonly found in industry than others.

The *Exebug* virus has been the cause of a number of virus infections at the School of Business Informatics at the Cape Technikon during 1993. It has also been included in the sample.

3.3.4 AVAILABILITY

Not all virus programs could be acquired for testing purposes by the investigator. Various attempts to obtain the *Dark Avenger* virus program from agents for anti-virus software, other researchers as well as from a virus research laboratory were unsuccessful. This was probably due to the security risk involved, or to the fact that the virus was not in their possession at the time. The *Dark Avenger* virus thus had to be excluded.

3.3.5 VIRUS TYPE

The general categories of computer viruses are: Boot Sector Viruses (BSV), Partition Record Viruses (PRV), Direct Action File Viruses (DAFV) and Indirect Action File Viruses (IAFV) (Solomon, 1989). It was considered important to include at least one virus of each of the four known types in the sample.

Solomon also classifies each virus according to the damage it supposedly inflicts. Trivial damage would take three minutes to rectify, Minor damage 30 minutes, and Moderate damage involves "disk trashing".

3.3.6 SUMMARY

The following table was constructed to summarize the sample of 15 viruses chosen for the laboratory experiments. Solomon's category definitions are used to classify the viruses. The degrees of damage claimed for each virus are indicated as follows:

Trivial: !
Minor: !!!
Moderate: !!!!!

VIRUS	BSV	PRV	DAFV	IAFV	DAMAGE
Aircop	X	X			!
Bouncing Ball	X	X			!
Brain	X	X			!
Cascade				X	!
Durban				X	!!!!!
Exebug	X	X			!!!!!
Frodo				X	!!!!!
Jerusalem				X	!!!
Michelangelo	X	X			!!!!!
NoInt	X	X			!
Plastique				X	!!!!!
Pretoria			X		!!!!!
Stoned	X	X			!!!!!
Sunday			X		!!!
Telefonica	X	X			!!!!!

TABLE 3-1 **VIRUS CLASSIFICATION**

Based on the motivations of point 3.3.1 to 3.3.5 above, it was considered to be a representative sample of the viruses which the average PC user had to deal with at the point of writing. Copies of these viruses were obtained from students, colleagues and various companies in commerce and industry. Each virus was positively identified using the Dr. Solomons Anti-Virus Toolkit program. This program will henceforth be referred to as the Toolkit.

According to Bock et al (1993:8), "Less than five years ago the term 'computer virus' was virtually unknown". As a result, up-to-date references on the detail of operation of computer virus programs were not freely available.

For the purposes of the laboratory experiments, the investigator had to find a reference which was recent enough to be of value. It was found that the manuals supplied with anti-virus programs could not be updated quickly enough to be usable. A number of books on viruses (Kane, 1989; Frost, 1989) were consulted, but in general the information on the operation of viruses discussed was not of enough substance to be used in this study. No other reference in book form could be found which covered the operation of all the viruses to be used in this study, in enough depth.

One reference was found which was updated on a monthly basis, and which contained a fairly detailed description on a large number of viruses: Hoffman's VSUM program. This regular updating was possible since the reference is in the form of a program and is thus not subject to publishing delays. A copy of the program was obtained via the CompuServe international network. The investigator used the latest version available (September 1993) at the time of carrying out the research.

The Hoffman program covers the history, symptoms of infection, detection and removal methods and the operation of viruses. This last feature was used as a guide-line during the experiments.

Each virus was activated and its symptoms and operation was compared to Hoffman's description at the start of each laboratory experiment. This was done to confirm that the virus program the investigator was using was a working copy. However, the damage done by viruses was not covered in detail by Hoffman. Therefore the investigator had to do detailed inspection of disk sectors, system areas and files to determine the degree of damage done by each virus program.

3.4 DISK PREPARATION

Three sets of disks were prepared for use in the laboratory experiments:

A set of Virus Master Disks, a set of User Master Disks, as well as a copy of the set of User Master Disks. All three disk types identified in Section 1.5 were included in the set of User Master Disks. Each one of the disks containing a boot sector virus program identified for the research was labeled as a Virus Master Disk, which was then write-protected to prevent accidental writing taking place to it. This master disk had in some cases been previously formatted under a different version of DOS. No attempt was made to install DOS 5.0 on these disks. Files infected by the file viruses to be used in the laboratory experiments were copied onto the remaining Virus Master Disks.

The Virus Master Disks were used to infect the User Master Disks described below. A set of User Master Disks was prepared, containing various system, program and data files.

The contents of each test disk are briefly described below (a list of files on each test disk is given in Appendix C):

Disk One: A 5,25-inch diskette, made bootable with MSDOS 5.0. It also contained various commonly used DOS program files. This diskette was included to simulate the environment of users who booted their computer from diskette.

Disk Two: A 5,25-inch diskette which contained only data files. Data files created by the following programs were included: DBase III+, Lotus 2.2, WordPerfect 5.1, RMCOBOL 85, Turbo Pascal 7 and TurboCash 2.0. This choice of data files was based on the answers to Question 4 of the questionnaire, and summarized in the previous chapter. According to this summary, more than 60% of the respondents indicated the use of Packages, Programming and Accounting applications. The programs mentioned above were considered to be common in practice, hence their inclusion. These six programs will henceforth be referred to as the Test Programs.

Disk Three: A 3,5-inch diskette containing all files necessary to load, run and use the RMCOBOL 85 compiler, as well as one Cobol source code file.

Disk Four: A 3,5-inch diskette containing all files necessary to load, run and use the DBase III+ database program, as well as one set of data files. This set included a database file (.DBF), a memo file (.DBT), a label file (.LBL) and a query file (.QRY).

Disk Five: A 3,5-inch diskette containing all files necessary to load, run and use the Lotus 2.2 spreadsheet program, as well as one data file.

Disk Six: A 3,5-inch diskette containing all files necessary to load, run and use the Turbo Pascal 7.0 compiler, as well as one Pascal source code file.

Disk Seven: A 3,5-inch diskette containing all files necessary to load, run and use the TurboCash 2.0 accounting package, as well as one set of files constituting the books of a company.

Disk Eight: A 3,5-inch diskette containing all files necessary to load, run and use the WordPerfect 5.1 word-processing program, as well as one document file.

Disk Nine: A 32-Mb hard disk drive, made bootable with MSDOS 5.0. It also contained the full MSDOS 5.0, as well as all the files contained on Disk Two to Disk Eight above.

3.5 LABORATORY PROCEDURES

3.5.1 PREPARATION OF TEST COMPUTER

- The test computer had the following specifications: 80286 processor, 360-kB 5,25-inch A drive, 1,44-Mb 3,5-inch B drive, 32-Mb C drive, Hercules monochrome monitor.

- Each one of the virus programs in the sample was tested to ensure that its operation was clear and that the symptoms of its presence and actual infection was in line with Hoffman's (1993) description. Exceptions are noted in the results.
- Copies of User Master Disk One to eight were made on another set of disks.
- Disk Nine (the hard drive) was backed up to a tape streamer.
- The test computer was not connected to a network, since the decision had been taken to consider virus effects in a standalone environment (Chapter One).
- The hard disk drive was physically write-protected (using mechanical switches in line with the read/write signals) to ensure that no virus could infect any part of it.
- These switches were set back to write enable only when the hard drive was intentionally infected.

3.5.2 INFECTION PROCEDURES

The set of copies of the User Master Disks and the hard drive were then exposed to the virus programs stored on the Virus Master Disks. Only one virus was used at a time, as described below.

- The test computer was booted, and a virus check was done to ensure that both memory and the hard disk were uninfected.
- Then the necessary program(s) were run to cause an infection by a virus program from the sample (in the case of a file virus).
- For a boot sector or partition record virus, the test computer was booted from the infected diskette.
- Each one of the copies of the User Master disks was then exposed to this infection in such a way that writing to the User Master disk copy could take place.
- This was done to allow the virus to infect each test disk.
- However, since the test disks contained different types of files, each one had to be exposed to the infection in a different way, as described below.

Disk One: The following programs were run from Disk One: COMMAND, CHKDSK, TREE, DISKCOPY and FORMAT.

Disk Two: Each one of the Test Programs was run in turn (from the hard disk), and its associated data file was loaded from Disk Two. One change was made to each data file, and the file was saved back to Disk Two. A normal exit from each test program was done.

Disk Three: The RMCOBOL file on Disk Three was used to compile the source code file, followed by the RUNCOBOL file which executed the file created by RMCOBOL.

Disk Four: The DBase program was run from Disk Four, and the data file (.DBF) loaded. One change to the file was made, and it was stored back to Disk Four. A label file was recalled and viewed on the screen, followed by a normal exit to DOS.

Disk Five: The Lotus program was run from Disk Five, and a spreadsheet file loaded. One change to the file was made, and it was stored back to Disk Five, followed by a normal exit to DOS.

Disk Six: The Pascal compiler was loaded, and a source code file loaded from Disk Six. One change was made to the source code, and it was saved back to Disk Six. The compiler was then used to compile and run the file, followed by a normal exit to DOS.

Disk Seven: The TurboCash program was run, and a set of books loaded. One change to the accounts was made, and it was stored back to Disk Seven, followed by a normal exit to DOS.

Disk Eight: The WordPerfect program was run, and a document file loaded. One change to the file was made, and it was stored back to Disk Eight, followed by a normal exit to DOS.

Disk Nine: The write protect switches were set to Write Enable, to allow virus infections on the hard drive to take place. Each one of the six Test Programs were then executed from the hard drive in turn. For each one, a data file was loaded from the hard disk, a change was made to it, it was saved back to the hard disk, followed by a normal exit to DOS.

3.5.3 INSPECTION PROCEDURES

Each one of the User Test Disk copies was then inspected for infection as determined by the hypotheses, and the results were noted.

- The Toolkit was used to check for infection of RAM and the disk(ette).
- Data files were checked by attempting to load them via a program file. Their contents were also checked by viewing the file.
- Program files were executed, and their sizes checked for any changes (an increase in size could imply a file virus infection). The root directory was checked with Norton Utilities.
- System files were checked by attempting to boot from the infected disk, and their respective sizes were compared with the uninfected files' size.
- Infected files were then disinfected using the Toolkit. This program sometimes renames e.g. disinfected EXE files to VXE.

- The disinfected program files were renamed and run. This was done to establish whether or not the file could be executed after disaffection.
- Finally, the utility programs were used to look for any bad sectors.

3.5.4 PREPARATION FOR NEXT INFECTION

- The test computer was switched off and on again, and rebooted from an uninfected diskette. This was done to ensure an uninfected memory.
- The hard drive write-protect switch was still set to write-enable. The hard drive was then formatted and all information restored from the backup cassette.
- The User Master Disks one to eight were then copied over the set of copies, thereby overwriting any virus code and all changes of any nature caused by the infection.
- In this way the investigator ensured that each experiment was carried out using an uninfected set of disks.
- Afterwards the test computer was switched off and on, and rebooted from the hard drive. A virus scan of the hard disk was done to ensure an uninfected hard disk and memory.

The processes described in Section 3.5.1 to 3.5.4 above were then repeated for each one of the 14 remaining viruses in the sample.

3.6 TEST DATA ANALYSIS

The tables below depict the results of the laboratory experiments. Tables 3-2 and 3-3 are to be used as reference and compared to the actual results following in Table 3-4 onwards.

Since entries in the tables are in the form of questions (e.g. Data files: Access?), the results were given in the form of answers (e.g. Yes or No). The reader must keep in mind that a "Yes" answer does not necessarily have a positive connotation and a "No" answer not necessarily a negative one. For example, a Yes answer to the question "Data files: Contents changed?" has a negative connotation.

A screendump has been included after each table. In the case of a BSV/PRV, it is the boot sector of the Virus Master Disk used for that specific virus infection. In the case of a file virus, it is a directory listing of the infected User Master Disk One.

RAM infection?

This shows whether or not the Toolkit indicated infection of RAM after allowing the virus to infect RAM (Hypothesis H_{1a}).

DISK NO: 1 2 3 4 5 6 7 8 9

Disk infection?

This row lists whether or not the Toolkit did indicate an infection on each one of the nine User Master Disks respectively. Thus hypothesis H_{1b}, H_{1c} and H_{1d} are tested.

Data files:

The next three rows test H_{2a}: the effect on data files.

Access? *Can the file be loaded by its originating program?*
C. ch.? *Has there been any change to the data file contents?*
R. dir.? *Has there been any change to file size in the root directory?*

Program files:

The next four rows test H_{2b}: the effect on program files.

Ex. succ1.? *Does the file run after having been infected?*
L. alt.? *Has its length been altered?*
R. dir? *Has there been any change to the root directory?*
Ex. succ2.? *Does the file run after having been disinfected?*

System files:

The next two rows test H_{2c}: the effect on system files.

Boot? *Can booting be done from the infected file(s)?*
L. alt.? *Has its length been altered?*

Individual sectors:

The next row tests H_{2d}: the effect on separate sectors.
M. bad? *Has any one sector been marked bad?*

Notes:
Y: *Yes*
N: *No*
X: *Not Applicable (e.g. System file infection on a disk with only data files.)*
*: *Any symbol contained in a table result column, excluding a Y, N or an X, refers to a Note at the end of that table.*

TABLE 3-2 **EXAMPLE RESULT LISTING**

```
0000: EB 3C 90 4D 53 44 4F 53 - 35 2E 30 00 02 02 01 00
      .<.MSDOS5.0.....
0010: 02 70 00 D0 02 FD 02 00 - 09 00 02 00 00 00 00 00
      .p..............
0020: 00 00 00 00 00 00 29 EE - 18 49 13 4E 4F 20 4E 41
      ......)..I.NO NA
0030: 4D 45 20 20 20 20 46 41 - 54 31 32 20 20 20 FA 33
      ME    FAT12    .3
0040: C0 8E D0 BC 00 7C 16 07 - BB 78 00 36 C5 37 1E 56
      .....|...x.6.7.V
0050: 16 53 BF 3E 7C B9 0B 00 - FC F3 A4 06 1F C6 45 FE
      .S.>|........E.
0060: 0F 8B 0E 18 7C 88 4D F9 - 89 47 02 C7 07 3E 7C FB
      ....|.M..G...>|.
0070: CD 13 72 79 33 C0 39 06 - 13 7C 74 08 8B 0E 13 7C
      ..ry3.9..|t....|
0080: 89 0E 20 7C A0 10 7C F7 - 26 16 7C 03 06 1C 7C 13
      .. |..|.&.|...|.
0090: 16 1E 7C 03 06 0E 7C 83 - D2 00 A3 50 7C 89 16 52
      ..|...|....P|..R
00A0: 7C A3 49 7C 89 16 4B 7C - B8 20 00 F7 26 11 7C 8B
      |.I|..K|. ..&.|.
00B0: 1E 0B 7C 03 C3 48 F7 F3 - 01 06 49 7C 83 16 4B 7C
      ..|..H....I|..K|
00C0: 00 BB 00 05 8B 16 52 7C - A1 50 7C E8 92 00 72 1D
      ......R|.P|...r.
00D0: B0 01 E8 AC 00 72 16 8B - FB B9 0B 00 BE E6 7D F3
      .....r........}.
00E0: A6 75 0A 8D 7F 20 B9 0B - 00 F3 A6 74 18 BE 9E 7D
      .u..▒ .....t...}
00F0: E8 5F 00 33 C0 CD 16 5E - 1F 8F 04 8F 44 02 CD 19
      ._.3...^....D...
0100: 58 58 58 EB E8 8B 47 1A - 48 48 8A 1E 0D 7C 32 FF
      XXX...G.HH...|2.
0110: F7 E3 03 06 49 7C 13 16 - 4B 7C BB 00 07 B9 03 00
      ....I|..K|......
0120: 50 52 51 E8 3A 00 72 D8 - B0 01 E8 54 00 59 5A 58
      PRQ.:.r....T.YZX
0130: 72 BB 05 01 00 83 D2 00 - 03 1E 0B 7C E2 E2 8A 2E
      r..........|....
0140: 15 7C 8A 16 24 7C 8B 1E - 49 7C A1 4B 7C EA 00 00
      .|..$|..I|.K|...
0150: 70 00 AC 0A C0 74 29 B4 - 0E BB 07 00 CD 10 EB F2
      p....t).........
0160: 3B 16 18 7C 73 19 F7 36 - 18 7C FE C2 88 16 4F 7C
      ;..|s..6.|....O|
0170: 33 D2 F7 36 1A 7C 88 16 - 25 7C A3 4D 7C F8 C3 F9
      3..6.|..%|.M|...
0180: C3 B4 02 8B 16 4D 7C B1 - 06 D2 E6 0A 36 4F 7C 8B
      .....M|.....6O|.
```

TABLE 3-3 **UNINFECTED BOOT SECTOR**

```
0190: CA 86 E9 8A 16 24 7C 8A - 36 25 7C CD 13 C3 0D 0A
      .....$|.6%|.....
01A0: 4E 6F 6E 2D 53 79 73 74 - 65 6D 20 64 69 73 6B 20
      Non-System disk
01B0: 6F 72 20 64 69 73 6B 20 - 65 72 72 6F 72 0D 0A 52
      or disk error..R
01C0: 65 70 6C 61 63 65 20 61 - 6E 64 20 70 72 65 73 73
      eplace and press
01D0: 20 61 6E 79 20 6B 65 79 - 20 77 68 65 6E 20 72 65
      any key when re
01E0: 61 64 79 0D 0A 00 49 4F - 20 20 20 20 20 20 53 59
      ady...IO      SY
01F0: 53 4D 53 44 4F 53 20 20 - 20 53 59 53 00 00 55 AA
      SMSDOS   SYS..U.
```

TABLE 3-3 (continued) **UNINFECTED BOOT SECTOR**

TABLE 3-3 shows an uninfected boot sector of a 5,25-inch 360-kb diskette. The first number in the first, third and every alternate row thereafter refers to the offset address of the memory locations viewed. The 16 two-digit codes following the address are the contents of 16 successive memory locations. The addresses and data are listed in hexadecimal format. The row of 16 characters in row two, four and every alternate row thereafter represent the ASCII characters of the 16 memory locations. Since some memory locations contain spaces or non-printable characters, some of the characters in this row may not be visible.

It is necessary to identify some sections of an uninfected boot sector, in order to compare it to possibly infected boot sectors (Dettmann, 1988:220-223). Whenever a BSV or PRV is to be used in the laboratory experiment, reference will be made to these five areas of the boot sector.

JUMP STATEMENT. The first three bytes (EB 3C 90) contain a jump statement to the boot code further on in the boot sector. In this case only the first two bytes are needed to execute the jump, so the third byte (90 hexadecimal translates to a No operation or NOP instruction) is used to pad this unused memory location.

OPERATING SYSTEM NAME. The next eight bytes (4D 53 44 4F 53 35 2E 30) are reserved for the name and version number of the operating system which was in memory when this disk was formatted.

FAT TYPE. The text string "FAT12" is visible in row 0030. This refers to the fact that this diskette type uses 12 bits per FAT entry.

BOOT CODE. The biggest part of the boot sector (approximately row 0040 to 0190) is occupied by the boot program code. This appears as garbage when viewed as ASCII.

BOOT MESSAGES. Row 01A0 to 01E0 contain messages that the user might see when attempting to boot from a non-system disk. These messages are displayed as normal text strings.

3.6.1 *AIRCOP* VIRUS

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	Y	Y	Y	Y	Y	Y	Y	N
Data files:									
Access?	X	Y	Y	Y	Y	Y	*	#	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	*	#	Y
Length altered?	N	X	N	N	N	N	N	N	N
Root dir. changed?	N	X	N	N	N	N	N	N	N
Execute success 2?	Y	X	Y	Y	Y	Y	N	N	Y
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-4 ***AIRCOP* RESULT LISTING**

Notes:

*: The TurboCash program loaded partially, then froze. This was confirmed during another two unsuccessful attempts. The test computer had to be re-booted after every attempt.

#: The WordPerfect program loaded, but froze and strange characters appeared on the screen when a document was loaded. This was confirmed during another two unsuccessful attempts. The test computer had to be re-booted after every attempt.

```
0000: EB 34 90 49 42 4D 20 20 - 33 2E 33 00 02 02 01 00
      .4.IBM  3.3.....
0010: 02 70 00 D0 02 FD 02 00 - 09 00 02 00 00 00 00 00
      .p..............
0020: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 12
      ................
0030: 00 00 00 00 01 00 FA 33 - C0 8E D8 A2 C4 7D B8 E4
      .......3.....}..
0040: 00 A3 B8 7D B8 31 01 A3 - BC 7D FF 0E 13 04 CD 12
      ...}.1...}......
0050: B1 06 D3 E0 8E C0 A3 BA - 7D A3 BE 7D FA 87 06 66
      ........}..}...f
0060: 00 A3 C2 7D B8 C8 00 87 - 06 64 00 A3 C0 7D FB 33
      ...}.....d...}.3
0070: FF BB 00 7C 8B F3 B9 00 - 01 1E 53 FC F3 A5 06 B8
      ...|......S.....
0080: 84 00 50 CB 1E 07 B8 01 - 02 B9 09 27 BA 00 01 CD
      ..P........'....
0090: 13 73 07 5B 07 0E B8 BC - 00 50 BB 48 00 FA 1E 56
      .s.[.....P.H...V
00A0: 50 51 33 C9 8E D9 BE 70 - 01 B1 02 8B 07 2E 87 00
      PQ3....p........
00B0: 89 07 43 43 E2 F5 59 58 - 5E 1F FB CB 0E 1F BE EE
      ..CC..YX^.......
00C0: 01 E8 30 00 32 E4 CD 16 - CD 12 33 C0 CD 13 0E 07
      ..0.2.....3.....
00D0: BB 00 02 B9 06 00 33 D2 - B8 01 02 CD 13 72 DD 2E
      ......3......r..
00E0: FF 2E C0 01 53 0E E8 B1 - FF 0E BB 4C 00 E8 AD FF
      ....S......L....
00F0: 5B CD 12 CF BB 07 00 FC - AC 0A C0 74 2C 79 07 34
      [..........t,y.4
0100: D7 80 CB 88 CD 09 3C 20 - 76 09 B5 40 E2 FE 41 B4
      ......< v..@..A.
0110: 09 CD 10 B4 0E CD 10 EB - DB BB 00 02 B9 01 00 B6
      ................
0120: 00 B0 01 9C 2E FF 1E BC - 01 C3 B9 09 27 B6 01 EB
      ............'...
0130: F0 50 53 51 52 06 1E 56 - 57 9C 80 FA 01 77 58 0A
      .PSQR..VW....wX.
0140: E4 74 54 8A C5 D0 E0 02 - C6 B4 09 F6 E4 32 ED 03
      .tT..........2..
0150: C1 3D 0C 00 77 41 3C 06 - 72 3D 0E 07 B4 02 E8 B8
      .=..wA<.r=......
0160: FF 72 2F 06 1F BE 36 00 - BF 36 02 B9 AE 00 56 57
      .r/...6..6....VW
0170: FC F3 A6 5E 5F 74 20 4E - 4F B9 33 00 FD F3 A4 33
      ...^_t NO.3....3
0180: DB B4 03 E8 96 FF 72 0A - BB 00 02 B4 03 E8 9A FF
      ......r.........
```

TABLE 3-5 *AIRCOP*-INFECTED BOOT SECTOR

```
0190: 73 13 33 C0 E8 8C FF 9D - 5F 5E 1F 07 5A 59 5B 58
      s.3....._^.ZY[X
01A0: 2E FF 2E BC 01 A0 C4 01 - 40 A2 C4 01 24 07 75 E7
      ........@...$.u.
01B0: BE C5 01 E8 3E FF EB DF - E4 00 C0 9F 82 11 70 00
      ....>.........p.
01C0: 6D 02 00 C8 00 DA DD 2E - 85 92 93 F7 84 83 96 83
      m...............
01D0: 92 2C 20 90 B2 A5 BA F7 - B8 B1 B1 B2 B9 A4 BE B9
     .,..............
01E0: B0 20 20 FA FA 96 BE A5 - B4 B8 A7 DA DD 00 0D 0A
      ..............
01F0: 4E 6F 6E 2D 73 79 73 74 - 65 6D 00 00 00 00 55 AA
      Non-system....U.
```

TABLE 3-5 (continued) ***AIRCOP*-INFECTED BOOT SECTOR**

ANALYSIS

RAM and all diskettes were infected, but the hard drive escaped infection. It was found that *Aircop* did not consider the disk type (with the exception of the hard disk) or the information on a disk before infecting it. No data or program files were specifically infected or altered in any way during the boot sector rewriting action.

During infection, the actual boot sector was written into the very last sector on a 360-kb 5,25-inch diskette. This is the last sector on the last track on the second side.

On a 1,44-Mb 3,5-inch diskette, a sector with the same location relative to the beginning of the disk was used. However, since this diskette format has double the number of tracks and sectors as compared to the first, the relevant sector was in the centre of the disk.

The actual contents of a file of any type would be deleted (partially or in full) only if one of its sectors occupied side one, track 39, sector nine on any one of the two diskette types. No file of any type was affected as a logical unit. One disk sector which had no relation to any specific file was destroyed by *Aircop*. Inspection of test Disks Seven and Eight confirmed the finding which related to the location to which the boot sector is transported.

On test Disk Seven (TurboCash), a file called DLEDGER.SCR was partially overwritten by the boot sector. This file occupied several sectors, one of which was the centre sector (numerically) on the disk. This file involves screen access, which explains the display problems encountered.

Test Disk Eight (WordPerfect) contains a file WP.FIL, which is also written on the area which includes the centre sector. The unexpected symptoms can be attributed to the corruption of this file. Neither of these two test programs ran after disinfection.

When the infected boot sector is compared to the uninfected sector, some differences are evident. The JUMP statement and Operating System name areas are intact, except for the version number change (the Virus Master Disk was formatted under a different version of DOS). The FAT type, boot code and most of the messages had been replaced by what appears to be foreign program code.

Only a part of one message (which has been moved) is visible. Thus the location of the virus code as being in side zero, track zero, sector one has been confirmed.

3.6.2 *BOUNCING BALL* VIRUS
* #

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	Y	N	N	N	N	N	N	Y
Data files:									
Access?	X	Y	X	X	X	X	X	X	Y
Contents changed?	X	N	X	X	X	X	X	X	N
Root dir. changed?	X	N	X	X	X	X	X	X	N
Program files:									
Execute success 1?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Root dir. changed?	N	X	X	X	X	X	X	X	N
Execute success 2?	Y	X	X	X	X	X	X	X	Y
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	Y	Y	N	N	N	N	N	N	Y

TABLE 3-6 ***BOUNCING BALL* RESULT LISTING**

Notes:

*: Neither the test computer nor an 80386-based computer booted from the Virus Master Disk which was infected by the *Bouncing Ball* virus.

Because the *Bouncing Ball* was identified as being one of the most common viruses by the results obtained from both the Virus Clinic and the field research, it was considered important to attempt infection on a different computer. A test computer with an 8088 Intel processor was used, on which infection did take place. The results given above are for tests done on this computer.

#: It was found that the test computer would not boot if the date of its ROM BIOS was earlier than January 1988.

```
0000: EB 1C 90 4D 53 44 4F 53 - 33 2E 32 00 02 02 01 00
      ...MSDOS3.2.....
0010: 02 70 00 D0 02 FD 02 00 - 09 00 02 00 00 00 33 C0
      .p............3.
0020: 8E D0 BC 00 7C 8E D8 A1 - 13 04 2D 02 00 A3 13 04
      ....|.....-.....
0030: B1 06 D3 E0 2D C0 07 8E - C0 BE 00 7C 8B FE B9 00
      ....-.......|....
0040: 01 F3 A5 8E C8 0E 1F E8 - 00 00 32 E4 CD 13 80 26
      ..........2....&
0050: F8 7D 80 8B 1E F9 7D 0E - 58 2D 20 00 8E C0 E8 3C
      .}....}.X- ....<
0060: 00 8B 1E F9 7D 43 B8 C0 - FF 8E C0 E8 2F 00 33 C0
      ....}C....../.3.
0070: A2 F7 7D 8E D8 A1 4C 00 - 8B 1E 4E 00 C7 06 4C 00
      ..}...L...N...L.
0080: D0 7C 8C 0E 4E 00 0E 1F - A3 2A 7D 89 1E 2C 7D 8A
      .|..N...*}..,}.
0090: 16 F8 7D EA 00 7C 00 00 - B8 01 03 EB 03 B8 01 02
      ..}..|..........
00A0: 93 03 06 1C 7C 33 D2 F7 - 36 18 7C FE C2 8A EA 33
      ....|3..6.|....3
00B0: D2 F7 36 1A 7C B1 06 D2 - E4 0A E5 8B C8 86 E9 8A
      ..6.|...........
00C0: F2 8B C3 8A 16 F8 7D BB - 00 80 CD 13 73 01 58 C3
      ......}.....s.X.
00D0: 1E 06 50 53 51 52 0E 1F - 0E 07 F6 06 F7 7D 01 75
      ..PSQR......}.u
00E0: 42 80 FC 02 75 3D 38 16 - F8 7D 88 16 F8 7D 75 22
      B...u=8..}...}u"
00F0: 32 E4 CD 1A F6 C6 7F 75 - 0A F6 C2 F0 75 05 52 E8
      2.....▒u....u.R.
```

TABLE 3-7 ***BOUNCING BALL*-INFECTED BOOT SECTOR**

```
0100: B1 01 5A 8B CA 2B 16 B0 - 7E 89 0E B0 7E 83 EA 24
      ..Z..+..~...~..$
0110: 72 11 80 0E F7 7D 01 56 - 57 E8 12 00 5F 5E 80 26
      r....}.VW..._^.&
0120: F7 7D FE 5A 59 5B 58 07 - 1F EA 56 02 00 C8 B8 01
      .}.ZY[X..V.....
0130: 02 B6 00 B9 01 00 E8 8A - FF F6 06 F8 7D 80 74 23
      ............}.t#
0140: BE BE 81 B9 04 00 80 7C - 04 01 74 0C 80 7C 04 04
      .......|..t..|..
0150: 74 06 83 C6 10 E2 EF C3 - 8B 14 8B 4C 02 B8 01 02
      t..........L....
0160: E8 60 FF BE 02 80 BF 02 - 7C B9 1C 00 F3 A4 81 3E
      .`......|......>
0170: FC 81 57 13 75 15 80 3E - FB 81 00 73 0D A1 F5 81
      ..W.u..>...s....
0180: A3 F5 7D 8B 36 F9 81 E9 - 08 01 C3 81 3E 0B 80 00
      ..}.6.......>...
0190: 02 75 F7 80 3E 0D 80 02 - 72 F0 8B 0E 0E 80 A0 10
      .u..>...r.......
01A0: 80 98 F7 26 16 80 03 C8 - B8 20 00 F7 26 11 80 05
      ...&..... ..&...
01B0: FF 01 BB 00 02 F7 F3 03 - C8 89 0E F5 7D A1 13 7C
      ............}..|
01C0: 2B 06 F5 7D 8A 1E 0D 7C - 33 D2 32 FF F7 F3 40 8B
      +..}...|3.2...@.
01D0: F8 80 26 F7 7D FB 3D F0 - 0F 76 05 80 0E F7 7D 04
      ..&.}.=..v....}.
01E0: BE 01 00 8B 1E 0E 7C 4B - 89 1E F3 7D C6 06 B2 7E
      ......|K...}...~
01F0: FE EB 0D 01 00 0C 00 03 - 00 0C 00 00 57 13 55 AA
      ............W.U.
```

TABLE 3-7 (continued) ***BOUNCING BALL*-INFECTED BOOT SECTOR ANALYSIS**

RAM, 5,25-inch diskettes and the hard drive were infected. The 3,5-inch diskettes were not affected in any way. During infection, the installation part of the virus code was copied into the location of the boot code.

Inspection revealed that the actual boot sector together with the second half of the virus code was copied into the first available two empty sectors.

The cluster containing these sectors was then marked as bad, but only in the first FAT. The second FAT was not updated. Diskettes without free space were not infected. No data, executable or system files were affected as a logical unit. Two disk sectors which had no relation to any specific file were occupied by the *Bouncing Ball* program code.

Highland's claims (1989:93) of the ability of this virus to remove characters from both the screen and disk files, could not be confirmed. However, the ability of this virus to successfully impair the booting of an 80286 or 80386 CPU computer system was confirmed. No hard drive infection took place in these two instances.

When the infected boot sector is compared to the uninfected sector, some differences are evident. The JUMP statement and Operating System name areas are intact, except for the version number change (the Virus Master Disk was formatted under a different version of DOS).

The FAT type, boot code and the messages have been replaced by what appears to be foreign program code. Thus the location of the virus code as being on side zero, track zero, sector one has been confirmed. When comparing these results of the *Bouncing Ball* virus with Hoffman, (1993), no differences could be found. The following facts were in agreement:

- 5,25-inch Diskettes were infected.
- The hard disk drive was infected.
- The new location of the boot sector was confirmed.
- The appearance of the bouncing ball symptom under certain conditions was confirmed.

3.6.3 *BRAIN* VIRUS

RAM infection?	X								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	X	X	X	X	X	X	X	X	X
Data files:									
Access?	X	X	X	X	X	X	X	X	X
Contents changed?	X	X	X	X	X	X	X	X	X
Root dir. changed?	X	X	X	X	X	X	X	X	X
Program files:									
Execute success.?	X	X	X	X	X	X	X	X	X
Length altered?	X	X	X	X	X	X	X	X	X
Root dir. changed?	X	X	X	X	X	X	X	X	X
System files:									
Boot?	X	X	X	X	X	X	X	X	X
Length altered?	X	X	X	X	X	X	X	X	X
Individual sectors:									
Marked bad?	X	X	X	X	X	X	X	X	X

TABLE 3-8 ***BRAIN* RESULT LISTING**

```
0000: FA E9 4A 01 34 12 00 09 - 18 00 01 00 00 00 00 00
      ..J.4...........
0010: 57 65 6C 63 6F 6D 65 20 - 74 6F 20 74 68 65 20 20
      Welcome to the
0020: 44 75 6E 67 65 6F 6E 20 - 20 20 20 20 20 20 20 20
      Dungeon
0030: 28 63 29 20 31 39 38 36 - 20 42 72 61 69 6E 17 26
      (c) 1986 Brain.&
0040: 20 41 6D 6A 61 64 73 20 - 28 70 76 74 29 20 4C 74
      Amjads (pvt) Lt
0050: 64 20 20 20 56 49 52 55 - 53 5F 53 48 4F 45 20 20
      d  VIRUS_SHOE
0060: 52 45 43 4F 52 44 20 20 - 20 76 39 2E 30 20 20 20
      RECORD   v9.0
0070: 44 65 64 69 63 61 74 65 - 64 20 74 6F 20 74 68 65
      Dedicated to the
0080: 20 64 79 6E 61 6D 69 63 - 20 6D 65 6D 6F 72 69 65
      dynamic memorie
0090: 73 20 6F 66 20 6D 69 6C - 6C 69 6F 6E 73 20 6F 66
      s of millions of
00A0: 20 76 69 72 75 73 20 77 - 68 6F 20 61 72 65 20 6E
      virus who are n
00B0: 6F 20 6C 6F 6E 67 65 72 - 20 77 69 74 68 20 75 73
      o longer with us
00C0: 20 74 6F 64 61 79 20 2D - 20 54 68 61 6E 6B 73 20
      today - Thanks
00D0: 47 4F 4F 44 4E 45 53 53 - 21 21 20 20 20 20 20 20
      GOODNESS!!
00E0: 20 42 45 57 41 52 45 20 - 4F 46 20 54 48 45 20 65
      BEWARE OF THE e
00F0: 72 2E 2E 56 49 52 55 53 - 20 20 3A 20 5C 74 68 69
      r..VIRUS  : \thi
0100: 73 20 70 72 6F 67 72 61 - 6D 20 69 73 20 63 61 74
      s program is cat
0110: 63 68 69 6E 67 20 20 20 - 20 20 20 70 72 6F 67 72
      ching      progr
0120: 61 6D 20 66 6F 6C 6C 6F - 77 73 20 61 66 74 65 72
      am follows after
0130: 20 74 68 65 73 65 20 6D - 65 73 73 65 67 65 73 2E
      these messeges.
0140: 2E 2E 2E 2E 20 24 23 40 - 25 24 40 21 21 20 8C C8
      .... $#@%$@!! ..
0150: 8E D8 8E D0 BC 00 F0 FB - A0 06 7C A2 09 7C 8B 0E
      ..........|..|..
0160: 07 7C 89 0E 0A 7C E8 57 - 00 B9 05 00 BB 00 7E E8
      .|...|.W......~.
0170: 2A 00 E8 4B 00 81 C3 00 - 02 E2 F4 A1 13 04 2D 07
      *..K..........-.
0180: 00 A3 13 04 B1 06 D3 E0 - 8E C0 BE 00 7C BF 00 00
      ............|...
```

TABLE 3-9 ***BRAIN*-INFECTED BOOT SECTOR**

```
0190: B9 04 10 FC F3 A4 06 B8 - 00 02 50 CB 51 53 B9 04
      ..........P.QS..
01A0: 00 51 8A 36 09 7C B2 00 - 8B 0E 0A 7C B8 01 02 CD
      .Q.6.|.....|....
01B0: 13 73 09 B4 00 CD 13 59 - E2 E7 CD 18 59 5B 59 C3
      .s.....Y....Y[Y.
01C0: A0 0A 7C FE C0 A2 0A 7C - 3C 0A 75 1A C6 06 0A 7C
      ..|....|<.u....|
01D0: 01 A0 09 7C FE C0 A2 09 - 7C 3C 02 75 09 C6 06 09
      ...|....|<.u....
01E0: 7C 00 FE 06 0B 7C C3 00 - 00 00 00 32 E3 23 4D 59
      |....|.....2.#MY
01F0: F4 A1 82 BC C3 12 00 7E - 12 CD 21 A2 3C 5F 0C 05
      .......~..!.<_..
```

TABLE 3-9 (continued) ***BRAIN*-INFECTED BOOT SECTOR**

ANALYSIS

During the laboratory experiments with the *Brain* virus, RAM was never successfully infected. In all tests, the booting process was halted before the DOS prompt was reached. Hence no disks could be infected to determine the effect of infection by this virus.

Since this virus was identified by the questionnaire results as having caused some infections in industry, further experiments were considered necessary. The same virus program was used to boot test computers using both an Intel 8088 and an Intel 80386 processor, with the same result. It was thus assumed that the copy of the virus program used was an inactive strain or mutation of an original copy of this virus. No results could be obtained from an infection caused by this virus.

However, comparison of the infected boot sector of the Virus Master Disk with the uninfected boot sector did show that the infected boot sector was abnormal.

None of the five areas identified earlier was present. Instead, a cryptic message filled about one half of this sector. The message read:

> "Welcome to the Dungeon (c) 1986 Brain.& Amjads (pvt) Ltd VIRUS_SHOE RECORD v9.0
> Dedicated to the dynamic memories of millions of virus (sic!) who are no longer with us today - Thanks (sic!) GOODNESS!! BEWARE OF THE er..VIRUS : \this program is catching program (sic!) follows after these messeges (sic!)."

3.6.4 *CASCADE* VIRUS

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	N	N	N	N	N	N	N	Y
Data files:									
Access?	X	Y	Y	Y	Y	Y	Y	Y	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	Y	Y	Y
Length altered?	Y	X	X	X	X	X	X	X	Y
Root dir. changed?	N	N	N	N	N	N	N	N	N
Execute success 2?	Y	X	Y	Y	Y	Y	Y	Y	Y
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	Y	X	X	X	X	X	X	X	Y
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-10 ***CASCADE*** **RESULT LISTING**

```
 Volume in drive A has no label
 Volume Serial Number is 15E1-2B3D
 Directory of A:\

CHKDSK   EXE      16200 04-09-91   5:00a
COMMAND  COM      49546 04-09-91   5:00a
DISKCOPY COM      13494 04-09-91   5:00a
FORMAT   COM      34612 04-09-91   5:00a
TREE     COM       8602 04-09-91   5:00a
        5 file(s)     122454 bytes
                      165888 bytes free
```

TABLE 3-11 **DIRECTORY LISTING:** ***CASCADE***

ANALYSIS

RAM and all disks except the 3,5-inch type were infected in all cases. *Cascade* infected only executable files with a COM extension. No data files were affected in any way. The COMMAND.COM system file was infected in all cases where the User Test Disk was bootable.

Infected files all increased in size by 1701 bytes (compare TABLE 3-11 to Appendix C). No change was made to the date and time stamps of the infected files. All infected files ran successfully after disinfection with the Toolkit. No sectors were affected separately in any way.

3.6.5 *DURBAN* VIRUS

RAM infection?	X								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	X	X	X	X	X	X	X	X	X
Data files:									
Access?	X	X	X	X	X	X	X	X	X
Contents changed?	X	X	X	X	X	X	X	X	X
Root dir. changed?	X	X	X	X	X	X	X	X	X
Program files:									
Execute success.?	X	X	X	X	X	X	X	X	X
Length altered?	X	X	X	X	X	X	X	X	X
Root dir. changed?	X	X	X	X	X	X	X	X	X
System files:									
Boot?	X	X	X	X	X	X	X	X	X
Length altered?	X	X	X	X	X	X	X	X	X
Individual sectors:									
Marked bad?	X	X	X	X	X	X	X	X	X

TABLE 3-12 ***DURBAN* RESULT LISTING**

ANALYSIS

This test was carried out after setting the system date to the claimed trigger date for this virus (any Saturday the 14th). The trigger date is the date on which the destructive action of the virus should take place (Hoffman, 1993; Anon, 1991:19). The test (infected) file was then run. The first program that was run immediately afterwards, caused the test computer to freeze.

All the executable files on all the User Test Disks were used in an attempt to load and terminate a program successfully, but all failed. It was thus impossible to determine whether the virus was in RAM at any instant after attempting to infect memory (as explained above, not even the anti-virus executable programs could be loaded). No results could be obtained from an infection caused by this virus. It is assumed that the copy of the virus program used by the investigator was corrupt.

3.6.6 *EXEBUG* VIRUS

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	*	Y	Y	Y	Y	Y	Y	#
Data files:									
Access?	X	*	Y	Y	Y	Y	Y	Y	*
Contents changed?	X	*	N	N	N	N	N	N	*
Root dir. changed?	X	*	N	N	N	N	N	N	*
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	Y	Y	*
Length altered?	N	X	N	N	N	N	N	N	*
Root dir. changed?	N	X	N	N	N	N	N	N	*
Execute success 2?	Y	X	Y	Y	Y	Y	Y	Y	*
System files:									
Boot?	Y	X	X	X	X	X	X	X	N
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-13 ***EXEBUG* RESULT LISTING**

Notes:

*: The hard disk drive was inaccessible after RAM was infected. No programs could therefore be run from the hard disk drive, not even to load the data files of test Disk Two.

#: Since the hard disk drive was inaccessible by standard DOS commands, e.g. DIR, the Norton Utilities program was used to inspect it. It was found that the virus moved the partition record from side zero, track zero, sector one to side zero, track zero, sector 17. The virus code occupied side zero, track zero, sector one.

```
0000: EB 1C 90 4D 53 44 4F 53 - 35 2E 30 00 02 02 01 00
      ...MSDOS5.0.....
0010: 02 70 00 D0 02 FD 02 00 - 09 00 02 00 00 00 33 C0
      .p............3.
0020: 8E D8 8B F8 8E D0 BC 00 - 7C B1 06 8B F4 8B DC C4
      ........|.......
0030: 06 4C 00 A3 AD 7C A1 13 - 04 8C 06 AF 7C 48 A3 13
      .L...|......|H..
0040: 04 D3 E0 8E C0 50 C7 06 - 4C 00 22 01 A3 4E 00 B8
      .....P..L."..N..
0050: C1 00 50 B9 00 01 FC F3 - A5 CB 10 87 01 28 28 00
      ..P..........((.
0060: 01 02 1E 50 B2 65 8B FA - B0 FF AB 83 C7 04 B0 3F
      ...P.e.........?
0070: AB B1 0B F3 AA B1 13 B7 - 03 E8 89 FE B4 13 CD 2F
      ................/
0080: 2E 8C 1E AF 01 8B CA CD - 2F 89 0E AD 01 81 F9 22
      ......../......"
0090: 01 74 0A 8C C9 83 C1 10 - 51 B8 F3 00 50 CB B0 FF
      .t......Q...P...
00A0: E6 21 BA 80 00 B9 01 00 - B8 11 03 9C 9A 59 EC 00
      .!...........Y..
00B0: F0 FE C6 80 E6 07 75 F0 - FE C5 75 EC 80 C1 40 EB
      ......u...u...@.
00C0: E7 E8 36 00 CD 19 B0 10 - E8 02 00 B0 2F 86 D6 E6
      ..6........./...
00D0: 70 E8 06 00 E4 71 86 F0 - E6 71 C3 B8 01 03 E8 05
      p....q...q......
00E0: 00 9C FF 1E AD 00 E8 05 - 00 50 E8 D9 FF 58 87 16
      .........P...X..
00F0: 5A 00 C3 E8 04 00 E8 ED - FF CB 0E 1F 8E C1 E8 C5
      Z...............
0100: FF F6 C2 F0 74 04 89 16 - 5A 00 2A F2 80 E2 0F 02
      ....t...Z.*.....
0110: F2 E8 B2 FF B2 80 B9 01 - 00 8A F5 58 9C 0E 50 B8
      ............X..P.
0120: 01 02 FC 1E 57 56 51 50 - 0E 1F FA 8C D7 BE 00 F0
      ....WVQP........
0130: 8E D6 90 8E D7 FB 80 FC - 03 75 24 26 80 3F 4D 75
      .........u$&.?Mu
0140: 1E 0A E2 3A CC 75 18 8B - FB BE 9E 00 B9 23 00 22
      ...:.u.......#."
0150: D2 75 0A BE 02 00 B8 EB - 60 AB B9 FE 01 F3 A4 58
      .u......`......X
0160: 59 8B F0 E8 78 FF 72 1B - 50 0A F6 75 14 83 F9 01
      Y...x.r.P..u....
0170: 75 0F 8B C6 80 FC 02 74 - 10 80 FC 03 75 03 E8 95
      u......t....u...
0180: FF F8 58 5E 5F 1F CA 02 - 00 51 26 80 7F 28 7C 75
      ..X^_....Q&.▒(|u
```

TABLE 3-14 ***EXEBUG*-INFECTED BOOT SECTOR**

```
0190: 0E 26 8B 8F 5C 00 B8 01 - 02 E8 42 FF 59 EB E2 52
      .&..\.....B.Y..R
01A0: B1 11 F6 C2 80 75 36 B5 - 28 26 80 7F 15 FC 73 02
      .....u6.(&.▒..s.
01B0: B5 50 88 2E 5E 00 06 53 - 33 C0 8E C0 26 C4 1E 78
      .P..^..S3...&..x
01C0: 00 06 53 FE C0 8A C8 26 - 86 4F 04 B4 05 BB 5E 00
      ..S....&.O....^.
01D0: 0E 07 E8 09 FF 5B 07 26 - 86 4F 04 5B 07 E8 FB FE
      .....[.&.O.[....
01E0: 5A 72 B9 89 0E 5C 00 26 - C7 07 EB 1C BE 1E 00 8D
      Zr...\.&........
01F0: BF 1E 00 B9 E0 01 F3 A4 - 59 E8 DF FE EB 80 55 AA
      ........Y.....U.
```

TABLE 3-14 (continued) ***EXEBUG*-INFECTED BOOT SECTOR**

ANALYSIS

Memory was infected in all cases. All test disks were infected: diskettes had their boot sectors replaced by the virus code and the hard drive's partition record was moved to make space for the virus. The first attempt to boot the computer after an infection produced a CMOS error.

The virus interfered with the CMOS set-up by changing the setting for the A (boot) drive to "None". Furthermore, the hard disk drive was found to be inaccessible.

To restore the proper operation of the infected test computer, the "None" CMOS setting of the A drive had to be replaced by the correct setting.

The computer had to be booted from an uninfected diskette, and the Norton Utilities program was then used to move sector 17 (side zero, cylinder zero) of the hard drive (the original partition record) back to sector one (its original location). This process replaced the virus code by the original partition record.

If the physical write-protection switches of the hard drive were set to write-protect, the computer would freeze during booting with the hard drive access light on. It was assumed that the virus was attempting to write to the hard disk, causing this symptom. No data, executable or system files were affected as a logical unit. No separate sectors were affected in any way. The system date was set to various test dates (all the days in March and 26th of May) to entice the virus to overwrite the hard disk, but it had no effect (Hoffman, 1993).

When the infected boot sector is compared to the uninfected sector, some differences are evident. The JUMP statement and Operating System name areas are intact. The FAT type, boot code and the messages have been replaced by what appears to be foreign program code.

Thus the location of the virus code as being on side zero, track zero, sector one has been confirmed.

On the 5,25-inch diskettes, the actual boot sector and parts of it were found at the following locations:

Cylinder 17, Side zero, Sector two: boot sector code starts approximately one third from the top of the sector.

Cylinder 20, Side zero, Sector eight: only the last one quarter of the boot sector was stored here.

Cylinder 26, Side one, Sector six: boot sector code starts approximately one quarter from the top of the sector.

Subsequent booting from the infected disk was successful, notwithstanding the unusual placing of the boot sector relevant to the beginning of a sector. The boot sector on an infected 3,5-inch diskette was nowhere to be found.

3.6.7 *FRODO* VIRUS

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	N	Y	Y	Y	Y	Y	Y	Y
Data files:									
Access?	X	Y	Y	Y	Y	Y	Y	Y	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	Y	Y	Y
Length altered?	*	X	*	*	*	*	*	*	*
Root dir. changed?	Y	X	Y	Y	Y	Y	Y	Y	Y
Execute success 2?	Y	X	Y	Y	Y	Y	Y	Y	Y
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	#	X	X	X	X	X	X	X	#
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-15 ***FRODO* RESULT LISTING**

Notes:

*: While the virus was resident, a DOS DIR command did not show any change in the length of infected files. However, inspection of the infected files on an uninfected computer indicated that their lengths did increase by 4096 bytes.

#: Only the length of the COMMAND.COM file was altered.

```
 Volume in drive A has no label
 Volume Serial Number is 15E3-2045
 Directory of A:\

CHKDSK   EXE      20296 04-09-91   5:00a
COMMAND  COM      51941 04-09-91   5:00a
DISKCOPY COM      15889 04-09-91   5:00a
FORMAT   COM      37007 04-09-91   5:00a
TREE     COM      10997 04-09-91   5:00a
        5 file(s)     136130 bytes
                      152576 bytes free
```

TABLE 3-16 **DIRECTORY LISTING: *FRODO***

ANALYSIS

Memory was infected in all cases. All disks with free space and either COM or EXE program files stored on them attracted infection. All infected files had their respective lengths increased by 4096 bytes (compare TABLE 3-16 to Appendix C), without altering the time and date stamps of these files. None of the test data files was affected in any way. However, if a data file had its extension renamed to one whose ASCII code sums to 223 or 226 (e.g. .BON, .GSE, .WIB), and that file was loaded into memory, it became infected.

Attempting to execute this renamed data file did not cause memory to become infected. All files executed normally after having been infected and disinfected using the test programs.

Of the three system files, only COMMAND.COM was infected, but it still allowed normal booting to take place afterwards. No individual sectors were affected in any way.

While the virus was resident in memory, DOS seemed to be unaware of the file size change that had taken place. A DIR command showed the file as having the same size as prior to the infection.

Due to the fact that *Frodo* is considered to be a stealth virus (Hoffman, 1993), and could therefore hide its presence from the user, the following scenario was simulated: one of the anti-viral program files was infected with *Frodo*. Loading that checking program into memory afterwards infected memory. Every executable file that was subsequently checked by the anti-viral program on a hard drive attracted *Frodo* infection, even though the files were not executed.

As a result over 400 executable files were infected, and booting from the hard drive placed the *Frodo* virus in memory. This resulted from the fact that the COMMAND.COM file was infected, which caused the *Frodo* virus to spread to any other program that was run. At this point there was no evidence or symptoms confirming the presence of the virus in the infected files, since a DOS DIR command showed all files as having their original sizes.

A complete low-level format followed by a full restore process had to be executed to clear the infection. All attempts to disinfect the hard drive without resorting to these two drastic steps failed.

A further problem was the inability of the DOS DIR program to perceive the change in file size of an infected file. To the average user, comparing program file sizes is an easily understood way of identifying an infection.

3.6.8 *JERUSALEM* VIRUS

RAM infection?	*								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	#	Y	Y	Y	Y	Y	Y	~
Data files:									
Access?	X	Y	Y	Y	Y	Y	Y	Y	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	#	#	Y	Y
Length altered?	$	X	Y	Y	Y	Y	Y	Y	Y
Root dir. changed?	Y	X	Y	Y	Y	Y	Y	Y	Y
Execute success 2?	@	X	N	N	Y	N	N	N	%
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-17 ***JERUSALEM*** **RESULT LISTING**

Notes:

*: When an attempt was made to run the Toolkit while the virus was resident, the program aborted to DOS with the following error message: "Critical error, re-install the Toolkit. If the problem persists, please call Technical support. Overlays failure -1". The computer was reset and rebooted from an uninfected diskette.

The Toolkit now executed normally. As a result, it was assumed that the virus was in RAM initially.

#: This test diskette showed no virus infection. When the Turbo Pascal program was run with the virus resident, the test computer froze. After rebooting from an uninfected diskette, Pascal executed normally. When the TurboCash program was run with the virus resident, it aborted to DOS with the error message: "Abnormal program termination". The other four test programs executed normally.

~: Files on the hard disk drive were infected by the virus. However, since the Toolkit would not run with a virus in memory, the computer was rebooted from an uninfected diskette, and the Toolkit was run from diskette.

$: All non-hidden files with a COM or EXE extension were infected, except COMMAND.COM. The infection involved that the file's length was increased by 1813 bytes.

@: The following programs did run after disinfection: CHKDSK, TREE, FORMAT. The DISKCOPY program did not run after disinfection.

%: The following programs did run after disinfection: 123.EXE (Lotus). The following programs did not run after disinfection: RMCOBOL.EXE (Cobol), RUNCOBOL.EXE (Cobol), DBASE.EXE (DBase), TURBO.EXE (Pascal), BTRIEVE.EXE (TurboCash), BETA.EXE (TurboCash), WP.EXE (WordPerfect).

```
 Volume in drive A has no label
 Volume Serial Number is 15E6-0D44
 Directory of A:\

CHKDSK   EXE     18016 04-09-91   5:00a
COMMAND  COM     47845 04-09-91   5:00a
DISKCOPY COM     13606 04-09-91   5:00a
FORMAT   COM     34724 04-09-91   5:00a
TREE     COM      8714 04-09-91   5:00a
        5 file(s)     122905 bytes
                      165888 bytes free
```

TABLE 3-18 **DIRECTORY LISTING: *JERUSALEM***

ANALYSIS

Since *Jerusalem* is a file virus, the diskette with no executable files did not show any infections. All three types of disks containing program files were infected. EXE files increased in size by 1816 and infected COM files by 1813 bytes (compare TABLE 3-18 to Appendix C). No change was made to any file's date or time stamp.

Memory also became infected in all cases. When an attempt was made to confirm memory infection after having infected the hard drive, the system froze. No data files were affected in any way.

All program files were infected when executed on a computer with infected memory (except COMMAND.COM). In these cases, the respective file sizes increased by 1813 bytes. Furthermore, all program files were deleted when executed on a computer with infected memory and a system date of Friday the 13th. It was found that the deletion process was based on the method DOS uses to delete files.

The first character of the filename of the file deleted (in the root directory) was changed to the E5 (hex) character, but the contents of the file on disk were left intact.

Mixed success was achieved when executing a disinfected file. Five out of six application programs and one out of four system utility programs did not execute after disinfection.

The only non-hidden system file did attract infection. This file was deleted upon subsequent booting (on the trigger date). No bad sectors were created, since the virus code was appended to a file during infection in all cases, and not stored on disk as a sector.

The statements about the data-destroying capabilities of the *Jerusalem* virus found in three of the prior studies (Denning (1988:236), Radai (1989:111) and Highland (1989:465)) were clarified. Both Highland's and Denning's findings were confirmed, while Radai's statement that infected files would be "...erased from the disk" was disproved.

3.6.9 *MICHELANGELO* VIRUS

RAM infection?	*								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	Y	N	N	N	N	N	N	Y
Data files:									
Access?	X	Y	Y	Y	Y	Y	Y	Y	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	Y	Y	Y
Length altered?	N	X	N	N	N	N	N	N	N
Root dir. changed?	N	X	X	X	X	X	X	X	N
Execute success 2?	X	X	X	X	X	X	X	X	Y
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-19 ***MICHELANGELO* RESULT LISTING**

Notes:

*: When an attempt was made to scan memory after infecting the test computer, the Toolkit reported: "Virus in memory - aborting." Subsequent boots from a clean diskette gave no such problems. It was thus assumed that the virus was in memory.

```
0000: E9 AC 00 F5 00 80 9F 02 - 03 00 94 00 00 CE 1E 50
      ...............P
0010: 0A D2 75 1B 33 C0 8E D8 - F6 06 3F 04 01 75 10 58
      ..u.3.....?..u.X
0020: 1F 9C 2E FF 1E 0A 00 9C - E8 0B 00 9D CA 02 00 58
      ...............X
0030: 1F 2E FF 2E 0A 00 50 53 - 51 52 1E 06 56 57 0E 1F
      .....PSQR..VW.
0040: 0E 07 BE 04 00 B8 01 02 - BB 00 02 B9 01 00 33 D2
      ..............3.
0050: 9C FF 1E 0A 00 73 0C 33 - C0 9C FF 1E 0A 00 4E 75
      .....s.3......Nu
0060: E4 EB 43 33 F6 FC AD 3B - 07 75 06 AD 3B 47 02 74
      ..C3...;.u..;G.t
0070: 35 B8 01 03 B6 01 B1 03 - 80 7F 15 FD 74 02 B1 0E
      5........▒..t...
0080: 89 0E 08 00 9C FF 1E 0A - 00 72 1B BE BE 03 BF BE
      .........r......
0090: 01 B9 21 00 FC F3 A5 B8 - 01 03 33 DB B9 01 00 33
      ..!.......3....3
00A0: D2 9C FF 1E 0A 00 5F 5E - 07 1F 5A 59 5B 58 C3 33
      ......_^.ZY[X.3
00B0: C0 8E D8 FA 8E D0 B8 00 - 7C 8B E0 FB 1E 50 A1 4C
      ........|....P.L
00C0: 00 A3 0A 7C A1 4E 00 A3 - 0C 7C A1 13 04 48 48 A3
      ...|.N...|...HH.
00D0: 13 04 B1 06 D3 E0 8E C0 - A3 05 7C B8 0E 00 A3 4C
      ..........|....L
00E0: 00 8C 06 4E 00 B9 BE 01 - BE 00 7C 33 FF FC F3 A4
      ...N......|3....
00F0: 2E FF 2E 03 7C 33 C0 8E - C0 CD 13 0E 1F B8 01 02
      ....|3.........
0100: BB 00 7C 8B 0E 08 00 83 - F9 07 75 07 BA 80 00 CD
      ..|.......u.....
0110: 13 EB 2B 8B 0E 08 00 BA - 00 01 CD 13 72 20 0E 07
      ..+.........r ..
0120: B8 01 02 BB 00 02 B9 01 - 00 BA 80 00 CD 13 72 0E
      ..............r.
0130: 33 F6 FC AD 3B 07 75 4F - AD 3B 47 02 75 49 33 C9
      3...;.uO.;G.uI3.
0140: B4 04 CD 1A 81 FA 06 03 - 74 01 CB 33 D2 B9 01 00
      ........t..3....
0150: B8 09 03 8B 36 08 00 83 - FE 03 74 10 B0 0E 83 FE
      ....6.....t.....
0160: 0E 74 09 B2 80 C6 06 07 - 00 04 B0 11 BB 00 50 8E
      .t............P.
0170: C3 CD 13 73 04 32 E4 CD - 13 FE C6 3A 36 07 00 72
      ...s.2.....:6..r
0180: CF 32 F6 FE C5 EB C9 B9 - 07 00 89 0E 08 00 B8 01
      .2..............
0190: 03 BA 80 00 CD 13 72 A6 - BE BE 03 BF BE 01 B9 21
      ......r........!
```

TABLE 3-20 ***MICHELANGELO*-INFECTED BOOT SECTOR**

```
01A0: 00 F3 A5 B8 01 03 33 DB - FE C1 CD 13 EB 90 00 00
      ......3.........
01B0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 0A 52
      ...............R
01C0: 65 70 6C 61 63 65 20 61 - 6E 64 20 70 72 65 73 73
      eplace and press
01D0: 20 61 6E 79 20 6B 65 79 - 20 77 68 65 6E 20 72 65
      any key when re
01E0: 61 64 79 0D 0A 00 49 4F - 20 20 20 20 20 20 53 59
      ady...IO      SY
01F0: 53 4D 53 44 4F 53 20 20 - 20 53 59 53 00 00 55 AA
      SMSDOS   SYS..U.
```

TABLE 3-20 (continued) ***MICHELANGELO*-INFECTED BOOT SECTOR**

ANALYSIS

RAM, 360 Kb diskettes and the hard drive were infected, but *Michelangelo* ignored 3,5-inch diskettes. No files of any type were affected by the infection, since only the boot sector or partition record was moved to another location.

On the 5,25-inch diskettes the boot sector was moved from cylinder zero side zero sector one to cylinder zero side one sector three (the 11th sector). The virus code was then stored in cylinder zero side zero sector one.

DOS stores the root directory in seven consecutive sectors on this diskette type (Appendix D). The last one of these seven sectors is the 11th sector from the start. DOS allows 112 files per directory on this diskette type, thus the directory entries of 112/7 = 16 files are stored per sector.

The action of copying the boot sector onto the 11th sector will delete any root directory entries of files starting at the 112 - 16 = 96 file count.

Since none of the test diskettes had 96 or more files stored on them, this deletion of root directory entries was not found. However, a test was done on a diskette with 112 files in the root, and *Michelangelo* did indeed overwrite the last 16 root directory entries. However, this action did not affect the contents of these files in any way. It was possible to retrieve their contents using the Norton program.

On the hard drive the partition record was moved from cylinder zero side zero sector one to cylinder zero side zero sector seven. The virus code was then stored in cylinder zero side zero sector one.

Sector seven on the test hard drive contained only zeroes before the infection, so the infection did not delete any information. A check was done on two other hard drives, and it was found that none of the three hard drives stored any information on cylinder zero side zero, sector two up to the last sector on that cylinder and side.

In an attempt to check the effect of the claimed trigger date (the 6th of March), the system date was set to the 6th of March before a *Michelangelo* infection took place. After the infection, the computer was rebooted from the (now infected) hard drive.

The screen cleared and the hard disk drive light remained on. At the same time the regular ticking sound of the hard drive stepping motor could be heard, similar to the sound produced during a DOS FORMAT process. The test computer was left in this status for 35 minutes, with no change in the symptoms described above.

After rebooting from an uninfected diskette, and running the Norton Utilities test program, it was found that the hard drive was overwritten by foreign data. No trace could be found of any system areas, program files or data files anywhere on the hard drive. Hoffman's claim (1993) that random characters from memory are written on the hard disk appears to be correct.

When the infected boot sector is compared to the uninfected sector, some differences are evident. The destination address of the JUMP statement appeared to have been replaced by a different address. The Operating System name has been removed. The FAT type, boot code and the first part of the messages have been replaced by what appears to be foreign program code. Only the last part of the messages is visible. Thus the location of the virus code as being in side zero, track zero, sector one has been confirmed.

3.6.10 *NOINT* VIRUS *

RAM infection?	#								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	~	Y	Y	Y	Y	Y	Y	Y
Data files:									
Access?	X	Y	Y	Y	Y	Y	$	$	#
Contents changed?	X	N	N	N	N	N	$	$	#
Root dir. changed?	X	N	N	N	N	N	$	$	#
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	@	Y	#
Length altered?	N	X	N	N	N	N	@	N	#
Root dir. changed?	N	X	N	N	N	N	@	Y	N
Execute success 2?	Y	X	N	N	N	N	@	N	#
System files:									
Boot?	%	X	X	X	X	X	X	X	N
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-21 ***NOINT* RESULT LISTING**

Notes:

*: Excessive disk accessing noises were evident when using both types of diskettes during testing of this virus.

#: The hard drive was inaccessible after having infected it. Therefore the Toolkit was run from diskette, and it was confirmed that RAM and the hard drive were indeed infected.

~: When the test programs had to be run from the hard drive, the DOS error message "Invalid drive specification" was received. Therefore test Disk Two could not be infected using the prescribed method.

However, a DIR command was executed on this test disk, assuming that any BSV or PRV present in RAM would now infect this diskette. A subsequent check confirmed infection.

$: An 18th file named Š<ÉMSDOS5.0 was added to this disk, with a size of zero bytes, date 18/0/1980 and time 12.00pm. The name and extension of this file are made up of bytes four to 15 from the boot sector of any diskette formatted under MSDOS 5.0. On test Disk Seven, the first 17 files were left unaltered. The 18th file was the one identified above, and the remaining 50 files, plus the subdirectory with its 18 files were missing. A CHKDSK on this test disk produced a DOS error message which warned that allocation units were being lost. This file plus one other one were cross-linked. On test Disk Eight, the 13th (and last) file on the disk was the data file (REPORT02.DOC). This file was deleted and replaced by the nonsensical file. A CHKDSK on this test disk produced 16 lost allocation units, including a reference to this file.

@: The program files needed to run TurboCash were apparently deleted, hence this program could not be run.

%: An attempt to boot from test Disk One produced the message "You cannot boot from this diskette. Please SWITCH OFF the computer and start again." The Norton Utilities test program showed that the Toolkit put this message into the boot sector during the disinfection process.

Although all the files on the disk were intact and accessible, booting was no longer possible due to the absence of the boot code in the boot sector.

```
0000: EB 3C 90 50 43 20 54 6F - 6F 6C 73 00 02 02 01 00
      .<.PC Tools.....
0010: 02 70 00 D0 02 FD 02 00 - 09 00 02 00 00 00 00 00
      .p..............
0020: 00 00 00 00 00 00 00 00 - 00 00 00 FA 33 C0 8E D0
      ............3...
0030: BC 00 7C 16 1F BE 00 7D - AC 0A C0 74 09 B4 FA 33
      ..|...}...t...3
0040: C0 8E D8 8B E0 B8 C0 07 - 8E D0 FB A1 4C 00 36 A3
      ............L.6.
0050: 0C 01 A1 4E 00 36 A3 0E - 01 A1 13 04 36 A3 AB 00
      ...N.6......6...
0060: 48 48 A3 13 04 B1 06 D3 - E0 8E C0 36 A3 8C 00 B8
      HH.........6....
0070: DA 00 A3 4C 00 8C 06 4E - 00 B9 00 02 16 1F 33 F6
      ...L...N.....3.
0080: 8B FE FC F3 A4 36 FF 2E - 8A 00 8E 00 80 9F 8C D0
      .....6..........
0090: 8E C0 B8 01 02 33 DB F6 - C2 80 74 11 B9 07 00 BA
      .....3....t.....
00A0: 80 00 9C 2E FF 1E 0C 01 - EB 16 90 80 02 B9 03 00
      ................
00B0: BA 00 01 9C 2E FF 1E 0C - 01 72 05 B2 80 E8 62 00
      .........r....b.
00C0: 33 C0 8E D8 8E C0 8E D0 - BC 00 04 33 DB 33 C9 33
      3..........3.3.3
00D0: D2 2E FF 2E D6 00 00 7C - 00 00 1E 50 80 FC 02 75
      .......|...P...u
00E0: 39 81 FA 80 00 75 29 83 - F9 01 75 24 51 B9 07 00
      9....u)...u$Q...
00F0: B8 01 02 9C 2E FF 1E 0C - 01 59 72 20 2E 88 26 21
      .........Yr ..&!
0100: 01 58 1F 55 8B EC 80 66 - 06 FE 5D CF CF 01 00 C8
      .XU...f..]......
0110: 83 FA 01 77 05 E8 0A 00 - 72 00 58 1F 2E FF 2E 0C
      ...w....r.X.....
0120: 01 00 53 51 52 56 57 06 - BE 02 00 B8 01 02 B9 01
      ..SQRVW.........
0130: 00 BB 00 02 0E 07 32 F6 - 9C 2E FF 1E 0C 01 73 0F
      ......2.......s.
0140: 33 C0 9C 2E FF 1E 0C 01 - 4E 75 E0 F9 EB 51 90 BE
      3.......Nu...Q..
```

TABLE 3-22 ***NOINT*-INFECTED BOOT SECTOR**

```
0150: D6 00 0E 1F 8B 04 3B 84 - 00 02 74 43 BF 03 00 BE
      .....;...tC....
0160: 03 02 B9 3B 00 FC F3 A4 - BE BE 03 BF BE 01 B9 42
      ...;...........B
0170: 00 F3 A4 B8 01 03 BB 00 - 02 B9 03 00 B6 01 80 FA
      ................
0180: 01 76 05 B9 07 00 32 F6 - 9C 2E FF 1E 0C 01 72 0F
      .v....2.......r.
0190: B8 01 03 33 DB 32 F6 B1 - 01 9C 2E FF 1E 0C 01 07
      ...3.2..........
01A0: 5F 5E 5A 59 5B C3 FC FC - 00 00 00 00 00 0D 00 06
      _^ZY[...........
01B0: 00 00 00 00 0B 05 34 03 - 00 00 00 00 00 53 00 00
      ......4......S..
01C0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
01D0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
01E0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
01F0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
```

TABLE 3-22 (continued) ***NOINT*-INFECTED BOOT SECTOR**

ANALYSIS

All disk types and RAM were infected. During infection, the partition record (for the hard disk) and the boot sector (for diskettes) were moved to the following locations:

5,25-inch diskette:	Cylinder zero, side one, sector three
3,5-inch diskette:	Cylinder zero, side one, sector three
Hard disk drive:	Cylinder zero, side zero, sector seven

The new location for the boot sector on 5,25-inch diskettes is the last sector of the root directory. This is a relatively safe area to store the boot sector, since it would only be noticed by an average user if that disk contained a large number of files.

However, the same location is used on the 3,5-inch diskette but this time it occupies space close to the beginning of the root directory. This explains the deletion of certain files on test Disk Seven and Eight - the overwriting of the boot sector destroyed those file entries in the root directory. The appearance of the foreign 18th file is now also clear - the first few characters of the boot sector appeared to be the name of a file in the root directory.

After infection, Norton Utilities indicated that the original partition record location on the hard disk contained all zeroes. Intermittent "Sector not found" errors occurred on the hard drive during the checking procedure.

At a later stage, Norton Utilities indicated that the original partition record contained apparent garbage, which is believed to be the virus program code. The Norton Utilities program was used to copy the partition record back to its original location, which restored the operation of the hard drive back to normal.

When the infected boot sector is compared to the uninfected sector, some differences are evident. The JUMP statement and the DOS version number (in this case the disk was formatted via the PCTools utility program) were intact. The FAT type, boot code and messages have been replaced by what appears to be foreign program code. Thus the location of the virus code as being on side zero, track zero, sector one has been confirmed.

3.6.11 *PLASTIQUE* VIRUS

RAM infection?	*								
DISK NO:	1	2	3	4	5	6	7	8	9
Disk infection?	#	N	#	#	#	#	#	#	#
Data files:									
Access?	X	Y	Y	Y	Y	#	#	Y	#
Contents changed?	X	N	N	N	N	#	#	N	#
Root dir. changed?	X	N	N	N	N	#	#	N	#
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	Y	Y	Y
Length altered?	~	X	~	~	~	N	~	~	~
Root dir. changed?	Y	X	Y	Y	Y	N	Y	Y	$
Execute success 2?	Y	X	Y	Y	Y	@	N	Y	$
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-23 ***PLASTIQUE* RESULT LISTING**

Notes:

*: While the virus was considered to be in RAM, running the Toolkit from the hard disk caused the computer to freeze. Running the Toolkit from diskette showed no viruses in memory. However, running a program file from a write-enabled diskette immediately afterwards did attract infection from *Plastique*.

No explanation could be found for the inability of the Toolkit to detect *Plastique* in RAM.

#: The Toolkit identified file infections as Anticad 3 (an alias for *Plastique*). The following files were listed as being infected:

Disk One:	CHKDSK.EXE, DISKCOPY.COM, FORMAT.COM, TREE.COM
Disk Three:	RMCOBOL.EXE, RUNCOBOL.EXE
Disk Four:	DBASE.EXE
Disk Five:	123.EXE
Disk Six:	TURBO.EXE
Disk Seven:	BETA.EXE, BTRIEVE.EXE
Disk Eight:	WP.EXE
Disk Nine:	The same 12 files as listed for Disk One to eight above were infected.

Furthermore, whenever Turbo Pascal was run (test Disks Six and Nine) with the virus in memory, the disk light would stay on and the computer would freeze. Whenever TurboCash was run (test Disks Seven and Nine) with this virus resident in memory, the message "Abnormal program termination" would appear, and the user was returned to DOS.

~: Except for TURBO.EXE and BETA.EXE, all the files experienced an increase in size, indicated in bytes below.

Disk One:	CHKDSK.EXE: 3020. The other three: 3012.
Disk Three:	RMCOBOL.EXE, RUNCOBOL.EXE: both 2996.
Disk Four:	DBASE.EXE: 2756.
Disk Five:	123.EXE: 3012.
Disk Seven:	BTRIEVE.EXE: 3016.
Disk Eight:	WP.EXE: 2612.
Disk Nine:	The figures are as for Disk One to eight above.

$: The root directory status and execution of programs on the hard drive followed the same pattern as the corresponding programs on diskette, as indicated in the columns to the left of this row.

@: While attempting to disinfect the infected files, the Toolkit reported that the file TURBO.EXE was "overwritten by the virus", but it nonetheless cleaned and renamed it.

```
 Volume in drive A has no label
 Volume Serial Number is 15E5-141D
 Directory of A:\

CHKDSK   EXE      19220 04-09-91   5:00a
COMMAND  COM      47845 04-09-91   5:00a
DISKCOPY COM      14805 04-09-91   5:00a
FORMAT   COM      35923 04-09-91   5:00a
TREE     COM       9913 04-09-91   5:00a
        5 file(s)     127706 bytes
                      160768 bytes free
```

TABLE 3-24 **DIRECTORY LISTING: *PLASTIQUE***

ANALYSIS

Infection of files on all three disk types took place. COM and EXE files were infected, with the exception of COMMAND.COM. It was assumed that this system file was skipped by the infection mechanism to escape easy detection by anti-virus programs or alert users. The virus added itself to the infected file, and increased the length of the infected file by between 2612 and 3020 bytes. No data files were affected in any way.

All the infected files executed successfully after infection. After disinfection neither Turbo Pascal nor TurboCash executed successfully. Booting was not affected in any way by infection. No separate sectors were affected in any way.

The directory listing of TABLE 3-24 clearly shows how the infected files grew by between 3012 and 3020 bytes (for this diskette) in size, without changing the date or time of the last write operation.

3.6.12 *PRETORIA* VIRUS *

RAM infection?	N								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	N	Y	Y	Y	Y	Y	Y	Y
Data files:									
Access?	X	Y	#	#	#	Y	#	%	#
Contents changed?	X	N	#	#	#	N	#	%	#
Root dir. changed?	X	N	#	#	#	N	#	%	N
Program files:									
Execute success 1?	N	X	N	N	N	Y	N	N	N
Length altered?	~	~	~	~	~	N	~	~	~
Root dir. changed?	Y	X	Y	N	N	X	Y	N	Y
Execute success 2?	Y	X	Y	Y	Y	X	N	Y	N
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	Y	X	X	X	X	X	X	X	Y
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-25 ***PRETORIA* RESULT LISTING**

Notes:

*: Since this virus is a DAFV, it could not be loaded from the Virus Master disk every time (it immediately tried to infect the write-protected master disk, failed, but did not go resident). The *Pretoria*-infected test file had to be copied to every User Test disk and executed from there. The infection step differed from that of the other viruses: the infected file was run first, since this is the only way to activate the virus. The other test programs were then run as before.

#: Whenever any one of the Test programs was run after infection, the test computer froze.

%: When the WP.EXE file was run, the message "Packed file is corrupt" appeared, and the user was returned to DOS.

~: The length of various program files was changed after infection as listed below. The increase in file size is given in bytes for each file.

Disk One:	CHKDSK.EXE	4096
	DISKCOPY.COM	4975
	FORMAT.COM	4975
	TREE.COM	4975
	COMMAND.COM	4975
Disk Two:	FILEMAN.EXE	4096
Disk Three:	RMCOBOL.EXE	4096
Disk Four:	DBASE.EXE	4096
Disk Five:	123.EXE	4096
	LOTUS.COM	4975
Disk Seven:	BTRIEVE.EXE	4096
Disk Eight:	WP.EXE	4096

Disk Nine: The same 12 files as listed for Disk One to eight above were infected, with the same resultant increase in file size.

```
 Volume in drive A has no label
 Volume Serial Number is 15E4-1961
 Directory of A:\

CHKDSK   EXE     20296 04-09-91   5:00a
COMMAND  COM     52820 04-09-91   5:00a
DISKCOPY COM     16768 04-09-91   5:00a
FORMAT   COM     37886 04-09-91   5:00a
TREE     COM     11876 04-09-91   5:00a
VCPRETDA COM      5854 01-01-80  12:33a
        7 file(s)     141404 bytes
                      146432 bytes free
```

TABLE 3-26 **DIRECTORY LISTING: *PRETORIA***

ANALYSIS

Memory was not infected, since direct action file viruses do not install their code into RAM (Hoffman, 1993). This was confirmed by the Toolkit. All disks with free space and program files stored on them attracted infection.

All EXE files increased by 4096 bytes, while COM files grew by 4975 bytes, without affecting the date or time stamps of the infected files. The infection process could not escape notice, since the execution of a simple program (which should take two or three seconds), sometimes took minutes to complete. Excessive disk accessing and seeking noises were also evident.

Further experiments were carried out after setting the test computer's system date to the claimed trigger date of the 16th of June (Hoffman, 1993; Anon, 1991:19). The following results refer to these laboratory experiments.

All disks containing non-hidden files had all files and directories in the root directory renamed to ZAPPED when an infected file was run on the trigger date. This made it impossible to run any of those files or to move to any subdirectory from the root directory using the DOS CD command.

Since the file sizes were visible after the rename process took place, some files and directories could be identified. An attempt to rename them to their original names using DOS failed. The Norton Utilities test program had to be used, in which case renaming and execution of infected files was successful. One exception was that of the COMMAND.COM system file, which caused the system to freeze after being renamed.

It was not possible to disinfect an infected disk using the Toolkit. Firstly, the Toolkit did not consider the files named ZAPPED to be infected, and secondly, it could not penetrate into different directories below the root, since all directories were renamed to ZAPPED.

3.6.13 *STONED* VIRUS

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	Y	N	N	N	N	N	N	Y
Data files:									
Access?	X	Y	Y	Y	Y	Y	Y	Y	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	Y	Y	Y
Length altered?	N	X	N	N	N	N	N	N	N
Root dir. changed?	N	X	N	N	N	N	N	N	N
Execute success 2?	Y	X	Y	Y	Y	Y	Y	Y	Y
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-27 ***STONED*** **RESULT LISTING**

```
0000: EA 05 00 C0 07 E9 99 00 - 00 83 03 00 C8 E4 00 80
      ................
0010: 9F 00 7C 00 00 1E 50 80 - FC 02 72 17 80 FC 04 73
      ..|...P...r....s
0020: 12 0A D2 75 0E 33 C0 8E - D8 A0 3F 04 A8 01 75 03
      ...u.3....?...u.
0030: E8 07 00 58 1F 2E FF 2E - 09 00 53 51 52 06 56 57
      ...X.....SQR.VW
0040: BE 04 00 B8 01 02 0E 07 - BB 00 02 33 C9 8B D1 41
      ...........3...A
```

TABLE 3-28 ***STONED*****-INFECTED BOOT SECTOR**

```
0050: 9C 2E FF 1E 09 00 73 0E - 33 C0 9C 2E FF 1E 09 00
      ......s.3.......
0060: 4E 75 E0 EB 35 90 33 F6 - BF 00 02 FC 0E 1F AD 3B
      Nu..5.3.......;
0070: 05 75 06 AD 3B 45 02 74 - 21 B8 01 03 BB 00 02 B1
      .u..;E.t!.......
0080: 03 B6 01 9C 2E FF 1E 09 - 00 72 0F B8 01 03 33 DB
      .........r....3.
0090: B1 01 33 D2 9C 2E FF 1E - 09 00 5F 5E 07 5A 59 5B
      ..3......._^.ZY[
00A0: C3 33 C0 8E D8 FA 8E D0 - BC 00 7C FB A1 4C 00 A3
      .3........|..L..
00B0: 09 7C A1 4E 00 A3 0B 7C - A1 13 04 48 48 A3 13 04
      .|.N...|...HH...
00C0: B1 06 D3 E0 8E C0 A3 0F - 7C B8 15 00 A3 4C 00 8C
      ........|....L..
00D0: 06 4E 00 B9 B8 01 0E 1F - 33 F6 8B FE FC F3 A4 2E
      .N.....3.......
00E0: FF 2E 0D 00 B8 00 00 CD - 13 33 C0 8E C0 B8 01 02
      .........3......
00F0: BB 00 7C 2E 80 3E 08 00 - 00 74 0B B9 07 00 BA 80
      ..|..>...t......
0100: 00 CD 13 EB 49 90 B9 03 - 00 BA 00 01 CD 13 72 3E
      ....I.........r>
0110: 26 F6 06 6C 04 07 75 12 - BE 89 01 0E 1F AC 0A C0
      &..l..u.........
0120: 74 08 B4 0E B7 00 CD 10 - EB F3 0E 07 B8 01 02 BB
      t...............
0130: 00 02 B1 01 BA 80 00 CD - 13 72 13 0E 1F BE 00 02
      .........r......
0140: BF 00 00 AD 3B 05 75 11 - AD 3B 45 02 75 0B 2E C6
      ....;.u..;E.u...
0150: 06 08 00 00 2E FF 2E 11 - 00 2E C6 06 08 00 02 B8
      ................
0160: 01 03 BB 00 02 B9 07 00 - BA 80 00 CD 13 72 DF 0E
      ............r...
0170: 1F 0E 07 BE BE 03 BF BE - 01 B9 42 02 F3 A4 B8 01
      ..........B.....
0180: 03 33 DB FE C1 CD 13 EB - C5 07 59 6F 75 72 20 50
      .3........Your P
0190: 43 20 69 73 20 6E 6F 77 - 20 53 74 6F 6E 65 64 21
      C is now Stoned!
01A0: 07 0D 0A 0A 00 4C 45 47 - 41 4C 49 53 45 20 4D 41
      .....LEGALISE MA
01B0: 52 49 4A 55 41 4E 41 21 - 00 00 00 00 00 00 00 00
      RIJUANA!........
01C0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
01D0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
01E0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
01F0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
```

TABLE 3-28 (continued) ***STONED*-INFECTED BOOT SECTOR**

ANALYSIS

RAM, 5,25-inch diskettes and the hard drive were infected. The 3,5-inch diskettes were not affected in any way. During infection, the actual boot sector was moved to sector 11 on the 5,25-inch diskette.

A part of the root directory on 5,25-inch diskettes was overwritten by the boot code. This would only cause a problem if the diskette contained more than 96 files in the root directory, since directory entries for files 97 and up normally occupied the sector to be overwritten. The files in question therefore would lose their root directory entries, but no change would be made to their actual contents.

A further experiment was carried out on test Disk One. The diskette was infected, and files were added to the diskette until the 96 count was exceeded. As expected, the moment the file count exceeded 96, the boot sector was overwritten, making that diskette unbootable. No files were affected as a logical unit, with the 96 file exception as mentioned above.

The partition record of the hard drive was moved from cylinder zero, side zero, sector one to physical sector seven (cylinder zero, side zero, sector seven). This location is normally unused.

The virus code installed itself in the sector normally used for the partition record. In this case, no data was lost as a result of the relocation of the partition record.

Solomon (1989) claims that a small percentage of hard disks (1% to 5%) do use physical sector seven for part of one of the FAT's, and *Stoned* infection would therefore cause file information loss in such cases. However, this claim could not be substantiated. Highland's claims (1989:97) that this virus changes sector headers on a track could not be confirmed.

No file of any type was affected as a logical unit. One disk sector which had no relation to any specific file was destroyed by *Stoned.*

When the infected boot sector is compared to the uninfected sector, some differences are evident. The (short) JUMP statement had been replaced by an inter-segment long JUMP, and the DOS version number, FAT type, boot code and messages have been replaced by what appears to be foreign program code. The only recognizable text is the string:

"Your PC is now Stoned!
LEGALISE MARIJUANA!"

Thus the location of the virus code as being in side zero, track zero, sector one has been confirmed.

3.6.14 *SUNDAY* VIRUS

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	*	Y	Y	Y	#	-	Y	Y
Data files:									
Access?	X	Y	Y	Y	Y	Y	Y	Y	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	N	N	Y	N
Length altered?	$	X	$	$	$	N	$	$	$
Root dir. changed?	Y	X	Y	Y	Y	N	Y	Y	Y
Execute success 2?	Y	X	Y	Y	Y	N	N	Y	N
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-29 ***SUNDAY* RESULT LISTING**

Notes:

*: With the virus resident and the hard drive write-protected, the test programs were run from the hard drive in an attempt to infect this test disk. The DBase program refused to load by exiting to DOS, while the other five test programs all caused the test computer to freeze. Thus test Disk Two could not be accessed to cause an infection. An infection check reported no infection, as expected. It was assumed that the action of the virus attempting to infect the program files on the write-protected hard disk as they were loaded, caused the test computer to freeze.

#: When the Pascal program was executed with the virus resident, the test computer froze. An infection check later showed that the run file of this program was infected by the virus.

~: When the TurboCash program was executed with the virus resident, it returned the message: "Abnormal program termination" and exited to DOS. However, an infection check later showed that the run file of this program was infected by the virus.

$: The length of various program files was changed after having been infected as listed below. The increase in file size is given in bytes for each file.

Disk One:	CHKDSK.EXE	1644
	DISKCOPY.COM	1636
	FORMAT.COM	1636
	TREE.COM	1636
Disk Three:	RMCOBOL.EXE	1620
	RUNCOBOL.EXE	1620
Disk Four:	DBASE.EXE	1380
Disk Five:	123.EXE	1636
Disk Seven:	BTRIEVE.EXE	1640
Disk Eight:	WP.EXE	1236

Disk Nine: The same 12 files as listed for Disk One to eight above were infected, with the same resultant increase in file size.

```
 Volume in drive A has no label
 Volume Serial Number is 15E2-262B
 Directory of A:\

CHKDSK   EXE     17844 04-09-91   5:00a
COMMAND  COM     47845 04-09-91   5:00a
DISKCOPY COM     13429 04-09-91   5:00a
FORMAT   COM     34547 04-09-91   5:00a
TREE     COM      8537 04-09-91   5:00a
        5 file(s)     122202 bytes
                      165888 bytes free
```

TABLE 3-30 **DIRECTORY LISTING: *SUNDAY***

ANALYSIS

RAM and executable files on all disks were infected. The COMMAND.COM file on bootable disks was a notable exception. It was assumed that the virus did not infect this file in an attempt to escape detection by anti-virus programs. No data files were affected in any way.

Only some program files executed successfully after infection. Disk disinfection had no effect on the damaged files - they still refused to execute. The lengths of the infected files were increased by between 1236 and 1644 bytes (compare TABLE 3-30 to Appendix C).

The boot process was not affected in any way, and no separate sectors were affected. Hoffman (1993) claims that the following message will be displayed when the system date is any Sunday:

> "Today is Sunday! Why do you work so hard?
> All work and no play make you a dull boy!
> Come on! Let's go out and have some fun!"

This message could not be evoked from the virus with a system date being that of any Sunday.

3.6.15 *TELEFONICA* VIRUS

RAM infection?	Y								
DISK NO:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Disk infection?	Y	Y	Y	Y	N	Y	N	Y	Y
Data files:									
Access?	X	Y	Y	Y	Y	Y	Y	Y	Y
Contents changed?	X	N	N	N	N	N	N	N	N
Root dir. changed?	X	N	N	N	N	N	N	N	N
Program files:									
Execute success 1?	Y	X	Y	Y	Y	Y	Y	Y	Y
Length altered?	N	X	N	N	N	N	N	N	N
Root dir. changed?	N	X	N	N	N	N	N	N	N
Execute success 2?	Y	X	Y	Y	Y	Y	Y	Y	Y
System files:									
Boot?	Y	X	X	X	X	X	X	X	Y
Length altered?	N	X	X	X	X	X	X	X	N
Individual sectors:									
Marked bad?	N	N	N	N	N	N	N	N	N

TABLE 3-31 ***TELEFONICA* RESULT LISTING**

```
0000: EB 1C 90 49 42 4D 20 20 - 33 2E 33 00 02 01 01 00
      ...IBM  3.3.....
0010: 02 E0 00 60 09 F9 07 00 - 0F 00 02 00 00 00 BB 00
      ...`............
0020: 7C 33 C0 FA 8E D0 8B E3 - FB 8E D8 A1 13 04 48 A3
      |3............H.
0030: 13 04 B1 06 D3 E0 8E C0 - B9 00 02 0E 1F 8B F3 33
      ..............3
0040: FF FC F3 A4 06 BB EE 00 - 53 CB BC 9E 92 8F 9E 5B
      ........S......[
0050: 9E DF BE 91 8B 96 D2 AB - BA B3 BA B9 B0 B1 B6 BC
      ................
0060: BE DF D7 BD 9E 8D 9C 9A - 93 90 91 9E D6 F2 F5 FF
      ................
0070: 40 01 06 00 68 01 08 00 - 80 02 01 01 D0 02 02 01
      @...h...........
0080: 60 09 0D 01 A0 05 04 01 - 40 0B 0E 01 FF FF 06 00
      `........@.......
0090: F4 02 02 01 B8 01 03 CD - 13 C3 BD 04 00 B8 01 02
      ................
00A0: CD 13 73 07 32 E4 CD 13 - 4D 75 F2 C3 9C 9A ED C1
      ..s.2...Mu......
00B0: 00 F0 C3 8A 0E EC 00 BE - 70 00 03 F1 8A 4C 02 8A
      ........p....L..
00C0: 74 03 C3 A0 E9 00 B4 03 - CD 13 FE C6 C3 52 8B D1
      t............R..
00D0: 86 F2 B1 06 D2 E2 80 CA - 01 8B CA 5A C3 E8 E3 FF
      ...........Z....
00E0: 3A 36 EA 00 75 F7 C3 50 - 00 0F 02 02 10 00 8E D8
      :6..u..P........
00F0: 32 E4 CD 13 BB 00 02 8A - EB 8A 16 ED 00 E8 B3 FF
      2...............
0100: E8 97 FF FF 06 EC 02 81 - 3E EC 02 90 01 76 03 E9
      ........>....v..
0110: 0F 01 E8 7F FF 33 C0 A3 - EC 02 8E C0 BB 00 7C FE
      ...▒.3........|.
0120: C1 E8 76 FF 80 FA 80 75 - 03 E9 81 00 8C CB 81 EB
      ..v....u........
0130: 00 10 8E C3 33 DB B1 01 - BA 80 00 E8 5C FF 72 6D
      ....3.......\.rm
0140: 26 81 BF 4A 00 BC 9E 74 - 64 51 52 B4 08 CD 13 72
      &..J...tdQR....r
0150: 20 FE C6 88 36 EA 00 8A - D1 86 E9 80 E5 3F 88 2E
      ...6........?..
0160: E9 00 51 B1 06 D2 EA 59 - 8A EA 41 89 0E E7 00 EB
      ..Q....Y..A.....
0170: 10 C6 06 EA 00 04 C6 06 - E9 00 11 C7 06 E7 00 63
      ...............c
0180: 02 5A 59 C6 06 EC 00 1C - 88 16 ED 00 B1 07 E8 03
      .ZY.............
```

TABLE 3-32 ***TELEFONICA*-INFECTED BOOT SECTOR**

```
0190: FF 06 1F 0E 07 B9 42 00 - BE BE 01 8B FE FC F3 A4
      .....B.........
01A0: FE C1 E8 EF FE BB 00 02 - B1 06 E8 E7 FE EB 51 00
      ..............Q.
01B0: 1F 5E 2E FF 2E AE 00 50 - BB 00 7C 53 CB AD 80 01
      ^.....P..|S....
01C0: 01 00 04 04 D1 02 11 00 - 00 00 EE FF 00 00 00 00
      ................
01D0: C1 03 05 04 D1 CF FF FF - 00 00 11 44 00 00 00 00
      ...........D....
01E0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
      ................
01F0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 55 AA
    ..............U.
```

TABLE 3-32 (continued) ***TELEFONICA*-INFECTED BOOT SECTOR**

ANALYSIS

All three disk types attracted infection. Infection of 5,25-inch diskettes caused the boot sector to be moved to cylinder zero, side one, sector three. The original location of the boot sector (cylinder zero, side zero, sector one) was now occupied by what appears to be the virus program code. Furthermore, the sector just before the relocated boot sector (cylinder zero, side one, sector two) also appeared to contain virus code.

Infection of 3,5-inch diskettes caused the boot sector to be moved to cylinder zero, side one, sector 15. The original location of the boot sector (cylinder zero, side zero, sector one) was now occupied by what appeared to be the virus program code.

Furthermore, the sector just before the relocated boot sector (cylinder zero, side one, sector 14) also appeared to contain virus code.

Infection of the hard disk drive caused the partition record to be moved to cylinder zero, side zero, sector seven. The original location of the partition record (cylinder zero, side zero, sector one) was now occupied by what appeared to be the virus program code. Furthermore, the sector just before the relocated partition record (cylinder zero, side one, sector six) also appeared to contain virus code. No evidence could be found of any file infections caused by *Telefonica*, as claimed by Hoffman (1993).

When the infected boot sector is compared to the uninfected sector, some differences are evident. The JUMP statement and DOS version number were not changed (the Virus Master Disk was formatted with a different version of DOS than test Disk One). The FAT type, boot code and messages have been replaced by what appears to be foreign program code.

Thus the location of the virus code as being in side zero, track zero, sector one has been confirmed.

CHAPTER FOUR ** TEST RESULTS AND CONCLUSIONS

4.1 INTRODUCTION

This research was undertaken to assist the computer users in industry in evaluating the danger that virus programs pose to stored information. If they drew any conclusions about the data-destroying potential of computer viruses based on reports in the general press, they would be left with a perception of a looming danger posed by these programs.

Many reports of virus epidemics were found, and some references explained the operation of virus programs. Conferences on the topic of computer viruses produced results which were too general to be of practical value. Most importantly, it was found that there was lack of references with regard to the actual damage caused by viruses to stored information. All the hypotheses formulated subsequently refer to the danger that viruses pose to the stored information of a PC user.

Since the results of this research are of importance to users in industry, it was considered necessary to determine whether viruses have already had detrimental effects on users' information in industry. It was clear that many users have had problems with virus infections, especially in the Western Cape.

Controlled laboratory tests were then used to determine exactly what the effects of infection by a number of viruses were on stored information.

4.2 TEST RESULTS

4.2.1 *AIRCOP*

Hard drives were not infected, and only 0,139% of data on a 360-kb diskette (0,0347% on a 1,44-Mb diskette) was lost due to the action of the virus. This data would be destroyed only if a file occupied a certain sector, which is unlikely on a 360-kb diskette, since it is the very last sector. A user is not likely to be using a diskette for further data storage if it is already over 99% full. Furthermore, even if a file was partially destroyed, it would involve only one sector, or 512 bytes. The location of the sector on a 1,44-Mb diskette is in the centre of the disk, resulting in a higher probability of damaging files.

No files were addressed as units, so that critical files on a diskette were as susceptible to deletion as non-critical files. Owing to their location at the beginning of the data area, the hidden files of the operating system would not be affected at all.

Since hard drives are not affected, the overall impact of this virus on the stored information of users is insignificant. **It was therefore concluded that the *Aircop* virus does not pose a threat to PC users.** Solomon's classification of this virus as causing Trivial damage is confirmed, since the time taken, for example, to delete a damaged file by re-copying it from a master disk could take approximately three minutes. The removal of the virus code by using an anti-virus program is equally easy.

However, the average user's perception of the results of this virus could differ from the above conclusion. A program which causes the computer to freeze when it is executed from diskette could be a real obstacle to a user.

4.2.2 *BOUNCING BALL*

This virus boots successfully only on 8088-based PC's and it requires relatively new ROM devices to function. This implies that the threat of the *Bouncing Ball* will diminish as time goes by, since 8088-based PC's have relinquished their market share to 80286 and higher processors. 8088-based motherboards have not been available as new components for a number of years. Therefore the number of 8088-based computers with new ROM devices in industry are fixed and can only decrease over time.

The bad sector that was created did not affect any other data on the disk, and no file of any type was altered in any way. The fact that it updated only the first copy of the FAT could create problems for programs when they attempt to update both FAT's.

However, this kind of symptom is easily overcome by utility programs such as Norton Utilities or PCTools.

It is concluded that the *Bouncing Ball* has only a nuisance value to PC users, and that it does not pose a threat to them. Solomon's classification of this virus as causing Trivial damage is confirmed, since the time taken to remove the virus code by making use of, for example, the Dr. Solomon program, could be less than three minutes.

Once again it is evident that an average user could experience the presence of this virus on his system as a problem. The sudden appearance of the travelling bouncing ball on the screen should be recognized by even a novice as an abnormal symptom, and could cause the user to experience a loss of confidence in his computer hardware and programs.

4.2.3 *BRAIN*

The copy of the *Brain* virus used was either corrupted or contained a bug. **Therefore no conclusions could be reached** as the virus could not be activated to enable results to be obtained.

4.2.4 *CASCADE*

This virus affected no data files, and all program files that were infected could be cleaned without any side-effects. No other negative results were found. The fact that the *Cascade* virus did infect the COMMAND.COM system file gives reason for concern. However, in all cases even COMMAND.COM was disinfected successfully by using the anti-virus program. Furthermore, some known anti-virus programs (Vaccine, for example) monitor the length, date and time of the system files, since these files are crucial to the functioning of the operating system. These programs would indicate an infection when used to check a suspected disk.

It is concluded that the *Cascade* virus does not pose a threat to a PC user. Solomon's classification of this virus as causing Trivial damage is confirmed. Even if a number of files were infected, disinfection via an anti-virus program could be done within three minutes.

Although the claimed symptom of the falling letters was not seen, its appearance in other copies of this virus program could annoy the average user.

It could even lead to irrational actions by the user, such as resetting the computer while disk files are open, or even formatting the disk.

These actions will result in information being lost, without removing the virus infection.

4.2.5 *DURBAN*

The copy of the *Durban* virus used appeared either to contain some programming errors, or was corrupted, and hence **no conclusions were reached.** Solomon's classification of this virus as causing Moderate damage could therefore not be confirmed.

4.2.6 *EXEBUG*

This virus did infect all disk types, but did not cause any direct damage to files or disk areas. Damage to hard disks could not be proved. However, inaccessibility of both the A diskette drive and the hard drive gives reason for concern. Even though a user may not boot from the A drive, or use it for data storage, the interference of the virus with the CMOS data will produce an error message after bootup. The user will then be faced with a choice: continue with the boot process (normally resulting in the A drive then being inaccessible) or enter the CMOS setup procedure to restore the A drive setting.

Although the second option will solve the problem temporarily, it cannot be assumed that the average user is familiar with CMOS settings.

The influence of this virus on the confidence level of the user cannot be ignored. However, the damage caused by this virus is easy to repair, provided that the user has access to some technical expertise. **It is thus concluded that this virus does not pose a threat to the information stored by the PC user.**

4.2.7 *FRODO*

Frodo did infect memory and files on all disk types. All program files could be executed normally after having been disinfected. This was a tedious process, since disinfection had to be done on a clean system. However, the capability *Frodo* has to infect almost any file loaded into memory via an executable file will eventually be detrimental to the information stored by the PC user. Loading an overlay file from an executable file (without the user being aware of it) for example, could infect that file and spread the infection from there.

In summary; the *Frodo* virus possesses the ability to spread faster and remain unnoticed longer in a given computer system than any one of the other viruses investigated in this research.

Furthermore, the difficulty experienced in removing *Frodo* from a hard drive gives reason for concern. Inexperienced users could, for example, destroy all information on a hard disk in an attempt to clear up the virus infection.

It is thus concluded that this virus does pose a threat to the PC user. Solomon's classification of this virus as causing Moderate damage is therefore verified. This is mainly due to the ability of this virus to by-pass detection by the average user, resulting in the virus possibly infecting many files before it is detected.

4.2.8 *JERUSALEM*

This virus appends its own code to all COM and EXE files when they are executed with the virus resident. However, the infected programs still ran successfully in all cases. The only exception was when an EXE file was run after it had been infected once. In this case re-infection occurred, which caused the file to grow in size upon every infection. The file was run consecutively on an infected computer, until it became too large to fit into available memory, causing it to abort loading. The resultant error message initially appears to be in error: "Program too big to fit into memory".

By the time the user sees this message, the infected file will probably have been run many times to allow it to grow to such proportions.

It is quite likely that the infection has spread to other program files at this point. However, no damage was done to the original program file.

A problem occurred when attempting to undelete program files that were deleted by executing them when the system date was Friday the 13th. However, during each of 1990, 1991 and 1992, only two days and in 1993 and 1994 only one day fell on Friday the 13th. Thus one can conclude that the probability of a PC's system date being the trigger date is approximately 0,438% (eight days out of 1826). Furthermore, owing to the awareness among PC users of the implication of this system date, many users are by-passing potential problems by setting their system date to a different value on that day.

Normally program files are easier to restore than data files. To recover application program files, for example, the user simply needs to copy them over from the master disks or from some backup media, or at worst reinstall the application program.

Should PC users have no back-up of any data files, and they lose all the information stored on their hard disk drives, it could be impossible to recover such files.

Consequently, it is regarded as not as serious a problem when program files are lost as when data files are lost. **It was concluded that the *Jerusalem* virus is not a serious threat to PC users' program or data files.**

4.2.9 *MICHELANGELO*

All disk types except 3,5-inch were infected, but no specific files or disk areas were affected.

The apparent deletion of files past the 96-file limit is not critical, since the contents of these files are not affected. The exact disk areas occupied by each deleted file are still stored in the FAT's, and the Norton Utilities program could build up the files' directory entries again.

However, the average user will probably not know this, and might once again act without thinking on the symptom of missing files. Furthermore, if files are added to this disk after the deletion of files, the new files will overwrite the old files if the deletion was not reversed.

The overwriting of the hard disk drive does give reason for concern. Although the virus takes this action on only one day per year (i.e. 0,275% of the time), the overwriting is permanent.

The only way the user can restore the information on the hard disk is by reformatting it and doing a complete restore.

It is thus concluded that this virus does pose a threat to the information stored by the PC user. Solomon's classification of this virus as causing Moderate damage is therefore verified.

4.2.10 *NOINT*

The excessive disk-accessing noises and delays produced while this virus is active cannot escape notice. Even an average user would be aware that his computer system is not behaving normally.

The action of this virus is similar to that of *Michelangelo* with regards to the apparent deletion of files. Once again the results of this action are reversible, but only if no new files have been added to the disk.

The damage to the hard disk drive can also be repaired. However, the average user's response to a message to the effect that he cannot access any programs or data on his hard disk drive, could cause further problems.

The damage caused by this virus is easy to repair, provided that the user has access to some technical expertise.

It is thus concluded that this virus does not pose a threat to the information stored by the PC user. Solomon's classification of this virus as causing Trivial damage is therefore verified.

4.2.11 *PLASTIQUE*

Although all disk types were infected, all programs could still be executed after infection. Furthermore, the files that could not be executed after disinfection are all program files. As discussed under 4.2.8 above, program files are relatively easy to replace.

It is thus concluded that this virus does not pose a threat to the information stored by the PC user. Solomon's classification of this virus as causing Moderate damage is disproved.

4.2.12 *PRETORIA*

During the experiments with this virus, it was clear that its scanning effect cannot escape notice. A small test program that simply displays a message on the monitor, normally took approximately two seconds to execute from a diskette. When running this program again after having been infected, it took more than a minute just to execute.

During this time it scanned the root directory and renamed all entries found to ZAPPED.

It is assumed that even a novice user will have his suspicions aroused as this extremely slow process holds up the execution of normal work. Furthermore, the renaming process only occurred on the trigger date, therefore it can be assumed that the probability of this occurrence is only 0,275% (one day out of 365). Restoring these renamed files is relatively easy, using to a utility program such as the Norton Utilities. **It is thus concluded that this virus does not pose a threat to the information stored by the PC user.**

4.2.13 *STONED*

The hard disk drive was infected, and diskette infections caused files, in isolated cases, to have their root directory entries deleted. These cases involved the existence of 96 or more files being present on a 360-kb diskette. This fact in isolation poses little cause for concern, since it is common practice rather to store files on a hard disk when this many files have to be stored on a magnetic disk.

The fact that a diskette with fewer than 96 files which had become infected, and subsequently had files added to it then became unbootable, is considered to be of little consequence. A bootable MSDOS 5.0 diskette (360 kb) leaves only 242688 bytes of space free, which translates to 237 clusters of 1 kb each.

To fill that space with another 93 files, requires files with an average size of 2,5 kb each. Program files of this small size are uncommon, and it is not likely that a user will create or store that many small data files on a bootable DOS diskette. The report by Solomon (1989) concerning damage to some hard disk system areas could not be confirmed during the laboratory experiments. If this did occur however, it would be possible to retrieve the lost data from the other copy of the FAT.

The damage caused by this virus under DOS is easy to repair, provided that the user has access to some technical expertise.

It is thus concluded that this virus does not pose a threat to the information stored by the PC user. Solomon's classification of this virus as causing Moderate damage is disproved.

4.2.14 *SUNDAY*

Some program files were adversely affected after infection by the *Sunday* virus, since they refused to execute afterwards. As discussed in 4.2.8 above, program files are relatively easy to replace, and this damage is therefore considered to be of little consequence.

Data files were not affected in any way. The booting process also executed normally. The only infection symptom that the average user would notice, is the fact that the execution of some programs may cause the computer to freeze.

It is thus concluded that this virus does not pose a threat to the information stored by the PC user. Solomon's classification of this virus as causing Minor damage is confirmed.

4.2.15 *TELEFONICA*

No detrimental effects on the average user of infection by this virus could be found. No program, data or system files were affected, no strange symptoms appeared and the booting process was not impeded in any way.

Removal of the virus code from, for example the hard drive, was a one-minute operation using the Norton Utilities program.

The damage caused by this virus under DOS is easy to repair, provided that the user has access to some technical expertise. **It is thus concluded that this virus does not pose a threat to the information stored by the PC user.** Solomon's classification of this virus as causing Moderate damage is disproved.

4.3 CONCLUSIONS

The results discussed above are summarized in Table 4.1.

	$H1_a$	$H1_b$	$H1_c$	$H1_d$	$H2_a$	$H2_b$	$H2_c$	$H2_d$
Aircop	T	T	T	F	F	T	F	T
Bouncing Ball	T	T	F	T	F	F	F	T
Brain	I	I	I	I	I	I	I	I
Cascade	T	T	F	T	F	T	T	F
Durban	I	I	I	I	I	I	I	I
Exebug	T	T	T	T	T	F	T	F
Frodo	T	T	T	T	F	T	T	F
Jerusalem	T	T	T	T	F	T	F	F
Michelangelo	T	T	F	T	F	F	F	F
NoInt	T	T	T	T	T	T	T	F
Plastique	T	T	T	T	T	T	F	F
Pretoria	F	T	T	T	T	T	T	F
Stoned	T	T	F	T	T	T	T	T
Sunday	T	T	T	T	F	T	F	F
Telefonica	T	T	T	T	F	F	F	F

TABLE 4-1 **RESULTS OF INFECTIONS OF TEST DISKS**

Key:
F: False
I: Inconclusive
T: True

Eleven of the 15 viruses used in this research lead to the conclusion that the PC user need not be unduly concerned about their effect (*Aircop*, *Bouncing Ball*, *Cascade*, *Exebug*, *Jerusalem*, *NoInt*, *Plastique*, *Pretoria*, *Stoned*, *Sunday* and *Telefonica*).

A further two cases were inconclusive (*Brain*, *Durban*), and the last two (*Frodo* and *Michelangelo*) could have a detrimental effect on the information stored by a PC user.

However, in almost all the cases it was evident that the effect a computer virus could have on information stored on a magnetic disk was to a large extent determined by the following:

- the way that the user responds to a symptom presented by a virus infection.
- the experience with and insight the person investigating and clearing the virus problem has in:
    - the operation of viruses
    - the layout of disks (Mantelman, 1989)
    - the usage of utility and anti-viral programs.

When each one of the hypotheses is considered in isolation, and the inconclusive results are ignored, the following conclusions can be drawn:

H_{1a}: Twelve out of 13 viruses did infect RAM. Since the 13th one (*Pretoria*) does not have to infect RAM for it to spread, it can be concluded that all the other virus programs used in this research make use of RAM to spread infection.

H_{1b}: All 13 viruses did infect 5,25 inch 360 kb diskettes. This type of diskette is therefore highly susceptible to infections.

H_{1c}: Nine out of 13 viruses did infect 3,5-inch 1,44-Mb diskettes. It can be concluded that users of this diskette type are less susceptible to virus infections than those using 5,25-inch 360-kb diskettes.

H_{1d}: Twelve out of 13 viruses did infect hard disk drives. It can be concluded that hard disk users are virtually as likely to attract virus infections as are 5,25-inch 360-kb diskette users.

H_{2a}: Five out of 13 viruses destroyed or adversely affected user data files. It can be concluded that data files are susceptible to the adverse effects of computer viruses.

H_{2b}: Nine out of 13 viruses affected program files. Program files are thus susceptible to computer virus actions.

H_{2c}: Six out of 13 viruses affected system files. It can be concluded that system files are susceptible to the adverse effects of computer viruses.

H_{2d}: Three out of 13 viruses did affect separate sectors. The fact that users' files could be addressed and potentially damaged via randomly chosen sectors on a disk by so few viruses does thus not pose a substantial threat to their stored information.

The main hypotheses of this research can now be evaluated.

- **"Computer viruses never pose danger to the stored information of a PC user."**

The potentially destructive and sometimes irreversible results of *Frodo* and *Michelangelo* infections have proven this hypothesis to be false.

- **"Computer viruses can sometimes pose danger to the stored information of a PC user."**

This hypothesis has been proven to be true. In some cases (*Bouncing Ball* and *Telefonica*, for example), infection by a virus had no visible detrimental effect on the user's stored information. In other cases the user could lose data under certain circumstances (*Jerusalem's* file deletion on certain dates, for example). In this case it will be possible to retrieve the lost data. In yet other cases, the user could lose data without being able to retrieve it (hard disk overwriting by *Michelangelo*, for example), except from a backup medium.

- **"Computer viruses will always pose danger to the stored information of a PC user."**

This hypothesis has been proven to be false. In some cases (*Aircop* infection of a 5,25-inch diskette, for example), infection by a virus had no visible detrimental effect on the user.

In general it can therefore be concluded that the majority of current computer viruses need not cause the user to have serious concerns about his stored information. This is subject to the prerequisite that the user has a recent backup, and an understanding of the following three points:

- the operation of viruses
- the layout of disks
- the usage of utility and anti-viral programs.

4.4 SUMMARY

The following emerged from the findings of this research:

- By following some basic ground-rules, PC users can avoid loss of stored information.

- The damage done by computer viruses to stored information is generally limited to one file or disk area.

- Where damage to stored information did occur, it was seldom irreversible.

- Irrational user responses to virus symptoms provide a large potential for damage to stored information.

- The availability of master program disks (for program file restoration) and recent, tested data backup is essential to recovery from a computer virus infection.

- Users can solve most problems caused by virus infections if they have a basic understanding of disk structure, i.e. tracks, sectors, sides, the FAT, etc, and of the use of a program like Norton Utilities or PCTools.

- The fact that some of the findings of prominent virus researchers could not be verified, points to the unstable nature of virus programs.

- Claims regarding the damage inflicted by viruses must be considered to be valid only for a specific copy of the virus under discussion.

CHAPTER FIVE ** IMPLICATIONS AND RECOMMENDATIONS

5.1 INTRODUCTION

The implications of the findings of this research are addressed, some recommendations made to the computer user in industry, and suggestions for further study are noted.

5.2 IMPLICATIONS OF FINDINGS

Certain computer users are more susceptible to suffer loss of stored information due to computer virus infections than others.

To take precautions against the loss of any stored information, PC users must:

5.2.1 Have access to the master disks of all the programs executed on a regular basis.

5.2.2 Make regular backup of at least data files.

5.2.3 Use a recent version of a legal anti-viral program.

5.2.4 Understand the basic operation of computer viruses (i.e. the four types and method of infection).

5.2.5 Understand the layout of a DOS disk (i.e. sectors, tracks, cylinders, sides, partitions).

5.2.6 Know and be able to use a disk utility program (e.g. Norton Utilities, PCTools).

5.3 RECOMMENDATIONS

It is recommended that the average PC user in the industry follow the set of guide-lines below. This will minimize the risk of losing information as a result of a computer virus infection.

- Use original legal software.
- Make regular backups of especially data files (use BACKUP and RESTORE, or even COPY, DISKCOPY or XCOPY).
- Use physical write-protection on diskettes where practically possible.
- Use logical write-protection (the DOS ATTRIB command, for example) to set all program files to read only.
- Minimize the use of diskettes on different PC's, including maintenance personnel using their own diskettes.
- Obtain and use a recent version of a reliable anti-virus program and arrange for regular updates.
- Check all new software with this program before installing or using it.
- Obtain and use a recent version of a reliable utility program.
- If it is impractical to train all users on anti-virus software, utility programs and the operation of viruses, train at least one support specialist.
- Be aware of the characteristic symptoms caused by the most popular viruses.

- Do not boot a hard drive PC from a diskette without good reason.

5.4 DISINFECTION PROCEDURE

The average PC user should be able to clear up a virus infection without assistance. This procedure can be done if the user has a set of prepared, marked diskettes available, as suggested below.

The preparation for the disinfection procedure must first be done on an **uninfected computer**, and in case of a suspected infection, the method described thereafter should be followed to the letter.

The assumptions below must hold for the disinfection procedure to be successful:

- The user knows the following basic DOS commands: DIR, FORMAT, COPY and DELETE.
- The user is familiar with the concepts: bootable diskette, booting a PC, installing a program, running an anti-virus program and physical diskette write-protection.
- The user has access to a computer without a hard drive.

5.4.1 PREPARATION FOR DISINFECTION

- Ensure that a bootable diskette is available (hereafter called the clean boot disk) which is of the same form factor as drive A of the computer. This diskette should have been formatted with the same version of DOS as on the hard drive, both containing the same system files.
- Ensure that a recent copy of an anti-virus program like Dr. Solomon's, CSIR VPS or Scan, is available on the same type of diskette as above (hereafter called the clean anti-virus disk). **Use physical write protection (the write protect tab for 5,25-inch or the square slider for 3,5-inch diskettes) to protect both these diskettes.**
- Identify a computer without a hard disk drive. Switch the power off. Use the clean boot disk to boot this computer. Run the anti-virus program from the clean anti-virus disk on this computer and check both diskettes for virus infections. If an infection is reported on the boot disk, it probably means that the boot sector or the COMMAND.COM file is infected. In this case, the hard disk from which this diskette was prepared, was infected. Repeat the first step above on a different computer. If the clean anti-virus disk is reported to be infected, reinstall the anti-virus software from the master disks on a known uninfected computer. Repeat this step until no infections are reported. Ensure that both diskettes are still write-protected.

The two disks mentioned above should be stored in a safe place away from the computer, possibly with the backup media.

5.4.2 DISINFECTION

Whenever a computer user suspects that a PC's memory or disk(s) have been infected by a virus, the method suggested below should be followed.

- Exit from all programs running on the suspect computer and get the DOS prompt on the screen. Switch the power off.
- Insert the clean boot disk into the A drive and switch the power on.
- After having booted successfully, run the anti-virus program from the clean anti-virus disk. Do not run any programs from the hard disk drive. Select the hard drive to be checked for infections. If a hard drive is not installed, specify the diskette drive to be used.
- Note the full path and name of each reported infected file. Also note whether or not a boot sector or partition record infection is reported.
- If file infections were reported, delete each infected file from the hard drive. Now replace these files by either copying them from a virus-free source or re-installing them from the master disks.

- If a boot sector or partition record infection has been reported, use the anti-virus program to remove the infection.
- Exit from all programs running on the suspect computer and get the DOS prompt on the screen. Switch the power off.
- Insert the clean boot disk into the A drive and switch the power on.
- After having booted successfully, run the anti-virus program from the clean anti-virus disk. Do not run any programs from the hard disk drive. Select the hard drive to be checked for infections. If a hard drive is not installed, specify the diskette drive to be used.
- No infections should be reported on the hard drive or in memory.

5.5 SUGGESTIONS FOR FURTHER STUDIES

This research points to areas for further study. Possible topics and methods are listed below.

5.5.1 VIRUS ORIGINS

Who writes viruses and why? Various authors of viruses and similar programs are known, for example, Morris who wrote the Internet worm (Highland, 1989:460) and the Alvi brothers who generated the *Brain* virus (Elmer De-Witt, 1988:62). The motives of these and other authors could be investigated and documented, in an attempt to answer this question.

5.5.2 NEW VIRUS GENERATIONS

The possibility and potential dangers of further generations of computer viruses need to be researched. No cases are known at present of viruses damaging hardware or by-passing physical write-protection on disks.

If any one or both of hardware damage or by-passing of write-protection could be managed by virus authors, it would give new insight to the whole problem of damage done by viruses to computer-stored information. This could be explored, possibly by attempting to write virus code to achieve the two goals mentioned.

5.5.3 VIRUSES AND SOFTWARE COPYING

The effect computer viruses might have on a user's perspective on the illegal copying of commercial software has not been researched. It has been proven during this research that a virus can be transferred from disk to disk by a file or disk copy operation. Therefore, if a user indiscriminately copies programs from other users instead of using original software, the chances of spreading a virus are increased.

5.5.4 VIRUS MUTATIONS

The results of the mutation of a computer virus could produce findings relevant to the damage done by viruses to stored information.

The symptoms a virus presents to a user could easily be changed. For example, by simply altering a text string which is displayed by the virus (contained in the code), even a novice could create a mutation of a known virus.

Often anti-viral software searches for a known string of text or code to identify a virus program. By changing this string, a "new" virus could be generated. A study could be done to determine if it is possible to change the actual operation of a virus without technical expertise, by attempting this on a known virus. The actions of the mutated virus could then be compared to those of the original copy.

5.5.5 MULTIPLE INFECTIONS

The possible results of multiple infections by different viruses of one disk or of memory or both have not been covered by this research. This research has documented the results and implications of single virus infections on disks. One could query the combined result of more than one virus infection on one disk or in one computer's memory.

The researcher could set up a table of possible multiple infections, activate these infections and then document the resultant damage to data and program files. A comparison between results so achieved and the results of this research would be informative.

5.5.6 VIRUSES ON NETWORKS

Reports on problems caused by computer viruses on networks are found in the literature. The first question a researcher could ask is: Do viruses cause damage on a network? If the answer is affirmative, the next point is: Can the damage be contained using the built-in network security features?

Furthermore, it could be determined whether or not a virus can spread from, for example, one workstation to another workstation via the file server.

5.5.7 VIRUSES IN THE FUTURE

The emergence of new operating systems such as Chicago and Windows NT could have a profound effect on the incidence of viruses. Both these operating systems will allow DOS programs to run, on the condition that they do not bypass the operating system, write directly to devices, etc.

However, neither will support the execution of any of the viruses considered in this research, since they all involve actions which by-pass the operating system (DOS). These actions include writing directly to disk (*Michelangelo* and *Aircop*) or to memory (*Frodo*). Most modern operating systems run in protected mode and do not allow programs direct access to memory or system devices.

The researcher could consider the possibility that virus authors might find ways to overcome the built-in safety measures of these operating systems. They could reverse engineer these operating systems to obtain their source code. The insight so obtained might enable them to create viruses which are complex enough to execute under control of the resident operating system.

Furthermore, the effect of viruses which run under operating systems other than DOS (Unix, Next, VMS, the Macintosh, etc) could be addressed.

5.6 SUMMARY

The results of this study amongst users in the business world are in line with findings of a study by Koo (1990), aimed at the academic community which found that: "... the people at greatest risk of computer virus infection are those college students who use a computer every day but have minimal knowledge about computer viruses."

Technical mistakes in widely read articles (see Section 1.4.1) also confirm this general lack of insight into the layout and operation of disks and computers in general.

Since this research was aimed at the average PC user and not the computer scientist, the results will be especially useful to the former group. A non-technical user should form a clear picture of the potential threat, or lack thereof, posed by a given virus. The value of anti-viral as well as utility-type programs is also evident from the research.

REFERENCES

Anon 1990. (a). **The Argus.** Supplement to Weekend Argus, Computer Virus Clinic, 5 May. Cape Town.

Anon 1990. (b). **PC Magazine.** Top Ten Sellers - A Five-Week History, 26 June.

Anon 1991. **Bit Magazine.** The Real Virus Story, December 1990/January 1991.

Bock, D.B. et al. 1993. Computer Viruses: Over 300 Threats to Microcomputing ... And Still Growing. **Journal of Systems Management**, 8 - 13. February.

Bradford, M. 1988. Computer Viruses Pose Business Peril. **Business Insurance**, 24, July 18.

Brown, J. 1993. Manufacturers team up to beat virus programs. **Computer Weekly**, 19, March 4.

Brunner, John. 1975. **The Shockwave Rider.** New York, Ballantine.

Cascarino, R. 1989. **Computer Security.** Unpublished lecture delivered at The Institute of Internal Auditor's Seminar on computer viruses, 22 November, Constantia, Cape Town.

Cullen, Scott W. 1989. The Computer Virus: Is There a Real Panacea?. **The Office**, 43 - 46, March.

Daly, James. 1993. Virus hunters look to Mac operating system. **Computerworld**, 38, May 10.

Denning, P.E. 1988. The Science of Computing: Computer Viruses. **American Scientist**, 236 - 238, May-June.

Detmann, T.R. 1988. **DOS Programmer's Reference.** QUE Books, 220 - 223.

Dewdney, A.K. 1984. Computer Recreations. **Scientific American**, 15 - 19, May.

Dvorak, J.C. 1992. New Stealth Viruses: A Menace to Users. **PC Magazine**, 93, April 14.

Elmer-DeWitt, P. 1988. Invasion of the Data Snatchers. **Time Magazine**, 56 - 64, 26 September.

Evans, D. 1993. Virus-selling IT boss says 'I'm innocent'. **Computer Weekly**, 1, March 18.

Francis, F. 1989. Do Computer Viruses Pose a Threat ? **Bank Administration**, 6 - 10, January.

Frost, D. 1989. **The Complete Computer Virus Handbook.** Pitman, September.

Highland, H.J.H. 1989. Random Bits & Bytes. **Computers & Security**, 8 (1), 11 - 13.

Highland, H.J.H. 1992. Random Bits & Bytes: Michelangelo Part 1. **Computers & Security**, 11 (3), 200 - 209.

Highland, H.J.H. 1993. Random Bits & Bytes: Virus Redux 1. **Computers & Security**, 12 (1), 4 - 14.

Highland, H.J.H. 1989. Random Bits & Bytes: The Internet Worm...Continued. **Computers & Security**, 8 (6), 460 - 478.

Hoffman, P.M. 1993. **Virus Information Summary List.** Version VSUM 9309, September 30. Downloaded from CompuServe.

Jones, M.C. et al. 1993. Perceptions of computer viruses: a cross-cultural assessment. **Computers & Security**, 12 (2), 191 - 197.

Joyce, E.J. 1988. Software Viruses: PC-Health Enemy Number One. **Datamation**, 27 - 30, October 15.

Kane, P. 1989. **V.I.R.U.S. Protection - Vital Information Resources Under Siege**. Bantam Books, June.

Koo, S.H. 1991. Identifying the Computer Virus Problem: College Students' Perceptions.

Mantelman, L. 1989. British Rail takes the steam out of a virus. **Data Communications International**, 33 - 34, April.

Palca, J. 1988. Networked Computers hit by intelligent 'virus'. **Nature**, 336,97, November 10.

Pozzo, M.D. 1990. Towards Computer Virus Prevention (Malicious Code, Trojan Horse).

Radai, Y. 1989. The Israeli PC virus. **Computers & Security**, 8 (2), 111 - 113.

Schoch, J.F. & Hupp, J.A., 1982. The "Worm" Programs - Early Experience with a Distributed Computation. **Communications of the ACM**, 25 (3), 172 - 180.

Solomon, A. 1989. **Computer Viruses**. Paper delivered at the ICIS Conference on Computer Viruses. Eskom College, Midrand, Johannesburg, 23 November.

Solomon, A. 1989. Dr Solomon's Anti-Virus Toolkit. **Program Manual**, Version 4.25, 11 - 13, S&S Computers.

Solomon, A. 1992. The Virus Authors Strike Back. **Computers & Security**, 11(7), 602 - 606.

Spafford, E.H. **The Internet Worm Program: An Analysis.** Purdue University Technical Report CSD-TR-823, 19, 44, 45.

Von Solms, B. 1989. **Computer Viruses.** Unpublished lecture delivered at The Institute of Internal Auditor's Seminar on Computer Viruses. Constantia, Cape Town, 22 November.

Van Wyk, K.R. 1989. The Lehigh Virus. **Computers & Security**, 8 (2), 107 - 109.

Watkins, S. 1993. Cop calls for help in virus battle. **Computing**, 7, March 4.

Whitmyer, Claude F. 1989. More Protection Programs Than There Are Viruses. **The Office**, 28, August.

Whitmyer, Claude F. 1989. Computer Viruses: the Potential for Damage Exists. **The Office**, 24, December.

Zajac, B.P. Jr. Computer Viral Risks - How Bad is the Threat ? **Computers & Security**, 11 (1), 29 - 34.

APPENDIX A - GLOSSARY

Average User

A computer user who runs application programs under a version of MSDOS or PCDOS, with the purpose of doing useful work. This person does not have any technical background, and his or her computer training, if any, involves only the usage of one or more application programs.

Bad sector

A sector on a DOS disk which can no longer be reliably used for data storage. DOS detects these sectors and records a code in the disk FATs to identify them.

Booting

The act of loading the operating system from disk into volatile memory (RAM).

Boot sector

The first logical sector on any DOS-formatted diskette, which contains the DOS boot program and information about the disk structure. On a hard disk the boot sector is physically preceded by the partition record.

Boot sector virus

A virus program which infects RAM after having booted (or attempted to boot) from a diskette with an infected boot sector. A write enabled disk is infected by a boot sector virus if it is accessed on a system with infected RAM.

Bug

An unintentional fault in program code.

Cluster

A grouping of one or more sectors on a DOS disk.

COM file

One of the two types of DOS executable files. COM files are limited in size to 64 kb (see EXE files).

Disk

A 3,5-inch or 5,25-inch diskette, or a hard disk drive.

DOS

Disk Operating System. The set of programs needed to boot a personal computer and allow the user to execute housekeeping routines on the computer. Either MSDOS or PCDOS could be implied.

EXE file

One of the two types of DOS executable files. EXE file size is limited by available memory only (see COM files).

FAT

The File Allocation Table, which consists of a series of disk sector addresses. Each file on a given disk is mapped by the addresses of the clusters it occupies in the FAT. All DOS disks contain two copies of its FAT.

File virus

A virus program which attaches itself to an executable file. Two types are known to exist: Direct and Indirect action file viruses.

Direct action file viruses do not become memory-resident when the infected program is executed; instead the virus will immediately attempt to infect executable files (normally on the same disk, often in the current directory).

An indirect action file virus will become memory-resident when the infected file is run, and will only attempt to infect other executable files when they are, in turn, run.

Form factor

This refers to the physical size of a disk. Two sizes of disk in use for example have 3,5-inch and 5,25-inch diameters.

Frozen

The state of a computer after some condition(s) has/have caused its useful functioning to cease.

Infection

The condition that exists after a virus program has either installed itself into memory, or copied itself onto a disk.

Multiple infection

The condition that exists when: a virus program installs itself into the memory or onto the disk of a computer already infected by that same virus program; or when a virus program installs itself into the memory or onto the disk of a computer already infected by a different virus program.

Mutation

A virus which produces fully operational copies of itself but which differs in the actual code is a mutation virus. Some viruses do this to evade scanning programs.

Network

A collection of computers connected in such a way that they can share program and/or data files.

Overlay file

A file which contains part of a program. This file is too big to fit in memory while the main file is resident, and has to be called in, or overlaid, when required.

Partition Record

An area, found only on hard disks, where information on the start and end points of up to four logically separate partitions of that hard disk is stored.

Partition Record virus

A virus which stores its own code in the area on disk normally occupied by the partition record.

Personal Computer (PC)

A single-user computer with a central processor of the Intel family, which is operating under a version of MS-DOS or PC-DOS.

PC user

A person who uses a personal computer of any description.

Sector

A portion of a track, consisting of 512 consecutive bytes.

Single User

A computer user who runs programs on a computer which is not in any way connected to any other computer.

Stamp

A date or time stamp (maintained by DOS) is that part of a file's root directory entry which indicates when that file was created or last modified.

Stealth virus

A type of virus which hides its presence from the user by, for example, not indicating a file size increase.

Trojan Horse

A computer program which appears to perform a useful function, but contains damaging routines. When run by the user, it might destroy data or do other damage to the computer system.

Virus program

Program code which has the ability to duplicate itself on disk system areas or attach itself to other files, to be activated by some condition(s), and to cause some unwanted action which could affect various parts of the computer system.

Virus hunt

A procedure executed to remove viruses from all disks in a given geographical area.

Write-enabled

A state that a disk is in which allows writing operations to that disk to take place.

Write-protected

A disk state which prohibits writing operations to that disk.

APPENDIX B - DETAIL OF VIRUSES

The virus detail below is an extract taken from the Virus Information Summary List (Hoffman, 1993). The following has been added/altered:

- The Common Name was altered in some cases, based on the investigator's perception of frequently used names in South Africa.

- Dr. Solomon's classification of the virus type was used, i.e. BSV, PRV, IAFV and DAFV.

No other information was added. No attempt was made to verify the correctness of the information extracted from the list.

Common name:	*AIRCOP.*
Other names:	None.
Type:	BSV/PRV.
Origin:	Taiwan.
Symptoms:	System halt, messages, decrease in RAM.
General:	
1.	Only infects 360-kb diskettes.
2.	Copies original boot sector to sector 719.
3.	"AIRCOP" message is displayed at random intervals.
4.	Variant displays flashing message in September.

TABLE B-1 **VIRUS DETAIL: *AIRCOP***

Common name:	*BOUNCING BALL.*
Other names:	*Ping Pong, Italian, Vera Cruz, Boot.*
Type:	BSV.
Origin:	Unknown.
Symptoms:	Small dot traversing screen at an angle.

General:

1. Infects diskettes.
2. Bouncing dot appears on screen at random intervals.
3. Reboot clears symptom.
4. Variant infects hard drives.

TABLE B-2 **VIRUS DETAIL: *BOUNCING BALL***

Common name:	*BRAIN*
Other names:	*Pakistani, Clone, Nipper.*
Type:	BSV.
Origin:	Pakistan.
Symptoms:	Extended boot time, volume label change, three contiguous bad sectors.

General:

1. Moves boot sector, marks that area bad.
2. Changes volume label to "(c) Brain".
3. Intercepts boot sector reads - some programs cannot see virus.
4. Variant does infect hard drives.

TABLE B-3 **VIRUS DETAIL: *BRAIN***

Common name:	*CASCADE.*
Other names:	*Blackjack, Falling letters, 1701, 1704.*
Type:	IAFV.
Origin:	Germany.
Symptoms:	Screen characters fall to bottom of screen, COM files grow.

General:

1. Uses encryption to avoid detection.
2. Activation of visual symptom is random.
3. Will activate on CGA or VGA monitors.
4. Increases file sizes by 1701-1704 bytes.

TABLE B-4 **VIRUS DETAIL: *CASCADE***

Common name: *DURBAN.*
Other names: *Saturday 14th.*
Type: IAFV.
Origin: South Africa.
Symptoms: File length increase, overwrites disks.
General:

1. Infects COM and EXE files.
2. File lengths will increase by 669-684 bytes.
3. On any Saturday 14th, overwrites 1st 100 sectors of C:, then B:, etc.
4. COMMAND.COM is not infected.

TABLE B-5 **VIRUS DETAIL: *DURBAN***

Common name: *EXEBUG.*
Other names: *Swiss Boot.*
Type: BSV/PRV.
Origin: Switzerland.
Symptoms: Drive C: inaccessible, decrease in RAM.
General:

1. Infects boot sector and partition record.
2. Intercepts boot sector reads - some programs cannot see virus.
3. "Invalid drive specification" message when C: is infected, booting from uninfected diskette.
4. Norton Disk Doctor can restore hard drive status.

TABLE B-6 **VIRUS DETAIL: *EXEBUG***

Common name: *FRODO.*
Other names: 4096.
Type: IAFV.
Origin: Israel.
Symptoms: File length increase, file corruption.
General:

1. COM, EXE and overlay files will grow by 4096 bytes.
2. The increase is not visible while virus is in RAM.
3. It cross-links disk files over time.
4. It will infect data files which will be corrupted after disinfection.

TABLE B-7 **VIRUS DETAIL: *FRODO***

Common name:	*JERUSALEM.*
Other names:	*PLO, Israeli, Friday 13th, 1813, Hebrew University.*
Type:	IAFV.
Origin:	Italy.
Symptoms:	File length increase, system slowdown, files deleted on Friday 13th.

General:

1. Infects many file types, increases length by 1808-1822 bytes.
2. EXE files are re-infected, size will increase each time.
3. An infected program will be deleted if executed on Friday 13th.
4. Over 40 variants exist.

TABLE B-8 **VIRUS DETAIL: *JERUSALEM***

Common name:	*MICHELANGELO.*
Other names:	None.
Type:	BSV/PRV.
Origin:	Sweden/Netherlands.
Symptoms:	Disk damage, format, decrease in RAM.

General:

1. Infects diskettes and hard drives.
2. Virus is based on Stoned virus.
3. Infection causes boot sector/partition record to be moved to another location.
4. On 6 March it will overwrite the hard disk.

TABLE B-9 **VIRUS DETAIL: *MICHELANGELO***

Common name:	*NOINT.*
Other names:	*Bloomington, LastDirSect, Stoned III.*
Type:	BSV/PRV.
Origin:	Canada.
Symptoms:	Corrupt directory, decrease in RAM.

General:

1. Infects diskettes and hard disks.
2. Infected systems take longer to boot and access disks.
3. Some anti-viral programs are mislead when attempting to read the infected partition record.
4. The directory entries of some files may be lost.

TABLE B-10 **VIRUS DETAIL: *NOINT***

Common name: *PLASTIQUE.*
Other names: *Plastic bomb, Anticad, 3012.*
Type: BSV/PRV.
Origin: Taiwan.
Symptoms: COM & EXE growth, system slowdown, bomb noises after September 20.
General:

1. COMMAND.COM is not infected.
2. Infected files grow by 3012 - 3020 bytes.
3. Infection is not always successful due to bugs in virus.
4. A number of variants exist.

TABLE B-11 **VIRUS DETAIL: *PLASTIQUE***

Common name: *PRETORIA.*
Other names: *June 16th, June.*
Type: DAFV.
Origin: South Africa.
Symptoms: COM file growth, long disk accesses.
General:

1. The virus is encrypted, and infects COM files.
2. When an infected file is executed, the virus will infect all COM files on the current drive.
3. The long access time is very obvious, especially on hard disk systems.
4. When an infected file is executed on June 16th, all entries in the root directory are changed to "ZAPPED".

TABLE B-12 **VIRUS DETAIL: *PRETORIA***

Common name: *STONED.*
Other names: *Marijuana, New Zealand, Rostov.*
Type: BSV/PRV.
Origin: New Zealand.
Symptoms: Bootup message: "Your PC is now Stoned!".
General:

1. Infects diskettes and hard disks.
2. When resident, it will infect a diskette if it is accessed.
3. The boot sector or partition record is moved to a different location.
4. Some files might lose their root directory entries when the disk is infected.

TABLE B-13 **VIRUS DETAIL: *STONED***

Common name: *SUNDAY.*
Other names: None.
Type: DAFV.
Origin: Washington.
Symptoms: COM & EXE file growth, messages.
General:

1. Activates on any Sunday, displays a message.
2. The virus code appears to be based on the Jerusalem virus.
3. Damage to a disk's FAT has been reported.
4. Three variants are known to exist.

TABLE B-14 **VIRUS DETAIL: *SUNDAY***

Common name: *TELEFONICA.*
Other names: *Telecom, Spanish Telecom-2.*
Type: IAFV.
Origin: Spain.
Symptoms: COM file growth, decrease in RAM, hard disk formatted.
General:

1. Infects COM files larger than 1 kb, and partition records.
2. File length increases are hidden from some programs.
3. The activation mechanism is contained in the partition record infector.
4. After 400 boots from an infected disk, the hard drives will be overwritten.

TABLE B-15 **VIRUS DETAIL: *TELEFONICA***

APPENDIX C - DISK LAYOUT DATA

		360-kb 5,25 Inch Diskette	1,44-Mb 3,5 Inch Diskette	32-Mb Hard Drive
Par.rec.:	Side			0
	Cyl.	Not	Not	0
	Sect.	present	present	1
	Space(kb)			0,5
Boot sec.:	Side	0	0	1
	Cyl.	0	0	0
	Sect.	1	1	1
	Space(kb)	0,5	0,5	0,5
FAT 1:	Sect.	1-2	1-9	1-63
	Space(kb)	1	4,5	31,5
FAT 2:	Sect.	3-4	10-18	64-126
	Space(kb)	1	4,5	31,5
Root Dir.:	Sect.	5-11	19-32	127-158
	Space(kb)	3,5	7	15,5
Data area:	Sect.	12-719	33-2879	159-63829
	Space(kb)	354	1423,5	31835,5
Number of:	Sides	2	2	4
	Cylinders	40	80	614
	Sect./clust.	2	1	4
	Sect./track	9	18	26
	Clusters	360	2880	15917
	Sectors	720	2880	63830
	Bytes	368640	1474560	32694272

TABLE C-1 **LAYOUT OF USER MASTER DISKS**

CONTENTS OF USER MASTER DISKS

DISK 1

```
 Volume in drive A has no label
 Volume Serial Number is 1349-18EE
 Directory of A:\

CHKDSK   EXE     16200 04-09-91   5:00a
COMMAND  COM     47845 04-09-91   5:00a
DISKCOPY COM     11793 04-09-91   5:00a
FORMAT   COM     32911 04-09-91   5:00a
TREE     COM      6901 04-09-91   5:00a
        5 file(s)     115650 bytes
                      173056 bytes free
```

DISK 2

```
 Volume in drive A has no label
 Volume Serial Number is 1F50-18E4
 Directory of A:\

ABBRIEVE DAT      1536 03-16-92  12:00p
ACCOUNTS DAT      9216 03-16-92  12:00p
BACKORDR DAT      2048 03-16-92  12:00p
BALANCE  REP      4352 03-16-92  12:00p
BATCH4   DB1        94 08-23-93  10:58a
CUSTLIST DBF     72294 06-14-93  12:04p
CUSTLIST DBT       513 07-30-92   2:22p
CUSTLIST LBL      1034 07-30-92   2:12p
CUSTLIST QRY       103 07-30-92  10:49a
FILEMAN  EXE     12416 09-23-93   1:34p
FILEMAN  PAS     11808 01-02-80  10:43p
GOODS    DAT      1536 03-16-92  12:00p
GROUPS   DAT       108 03-16-92  12:00p
GSTUD92  WK1     58021 10-12-92  12:59p
INCOME   REP      2725 03-16-92  12:00p
INVLINK  DAT      2048 03-16-92  12:00p
INVOICE  DAT      1536 03-16-92  12:00p
NEW      REP        33 03-16-92  12:00p
OPENLINK DAT      2560 03-16-92  12:00p
REPOP    DAT      2940 08-23-93  11:10a
REPORT02 DOC     24868 09-27-93   3:03p
SALESREP CBL      4659 07-16-92   2:03p
SALESREP COB      2816 09-27-93   3:08p
SALESREP LST      7778 01-01-80  12:21a
STOCK    DAT      2560 03-16-92  12:00p
STOCKTRN DAT      2048 03-16-92  12:00p
SYSVARS  DAT      1961 09-27-93   2:24p
TRANSACT DAT      3072 03-16-92  12:00p
USER     B         659 08-23-93  10:58a
       29 file(s)     237342 bytes
                      111616 bytes free
```

DISK 3

```
 Volume in drive B has no label
 Volume Serial Number is 3F3F-1C02
 Directory of B:\

RMCOBOL  EXE     98528 02-09-87   6:27a
RMCOBOL  OVY     65280 01-05-87  12:37p
RUNCOBOL EXE    125952 02-09-87   6:27a
SALECP1  DAT        64 07-16-92  12:49p
SALESREP CBL      4659 07-16-92   2:03p
SALESREP COB      2816 09-27-93   4:22p
SALESREP LST      7778 01-01-80  12:21a
        7 file(s)     305077 bytes
                     1150464 bytes free
```

DISK 4

```
 Volume in drive B has no label
 Volume Serial Number is 3F5B-1202
 Directory of B:\

ASSIST   HLP     17642 02-27-87  10:53a
CHKLIST  MS        81 06-10-93   2:52p
CUSTLIST DBF     72294 06-14-93  12:04p
CUSTLIST DBT       513 07-30-92   2:22p
CUSTLIST LBL      1034 07-30-92   2:12p
CUSTLIST QRY       103 07-30-92  10:49a
D        BAT        59 06-01-92   8:47p
DBASE    EXE    133632 05-26-92   6:41p
DBASE    MSG     12420 05-26-92   6:41p
DBASE    OVL    266240 02-27-87  10:53a
DBASEINL OVL     27648 02-27-87  10:53a
HELP     DBS     66560 02-27-87  10:53a
       12 file(s)     598226 bytes
                      856064 bytes free
```

DISK 5

```
 Volume in drive B has no label
 Volume Serial Number is 1442-1203
 Directory of B:\

123      CMP    138681 08-20-89  12:00a
123      CNF       376 08-20-89  12:00a
123      DLD      5148 08-20-89  12:00a
123      EXE     15392 08-20-89  12:00a
123      RI      36321 08-20-89  12:00a
123      SET     43445 02-16-93  10:14a
EX800    APD      7697 08-20-89  12:00a
GSTUD92  WK1     58021 10-12-92  12:59p
HERCULES ASD      3469 08-20-89  12:00a
INIT     CNF     19912 08-20-89  12:00a
INIT     RI      62158 08-20-89  12:00a
LICENSE  000         1 08-20-89  12:00a
LOTUS    COM      5631 08-20-89  12:00a
LOTUS    FNT      8686 08-20-89  12:00a
UTIL     SET     10074 08-20-89  12:00a
       15 file(s)     415012 bytes
                     1039360 bytes free
```

DISK 6

```
 Volume in drive B has no label
 Volume Serial Number is 3A15-1BFC
 Directory of B:\

FILEMAN  EXE     12416 09-23-93   1:34p
FILEMAN  PAS     11808 01-02-80  10:43p
TURBO    DSK       606 02-11-93   1:10p
TURBO    EXE    403655 03-09-93  10:02a
TURBO    ICO       766 10-30-92   7:00a
TURBO    TP       4048 02-11-93   1:10p
TURBO    TPH    700786 10-30-92   7:00a
TURBO    TPL     48432 10-30-92   7:00a
        8 file(s)    1182517 bytes
                      272896 bytes free
```

DISK 7 (ROOT)

```
 Volume in drive B has no label
 Volume Serial Number is 3E1F-16D9
 Directory of B:\

ACCLIST  SCR       247 03-16-92  12:00p
ACCMOVE  SCR       300 03-16-92  12:00p
ACCOUNTS SCR      1307 03-16-92  12:00p
ACTIVITY SCR       175 03-16-92  12:00p
AGE      SCR       929 03-16-92  12:00p
BACKORD  SCR       166 03-16-92  12:00p
BACKORDR SCR       206 03-16-92  12:00p
BATCH    SCR       829 03-16-92  12:00p
BATCHTYP SCR       311 03-16-92  12:00p
BATTYPE  SCR        75 03-16-92  12:00p
BETA     EXE    673936 01-27-93  10:32a
BTRIEVE  EXE     42524 03-16-92  12:00p
BUDGETS  SCR       754 03-16-92  12:00p
CASHTAX  SCR       216 03-16-92  12:00p
CLEAN    BAT       578 03-16-92  12:00p
CREDBAT  SCR       124 03-16-92  12:00p
CREDLIST SCR       172 03-16-92  12:00p
CREDNOTE SCR       316 03-16-92  12:00p
DATES    SCR      1654 03-16-92  12:00p
DISKDRV  SCR        71 03-16-92  12:00p
DLEDGER  SCR       473 03-16-92  12:00p
DRCRLIST SCR       247 03-16-92  12:00p
DRCRMOVE SCR       252 03-16-92  12:00p
EGAVGA   BGI      5554 03-16-92  12:00p
GLOBREC  SCR       107 03-16-92  12:00p
GROUPS   SCR        74 03-16-92  12:00p
GRV      SCR       313 03-16-92  12:00p
GRVBAT   SCR       127 03-16-92  12:00p
GRVHEAD  SCR       410 03-16-92  12:00p
GRVLIST  SCR       179 03-16-92  12:00p
HERC     BGI      6204 03-16-92  12:00p
```

```
INVBAT   SCR        126 03-16-92   12:00p
INVHEAD  SCR        620 03-16-92   12:00p
INVLIST  SCR        177 03-16-92   12:00p
INVOICE  SCR        348 03-16-92   12:00p
LABELOP  SCR        246 03-16-92   12:00p
LABELS   SCR        745 03-16-92   12:00p
MENU     SCR       2431 03-16-92   12:00p
MESSAGE  SCR        130 03-16-92   12:00p
OPENITEM SCR        300 03-16-92   12:00p
PRINTER  DAT       3878 03-16-92   12:00p
PRINTER  SCR        950 03-16-92   12:00p
REALLOC  SCR        250 03-16-92   12:00p
RECONCIL SCR        173 03-16-92   12:00p
RECONTRN SCR        237 03-16-92   12:00p
REPORT   SCR       1239 03-16-92   12:00p
RETBAT   SCR        122 03-16-92   12:00p
RETLIST  SCR        177 03-16-92   12:00p
SALESINV SCR        184 03-16-92   12:00p
SALESPER SCR         66 03-16-92   12:00p
STATMENT SCR        864 03-16-92   12:00p
STOCK    SCR        633 03-16-92   12:00p
STOCKLST SCR        380 03-16-92   12:00p
STOCKMOV SCR        284 03-16-92   12:00p
SUPPORT  SCR         88 03-16-92   12:00p
SYSACC   SCR        171 03-16-92   12:00p
SYSINV   SCR        861 03-16-92   12:00p
SYSTEM   SCR        441 03-16-92   12:00p
TAXREP   SCR        250 03-16-92   12:00p
TC       BAT        355 03-16-92   12:00p
TOGGLE   SCR       1009 03-16-92   12:00p
TRANSACC SCR        121 03-16-92   12:00p
TRIALBAL SCR        348 03-16-92   12:00p
TRIP     CHR      16677 03-16-92   12:00p
UNITS    SCR         70 03-16-92   12:00p
USER     SCR        474 03-16-92   12:00p
BTRIEVE  TMP          0 01-27-93   10:30a
FUTURE       <DIR>      09-27-93    3:19p
       68 file(s)     774255 bytes
                      620544 bytes free
```

DISK 7 *(FUTURE SUBDIRECTORY)*

```
 Volume in drive B has no label
 Volume Serial Number is 3E1F-16D9
 Directory of B:\FUTURE

.            <DIR>      09-27-93    3:19p
..           <DIR>      09-27-93    3:19p
ABBRIEVE DAT       1536 03-16-92   12:00p
ACCOUNTS DAT       9216 03-16-92   12:00p
BACKORDR DAT       2048 03-16-92   12:00p
BALANCE  REP       4352 03-16-92   12:00p
GOODS    DAT       1536 03-16-92   12:00p
GROUPS   DAT        108 03-16-92   12:00p
INCOME   REP       2725 03-16-92   12:00p
INVLINK  DAT       2048 03-16-92   12:00p
INVOICE  DAT       1536 03-16-92   12:00p
NEW      REP         33 03-16-92   12:00p
```

```
OPENLINK DAT       2560 03-16-92  12:00p
REPOP    DAT       2940 08-23-93  11:10a
STOCK    DAT       2560 03-16-92  12:00p
STOCKTRN DAT       2048 03-16-92  12:00p
SYSVARS  DAT       1961 09-27-93   2:24p
TRANSACT DAT       3072 03-16-92  12:00p
USER     _B         659 08-23-93  10:58a
BATCH4   DB1         94 08-23-93  10:58a
       20 file(s)      41032 bytes
                     620544 bytes free
```

DISK 8

```
 Volume in drive B has no label
 Volume Serial Number is 4279-15CF
 Directory of B:\

WPHELP   FIL     217056 12-12-91   4:06p
WP       EXE     228864 12-12-91   4:06p
WP{WP}UK LCN        16 08-10-92   9:22a
KEYS     MRS       4800 12-12-91   4:06p
STANDARD IRS       4868 12-12-91   4:06p
STANDARD PRS       1942 12-12-91   4:06p
EPLX800  PRS       7821 09-02-92   4:54p
STANDARD VRS      30544 12-12-91   4:06p
WP       FIL     617619 12-12-91   4:06p
WP       MRS       6072 12-12-91   4:06p
WP       QRS      17034 12-12-91   4:06p
WP{WP}   SET       1880 08-10-92   9:51a
REPORT02 DOC       7722 09-29-93   4:17a
       13 file(s)    1146238 bytes
                      308224 bytes free
```

DISK 9

```
Directory PATH listing
Volume Serial Number is 2C55-1203
C:.
|    COMMAND.COM
|    CONFIG.SYS
|    Z.BAT
|    IPXNE2.COM
|    NETX.EXE
|    NOVELL.BAT
|    A.BAT
|    AUTOEXEC.BAT
|    C.BAT
|    CONFIG.B00
|    D.BAT
|    DD.BAT
|    DD.FIL
|    E.BAT
|    F.BAT
|    G.BAT
|    I.BAT
|    L.BAT
```

```
    LT.BAT
    M.BAT
    MEM.HI
    MEM.LO
    MENU.DOC
    N.BAT
    O.BAT
    P.BAT
    Q.BAT
    R.BAT
    RR.BAT
    S.BAT
    SEEW.BAT
    T.BAT
    TREE.FIL
    TREE-F.FIL
    U.BAT
    V.BAT
    W.BAT
    X.BAT
    IPXNE.COM
    IPXSM.COM
    NET.BAT
    NETNE2.BAT
    NETNE.BAT
    NETSM.BAT
    NETWORK.TXT
    WP.BAT
    CO.BAT
    PA.BAT
    TC.BAT
    B
    DISK9.WPS

---TRAKKER
        TAPE.EXE
        TAPE.TXT
        AUTOBACK.COM
        CONFIG.EXE
        TAPE.CFG
        ERROR.LOG

---DBASE
        ASSIST.HLP
        CHKLIST.MS
        D.BAT
        DBASE.EXE
        DBASE.MSG
        DBASE.OVL
        DBASEINL.OVL
        CUSTLIST.DBF
        CUSTLIST.DBT
        CUSTLIST.LBL
        CUSTLIST.QRY
        CUSTLIST.TBK
        HELP.DBS
        NDX1.NDX
        NDX2.NDX
```

```
|       NDX3.NDX
|       REPORT.FRM
|
|---DOS
|       COMMAND.COM
|       4201.CPI
|       4208.CPI
|       5202.CPI
|       8C00DOSC.BAT
|       ANSI.SYS
|       APPEND.EXE
|       APPNOTES.TXT
|       ASSIGN.COM
|       ATTRIB.EXE
|       BACKUP.EXE
|       CHKDSK.EXE
|       COMP.EXE
|       COUNTRY.SYS
|       DEBUG.EXE
|       DISKCOMP.COM
|       DISKCOPY.COM
|       DISPLAY.SYS
|       DOSHELP.BAK
|       DOSKEY.COM
|       DOSSHELL.COM
|       DOSSHELL.EXE
|       DOSSHELL.GRB
|       DOSSHELL.HLP
|       DOSSHELL.INI
|       DOSSHELL.SWP
|       DOSSHELL.VID
|       DOSSWAP.EXE
|       DRIVER.SYS
|       E.BAT
|       EDIT.COM
|       EDIT.HLP
|       EDLIN.EXE
|       EGA.CPI
|       EGA.SYS
|       EMM386.EXE
|       EXE2BIN.EXE
|       EXPAND.EXE
|       FASTOPEN.EXE
|       FC.EXE
|       FDISK.EXE
|       FIND.EXE
|       FORMAT.COM
|       GORILLA.BAS
|       GRAFTABL.COM
|       GRAPHICS.COM
|       GRAPHICS.PRO
|       HELP.EXE
|       HIMEM.SYS
|       JOIN.EXE
|       KEYB.COM
|       KEYBOARD.SYS
|       LABEL.EXE
|       LCD.CPI
```

```
        LOADFIX.COM
        MEM.EXE
        MIRROR.COM
        MODE.COM
        MONEY.BAS
        MONEY.DAT
        MORE.COM
        MSHERC.COM
        NIBBLES.BAS
        NLSFUNC.EXE
        PACKING.LST
        PRINT.EXE
        PRINTER.SYS
        QBASIC.EXE
        QBASIC.HLP
        QBASIC.INI
        RAMDRIVE.SYS
        README.TXT
        RECOVER.EXE
        REMLINE.BAS
        REPLACE.EXE
        RESTORE.EXE
        SETVER.EXE
        SHARE.EXE
        SMARTDRV.SYS
        SORT.EXE
        SUBST.EXE
        SYS.COM
        TREE.COM
        UNDELETE.EXE
        UNFORMAT.COM
        XCOPY.EXE
        DOSHELP.HLP
        YMPMFM.BAS

---LOT
        123.CMP
        123.CNF
        123.DLD
        123.DYN
        123.EXE
        123.HLP
        123.RI
        123.SET
        BLOCK1.FNT
        BLOCK2.FNT
        BOLD.FNT
        CGA.ASD
        CHKLIST.MS
        COUR.AFL
        DBF2.XLT
        DBF3.XLT
        DEL_MGR.EXE
        DIF.XLT
        EGACOLOR.ASD
        EGAMONO.ASD
        EX800.APD
        FONTSET.CNF
```

```
FORUM.FNT
FX80.APD
FX85.APD
FX850.APD
FX86E.APD
HERCULES.ASD
HPDJ.APC
HPDJ.APD
HPDJ.APF
HPLJ.APC
HPLJ.APD
HPLJ.APF
HPLJE.APD
HPLJII.APC
HPLJII.APD
HPLJIID.APC
HPLJIID.APD
HPLJP.APC
HPLJP.APD
HPLJPX.APD
IBMGRAPH.APD
IBMPP.APD
IBMPP.APF
IBMPRO.APD
INIT.CNF
INIT.RI
INSTALL.DVC
INSTALL.EXE
INSTALL.LBR
INSTALL.SCR
ITALIC1.FNT
ITALIC2.FNT
LICENSE.000
LOTUS.COM
LOTUS.FNT
MACROMGR.ADN
PGRAPH.CNF
PGRAPH.EXE
PGRAPH.HLP
PICA.AFL
PSCRIPT.API
ROMAN1.FNT
ROMAN2.FNT
SCRIPT1.FNT
SCRIPT2.FNT
SINGLE.LBR
SYLK.XLT
TIMES.AFL
TRANS.COM
TRIUM.AFL
UTIL.SET
VCWRK.XLT
VGACOLOR.ASD
VGAMONO.ASD
WR1WKS.XLT
WR1WRK.XLT
WRKWR1.XLT
ZAP.EXE
```

```
        GSTUD92.WK1
        GSWLECTU.ALL
        GSWLECTU.DOC
        GSWLECTU.WK1

---NUT
        READ.ME
        NORTON.OVL
        NORTON.EXE
        NORTON.INI
        NUCONFIG.OVL
        NDD.EXE
        UNFORMAT.EXE
        DISKTOOL.EXE
        CALIBRAT.EXE
        UNERASE.EXE
        FILEFIX.EXE
        SFORMAT.EXE
        IMAGE.EXE
        SYSINFO.EXE
        NCC.EXE
        SPEEDISK.EXE
        NCACHE.EXE
        DS.EXE
        BE.EXE
        DISKEDIT.EXE
        FILEFIND.EXE
        LP.EXE
        DISKMON.EXE
        NU.HLP
        TROUBLE.HLP
        EP.EXE
        TS.EXE
        NUCONFIG.EXE
        FA.EXE
        FD.EXE
        FL.EXE
        FS.EXE
        NCD.EXE
        WIPEINFO.EXE
        DISKEDIT.ICO
        DISKREET.ICO
        FILEFIND.ICO
        FILEFIX.ICO
        NCD.ICO
        NDD.ICO
        NDOS.ICO
        NORTON.ICO
        PETER.ICO
        SFORMAT.ICO
        SYSINFO.ICO
        NORTON.CMD

---PCT
        ASCII.OVL
        B.BAT
        BACKTALK.EXE
        BINARY.VWR
```

CALC.OVL
CALC.TMP
CHKLIST.MS
CIS.SCR
COMPRESS.CFG
COMPRESS.EXE
COMPRESS.HLP
CPS.SCR
D.BAT
DESKTOP.CFG
DESKTOP.EXE
DESKTOP.IMG
DESKTOP.OVL
DESKTOP.THM
DISKFIX.EXE
DSKERR.DBF
EPSON.PRO
ESL.SCR
FINCALC.OVL
FORMAT.BAT
HEXCALC.OVL
HOTKEY.OVL
HPLJF.PRO
INKILL.OVL
ITLFAX.EXE
KILL.EXE
LETTER.FOR
MACROS.OVL
MCI.SCR
MENU.DOC
MI.COM
MIRROR.COM
OLDSHELL.CFG
PANA.PRO
PARK.COM
PCFORMAT.COM
PCRUN.COM
PCSECURE.HLP
PCSETUP.CFG
PCSHELL.CFG
PCSHELL.EXE
PCSHELL.HLP
PCSHELL.IMG
PCSHELL.OVL
PCSHELL.THM
PCSHELLF.TRE
PCSHELLP.TRE
PCSHELLQ.TRE
PCSHELLR.TRE
PCSHELLS.TRE
PCSHELLT.TRE
PCSHELLU.TRE
PCSHELLV.TRE
PCSHELLW.TRE
PCSHELLX.TRE
PCSHELLY.TRE
PCSHELLZ.TRE
PCTOOLS.PCX

```
        PHONE.TEL
        PROPTR.PRO
        README.TXT
        REBUILD.COM
        RECOLOR.OVL
        S.BAT
        SCICALC.OVL
        SCICALC.TMP
        TELECOM.DBF
        TELECOM.FOR
        TEXT.VWR
        TIME.OVL
        UNDELETE.EXE
        WORD.VWR
        WORK.PRO
        X.BAT

---PROG
        CHKLIST.MS
        HELP.EXE
        TECH.H!

---TEMP
        VSUMX309.ZIP
        PKUNZIP.EXE
        VSUM.EXE
        VSUMX.XDB
        VSUM_REG.DOC
        READ_ME.1ST
        VALIDATE.COM
        VALIDATE.DOC

---VIR
    ---SOL
            AUTHOR.COM
            CERT.EXE
            CERTIFY.COM
            DEFERBAT.COM
            DEFERKEY.COM
            DEFINKEY.COM
            EXTRA.DRV
            FINDVIRU.EXE
            FRIDAY.BAT
            FV.BAT
            GUARD.DRV
            GUARD.SYS
            GUARDMEM.COM
            MEM.DRV
            NOFLOPPY.COM
            NOHARD.COM
            QFVE.DRV
            README.DOC
            RESCUE.BAT
            RESCUE.INF
            TKUTIL.EXE
            TOOLKIT.EXE
            TOOLKIT.HLP
            TOOLKIT.INI
```

```
            TOOLKIT.SYS
            VGPOPUP.EXE
            VIRDATA.DAT
            VIV1.BAT
            VIV2.BAT
            VIVERIFY.EXE
            GUARD.COM

---WORKS3
        COMM.SCD
        EPL6000.PRD
        EPLX800.PRD
        EPSONFX.PRD
        EPSONLQ2.PRD
        HP3.INI
        HP3.PRD
        HPDJ.PRD
        HPLASER.INI
        HPLASER.PRD
        IBMGRAPH.PRD
        IBMPRO.PRD
        INTL.RSC
        LQ2500.PRD
        MACROS.INI
        MAIN.DIC
        PANA11.PRD
        PRINTERS.INI
        SCREEN.VID
        SPELL.OVL
        W.BAT
        WORKS.CAL
        WORKS.EXE
        WORKS.HLP
        WORKS.INI
        WORKS.OVL
        WORKS.PIF
        LEDE.WDB
        GSS2-93.WKS
        3-MASTED.PCX
        ALPSCENE.PCX
        ALRMCLCK.PCX
        APSE.PCX
        BARN.PCX
        BOXGLOVE.PCX
        BUILDING.PCX
        BUTTRFLY.PCX
        CASTLE.PCX
        CLIFF.PCX
        CLOCK.PCX
        CROPS.PCX
        CROWN.PCX
        DARTS.PCX
        DCA_RTF.EXE
        DICE.PCX
        DRINKS.PCX
        F001.SFT
        F00225.RFT
        F00230.RFT
```

F00235.RFT
F017.SFT
F033.SFT
F04003.RFT
F04004.RFT
F04005.RFT
F04006.RFT
F04830.RFT
TEMP.WKS
TEMPLATE.7
TEMPLATE.6
TEMPLATE.4
TEMPLATE.0
TEMPLATE.19
TEMPLATE.11
TEMPLATE.16
TEMPLATE.3
TEMPLATE.2
TEMPLATE.13
TEMPLATE.18
TEMPLATE.8
TEMPLATE.9
TEMPLATE.17
TEMPLATE.5
TEMPLATE.10
TEMPLATE.14
TEMPLATE.12
TEMPLATE.15
TEMPLATE.1
TEMP.WPS
SUN.PCX
TELEPHNE.PCX
THESAUR.OVL
THESAUR.LEX
WATERFAL.PCX
WELL.PCX
WHEAT.PCX
WORD_RTF.EXE
F04837.RFT
F04843.RFT
F06625.RFT
F06630.RFT
F06635.RFT
F081.SFT
F129.SFT
F13025.RFT
F13030.RFT
F13035.RFT
F145.SFT
F209.SFT
FISH.PCX
FISHES.PCX
GEARS.PCX
HELP.OVL
HELPWANT.PCX
HIGHWAY2.PCX
HNDSHAKE.PCX
HRGLASS.PCX

```
        KERMIT.FTD
        KEY.PCX
        LEARN.EXE
        LEARN.PIF
        LGHTBULB.PCX
        LITHOUSE.PCX
        MELON.PCX
        MONEY.PCX
        MONEYBAG.PCX
        MOUNTAIN.PCX
        NETWORKS.TXT
        NEWDAY.PCX
        NEWENGLD.PCX
        NYCITYSL.PCX
        PALMTREE.PCX
        PEOPLE.PCX
        PIANO.PCX
        PITCHER.PCX
        PUDDLE.PCX
        RAINIER.PCX
        RAINIERN.PCX
        RAINMAN.PCX
        RAYS.PCX
        RIBBON.PCX
        ROADBLOK.PCX
        ROADTO.PCX
        RTF_WP5.EXE
        RUINS.PCX
        RURAL.PCX
        SOBER.PCX
        STORMSEA.PCX
        WORKSFOU.SOB
        WORKSFOU.CTX
        WORKSFOU.SCN
        WORKSONE.SCN
        WORKSONE.SOB
        WORKSONE.CTX
        WORKSTHR.SCN
        WORKSTHR.SOB
        WORKSTHR.CTX
        WORKSTWO.SCN
        WORKSTWO.SOB
        WORKSTWO.CTX
        WORKSWIZ.OVL
        WORK_RTF.EXE
        WORLDBIG.PCX
        WP5_RTF.EXE
        XMODEM.FTD
        YMODEM.FTD
        ZMODEM.FTD
        RFORM.WPS
        GWSSS393.WPS
        PERSONAL.DIC
        RTHCH3.WPS

---COBOL
        RMCOBOL.EXE
        RUNCOBOL.EXE
```

```
        RMCOBOL.OVY
        SALESREP.COB
        SALESREP.CBL
        SALESREP.LST
        RITBUG.CBL
        RITBUG.COB
        SALECP1.DAT

---PASCAL
        TURBO.DSK
        FILEMAN.EXE
        TURBO.ICO
        TURBO.TP
        TURBO.TPH
        TURBO.TPL
        FILEMAN.BAK
        TURBO.EXE
        FILEMAN.PAS

---TCASH
    |   ACCLIST.SCR
    |   ACCMOVE.SCR
    |   ACCOUNTS.SCR
    |   ACTIVITY.SCR
    |   AGE.SCR
    |   BACKORD.SCR
    |   BACKORDR.SCR
    |   BATCH.SCR
    |   BATCHTYP.SCR
    |   BATTYPE.SCR
    |   BETA.EXE
    |   BTRIEVE.EXE
    |   BUDGETS.SCR
    |   CASHTAX.SCR
    |   CLEAN.BAT
    |   CREDBAT.SCR
    |   CREDLIST.SCR
    |   CREDNOTE.SCR
    |   DATES.SCR
    |   DISKDRV.SCR
    |   DLEDGER.SCR
    |   DRCRLIST.SCR
    |   DRCRMOVE.SCR
    |   EGAVGA.BGI
    |   GLOBREC.SCR
    |   GROUPS.SCR
    |   GRV.SCR
    |   GRVBAT.SCR
    |   GRVHEAD.SCR
    |   GRVLIST.SCR
    |   HERC.BGI
    |   INVBAT.SCR
    |   INVHEAD.SCR
    |   INVLIST.SCR
    |   INVOICE.SCR
```

```
|   |   MESSAGE.SCR
|   |   OPENITEM.SCR
|   |   PRINTER.DAT
|   |   PRINTER.SCR
|   |   REALLOC.SCR
|   |   RECONCIL.SCR
|   |   RECONTRN.SCR
|   |   REPORT.SCR
|   |   RETBAT.SCR
|   |   RETLIST.SCR
|   |   SALESINV.SCR
|   |   SALESPER.SCR
|   |   STATMENT.SCR
|   |   STOCK.SCR
|   |   STOCKLST.SCR
|   |   STOCKMOV.SCR
|   |   SUPPORT.SCR
|   |   SYSACC.SCR
|   |   SYSINV.SCR
|   |   SYSTEM.SCR
|   |   TAXREP.SCR
|   |   TC.BAT
|   |   TOGGLE.SCR
|   |   TRANSACC.SCR
|   |   TRIALBAL.SCR
|   |   TRIP.CHR
|   |   UNITS.SCR
|   |   USER.SCR
|   |   BTRIEVE.TMP
|   |
|   |---FUTURE
|   |       ABBRIEVE.DAT
|   |       ACCOUNTS.DAT
|   |       BACKORDR.DAT
|   |       BALANCE.REP
|   |       GOODS.DAT
|   |       GROUPS.DAT
|   |       INCOME.REP
|   |       INVLINK.DAT
|   |       INVOICE.DAT
|   |       NEW.REP
|   |       OPENLINK.DAT
|   |       REPOP.DAT
|   |       STOCK.DAT
|   |       STOCKTRN.DAT
|   |       SYSVARS.DAT
|   |       TRANSACT.DAT
|   |       USER._B
|   |       BATCH4.DB1
|
|---WPF
|       WPHELP.FIL
|       WP.EXE
|       WP{WP}UK.LCN
|       KEYS.MRS
|       STANDARD.IRS
|       STANDARD.PRS
|       EPLX800.PRS
```

```
|       STANDARD.VRS
|       WP.FIL
|       WP.MRS
|       WP.QRS
|       WP{WP}.SET
|       WP{WP}UK.LEX
|       WP{WP}AF.LEX
|       WP{WP}.SPW
|       WPDM3.ALL
|       WP51.INS
|       REPORT02.DOC
|
|---HOFFMAN
|       VSUMX309.ZIP
|       PKUNZIP.EXE
|       VSUM.EXE
|       VSUMX.XDB
|       VSUM_REG.DOC
|       READ_ME.1ST
|       VALIDATE.COM
|       VALIDATE.DOC
```

APPENDIX D

Attached is a copy of the questionnaire used to determine the status of computer virus infections in the South African industry.

Cape
Kaapse
Technikon

P.O. Box 652, Cape Town 8000
Posbus 652, Kaapstad 8000

Longmarket Street Cape Town 8001
Langmarkstraat Kaapstad 8001
Telegrams . TECCOM . Telegramme
Telex . 5-21666 . Teleks
Telefax (021) 461-7564
Tel.: 461-6220 Main
Tel.: 460-3911 Zonnebloem

Ref./Verw.

23 July 1992

Dear Sir/Madam,

At present I am employed as a Senior Lecturer in various computer subjects at the School of Business Informatics. I am currently busy with the last part of my research into computer viruses towards obtaining a Master's Diploma in Computer Data Processing at the Cape Technikon.

This research is aimed at assisting the industry in correctly evaluating the computer virus threat. It would thus be appreciated if you could complete the enclosed questionnaire, or have it done by an employee who, in your opinion, is best suited for the task. Kindly return it in the enclosed, stamped envelope before 15 August 1992.

In the questionnaire you have the option to indicate whether or not you would like to receive various information sheets on computer viruses. Upon completion of the processing of the data, this will be sent to you.

It is hereby guaranteed that none of the following information will be listed in the thesis, in the sheets mentioned above, or made known to any person except myself and my study leader:

- Company name or address.
- Any detail which could uniquely identify a company.
- Any information which could lead to the identification of the individuals who received or completed the questionnaire.

Your co-operation would be greatly appreciated in this matter.

Kind regards,

Mr. M. Weideman

QUESTIONNAIRE:

COMPUTER VIRUSES

OBJECTIVE

The objective of this questionnaire is to determine whether or not computer viruses have caused damage to stored information in the computer industry.

CONFIDENTIALITY

No company- or person-specific information from the returned questionnaires will be made available to any person or organization except the researcher and his internal study leader.

THESIS TITLE

A critical evaluation of the destructive impact of computer viruses on files stored by personal computer users.

A. COMPUTER VIRUS INFORMATION

If you return the completed questionnaire, you may indicate below on which topics you require more information. This information will be sent to you once all the received data has been processed.

Please tick the relevant boxes.

☐ Statistical summary of the results of this survey

☐ Information on anti-virus programs

☐ List of viruses known to be in the country

☐ Hints on preventing viral infections

If you have ticked any one or more boxes above, kindly enclose a stamped, self addressed envelope with this questionnaire.

B. BIOGRAPHICAL DETAILS

Please fill in the detail below. You are again reminded of the confidentiality of this information. The researcher only needs to know the name of the company so as to control the questionnaires sent out and received back.

The term "respondent" refers to the person actually completing the questionnaire.

1. Date: _____

2. Name of respondent: _____

3. Job description of respondent: _____
(eg. Programmer, Analyst, Director, PC support, Consultant, etc.)

_____

4. Name of Company: _____

5. Approximate number of employees in company: _____

Please address any queries to:

Mr M. Weideman
P.O. Box 3109
Tygerpark
7536

Tel: 021 - 913 5515 (h)
021 - 460 3281/31 (o)

Fax: 021 - 461 4930

C. COMPANY PROFILE

1. **What type of business is your company involved in ? Put a tick in any one or more of the boxes below. You could also add more detail under Other.**

☐ Banking	☐ Building	☐ Clothing
☐ Computers/related	☐ Education	☐ Energy
☐ Entertainment	☐ Farming/related	☐ Food/Liquor
☐ Government	☐ Insurance	☐ Medical
☐ Mining	☐ Municipal	☐ Research
☐ Sales		

Other: _____

_____

_____

2. **Please indicate the number of personal computers being used in your company, by putting a tick in the relevant box below. The term "personal computer", as used in this questionnaire, refers to a microcomputer based on any one of the following microprocessors: 8088/8086, 80286, 80386, 80486 and derivatives.**

0	1 - 10	11 - 100	101 +

If you have put a tick in the 0 box for question 2 above, kindly ignore the remainder of the questionnaire, and return it in the enclosed envelope.

3. **Is a version of PCDOS or MSDOS being used as operating system on any one of these personal computers ?**

YES	COMMENTS
NO	
UNSURE	

If you have answered NO or UNSURE to question 3 above, kindly ignore the remainder of the questionnaire, and return it in the enclosed envelope.

4. **What are the personal computers in your company being used for ? Put a tick in any one or more of the boxes below. You could also add more detail under Other.**

☐ Accounting ☐ Design ☐ Program development

☐ Research ☐ Training ☐ Packaged software

Other: _____

_____

5. **Does more than one person use any one personal computer during a typical working day ?**

YES	COMMENTS
NO	
UNSURE	

D. VIRUS INFECTIONS

6. How many personal computers in your company have had a computer virus infection that you are aware of ?

0	UNSURE	COMMENTS
1		
MORE THAN 1		

If you have put a tick in the 0 or UNSURE box for question 6 above, kindly ignore the remainder of the questionnaire, and return it in the enclosed envelope.

7. How do you know that (an) infection(s) did actually take place ?

☐ An anti-viral program identified the infection. (If so,tick here and name the program under Other below.)

☐ Some known virus symptom(s) appeared. (If so, tick here and describe the symptom(s) under Other below.)

☐ I lost some data. (If so, tick here and describe how you determined that you have lost data).

☐ Strange characters appeared on the screen. (If so,tick here and describe what the screen looked like under Other below.)

☐ Something happened on the computer that has never happened before. (If so, tick here and describe what happened under Other below).

☐ Unknown.

Other: _____

_____

_____

8. **Who detected the infection(s) ?**

- [ ] The respondent.
- [ ] A technical support person.
- [ ] Unknown.

Other: _____

_____

_____

9. **Which virus(es) caused the infection(s) ?**

- [ ] Agiplan
- [ ] Aids
- [ ] Aircop
- [ ] Anarcia
- [ ] Bouncing Ball
- [ ] Brain
- [ ] Cascade
- [ ] Frodo
- [ ] Dark Avenger
- [ ] Durban
- [ ] Jerusalem
- [ ] Michelangelo
- [ ] Ogre
- [ ] Plastique
- [ ] Pretoria
- [ ] Stoned
- [ ] Sunday
- [ ] Telefonica
- [ ] Vienna
- [ ] Void
- [ ] Yankee Doodle
- [ ] Unknown

Other: _____

_____

_____

10. **How was the infection(s) removed ?**

☐ Through the use of an anti-virus program. (If so, tick here and name the program under Other below.)

☐ By using a general disk utility program. (If so, tick here and name the program under Other below.)

☐ By reformatting the infected disk.

☐ By switching the infected computer off.

☐ Unknown.

Other:_____

_____

_____

11. **Who removed the infection(s) ?**

☐ The respondent.

☐ A technical support person.

☐ Unknown.

Other:_____

_____

_____

E. VIRUS INFECTION RESULTS

12. Did the virus install itself into the main memory (RAM) of the infected computer ?

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 12 above, briefly describe how this was determined under *COMMENTS*.

13. Did the virus install itself onto a diskette of the 5,25" 360 kb type ?

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 13 above, briefly describe how this was determined under *COMMENTS*.

14. Did the virus install itself onto a diskette of the 3,5" 1,44 Mb type ?

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 14 above, briefly describe how this was determined under *COMMENTS*.

15. **Did the virus install itself onto the non-removable hard disk drive ?**

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 15 above, briefly describe how this was determined under COMMENTS.

Before answering the last four questions, please ensure that you interpret them correctly. Consider the difference between information having been lost as a result of virus action, as opposed to information having been lost due to attempted retrieval procedures.

For example, if data files were lost after having formatted an infected disk, answer NO for Question 16, and mention this fact under COMMENTS.

Since these four questions initially appear to be similar, first read through them all before answering.

16. **Did the virus destroy or detrimentally affect any data files on any disk ? (eg word processor documents, data base files, spreadsheets, program source code, etc.)**

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 16 above, briefly describe how this was determined under COMMENTS.

17. **Did the virus destroy or detrimentally affect any <u>program</u> files on any disk ? (eg word processor programs, financial programs, editors, utilities, games, etc.)**

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 17 above, briefly describe how this was determined under COMMENTS.

18. **Did the virus destroy or detrimentally affect any <u>system</u> files on any disk ? (specifically the three DOS system files: COMMAND.COM, MSDOS.SYS and IO.SYS)**

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 18 above, briefly describe how this was determined under COMMENTS.

19. **Did the virus destroy or detrimentally affect any separate <u>disk sectors</u> which do not belong together as a file ?**

YES	COMMENTS
NO	
UNSURE	

If you answered YES to question 19 above, briefly describe how this was determined under COMMENTS.

Thank you very much for your time.