13.5.1

Computer Forensics - Disk Editing

(Runtime's DriveLook)

Laboratory Overview

Objective

At the end of this lab students will be able to index and browse a disk drive.

Information for Laboratory

A. Students will index a floppy disk and a hard drive for all text ever written to it.
B. Students will browse a list of all words stored on the drives.
C. Students will search for words or combinations of works on the drives.
D. Students will view the location of words in a disk editor.
E. Students will switch between hex and text views.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Students can download the software from the Runtime website.

Estimated Completion Time

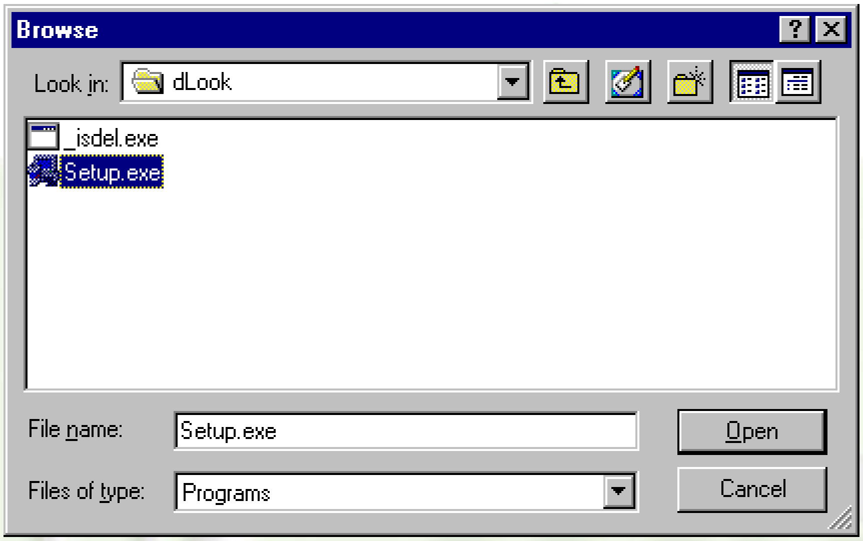
60 Minutes

Disk Indexing

The Runtime Drive Look software will allow you to index all the text ever written to the disk drive. You can then browse through the words indexed or search for a particular word or phrase on the drive. You can view the location on the drive where the word or phrase is found. The data can be looked at in either ASCII text or Hex format.

Step I:

Click on Start-->Run-->(browse to where the directory on the cd or hard drive where the Drive Look software resides)-->setup.exe.



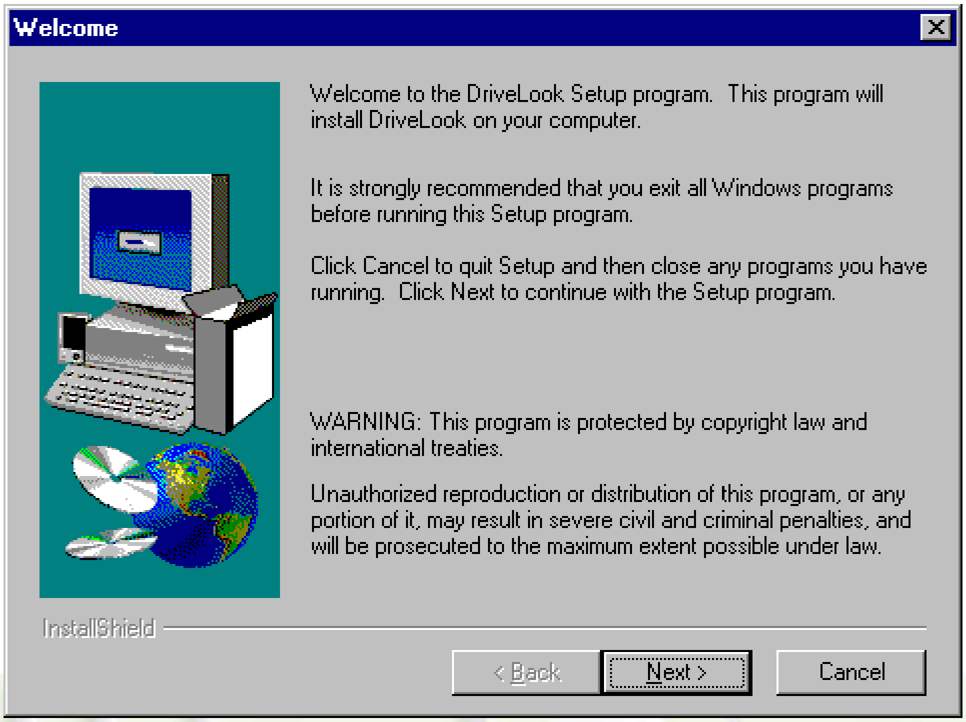
Look in: dLook

_isdel.exe
Setup.exe

File name: Setup.exe

Files of type: Programs

Click on Open, then on ok. The InstallShield will start.



Welcome to the DriveLook Setup program. This program will install DriveLook on your computer.

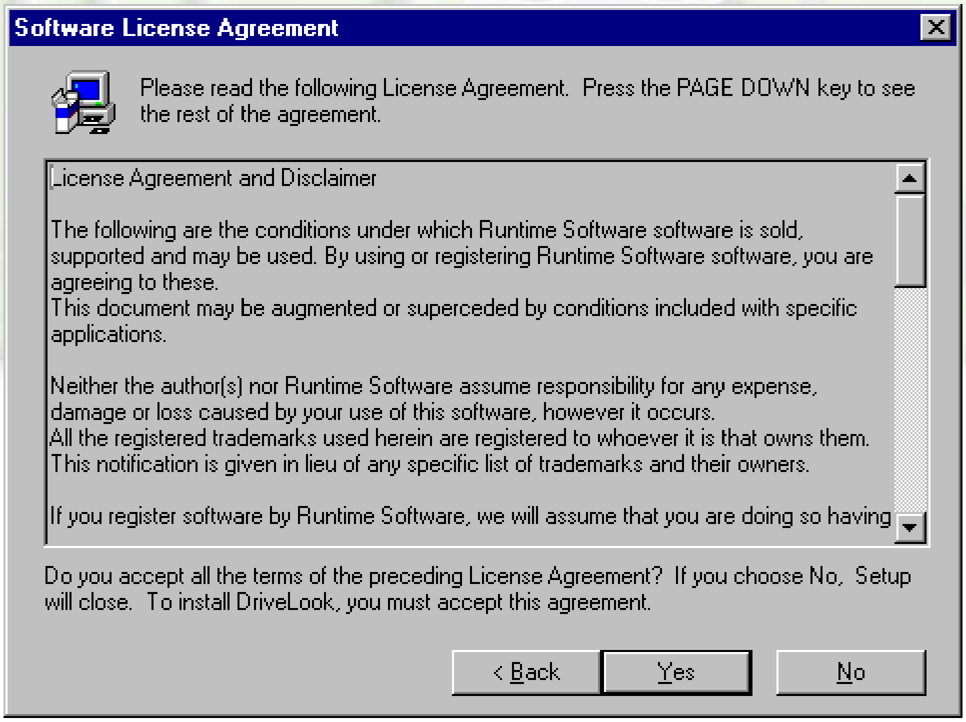
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Click on Next.



Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

License Agreement and Disclaimer

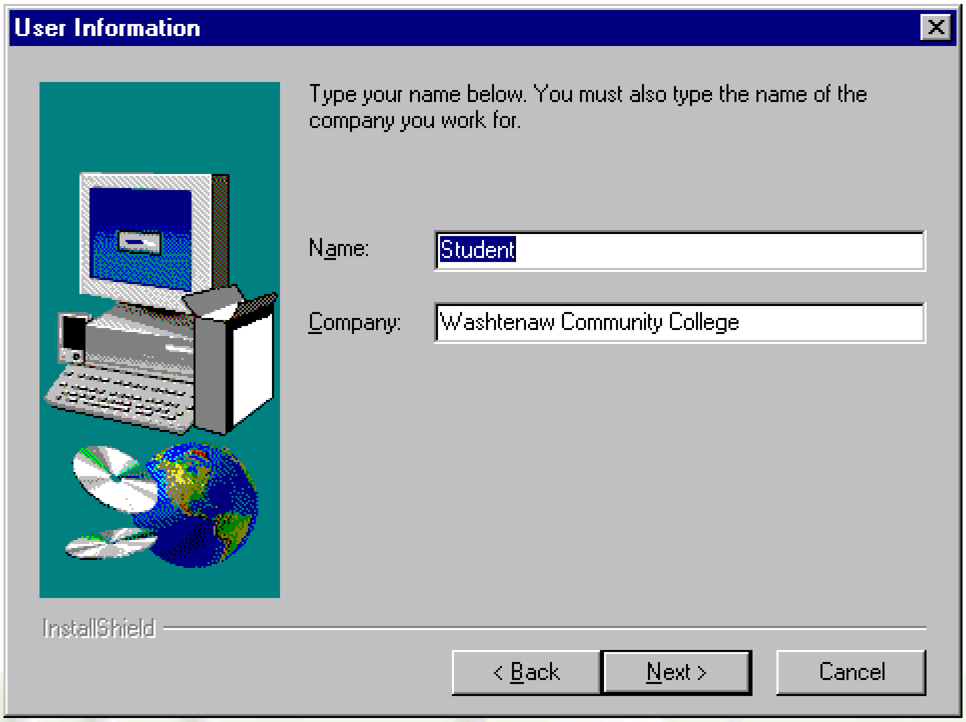
The following are the conditions under which Runtime Software software is sold, supported and may be used. By using or registering Runtime Software software, you are agreeing to these.
This document may be augmented or superceded by conditions included with specific applications.

Neither the author(s) nor Runtime Software assume responsibility for any expense, damage or loss caused by your use of this software, however it occurs.
All the registered trademarks used herein are registered to whoever it is that owns them.
This notification is given in lieu of any specific list of trademarks and their owners.

If you register software by Runtime Software, we will assume that you are doing so having

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install DriveLook, you must accept this agreement.

Click on Yes.



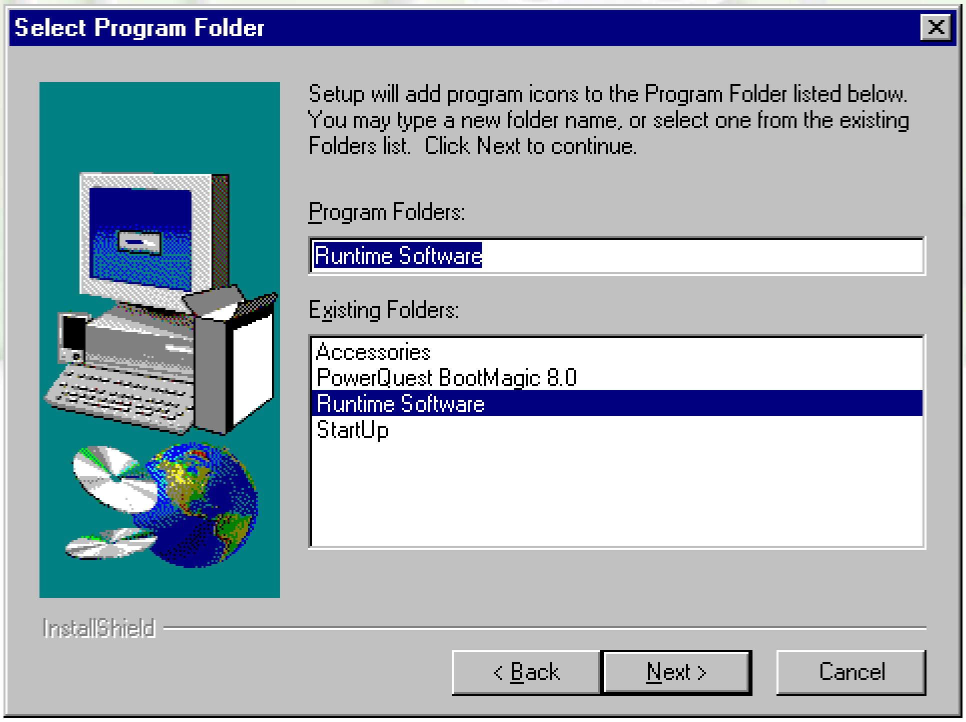
User Information

Type your name below. You must also type the name of the company you work for.

Name: Student

Company: Washtenaw Community College

Click on Next.



Select Program Folder

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

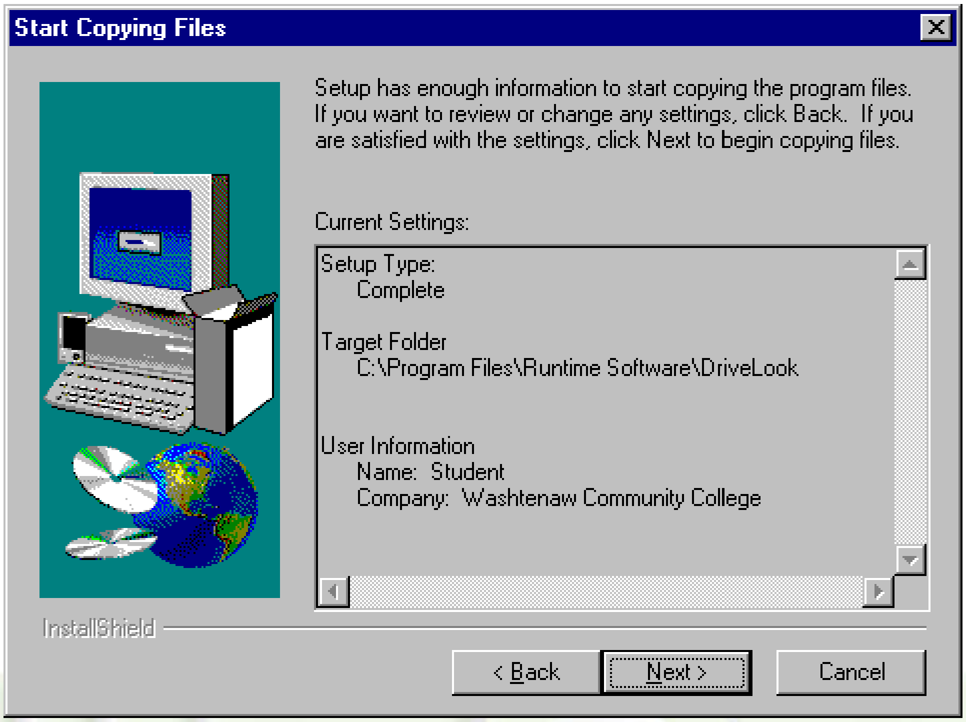
Program Folders:

Runtime Software

Existing Folders:

Accessories
PowerQuest BootMagic 8.0
Runtime Software
StartUp

Click on Next.



Start Copying Files

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

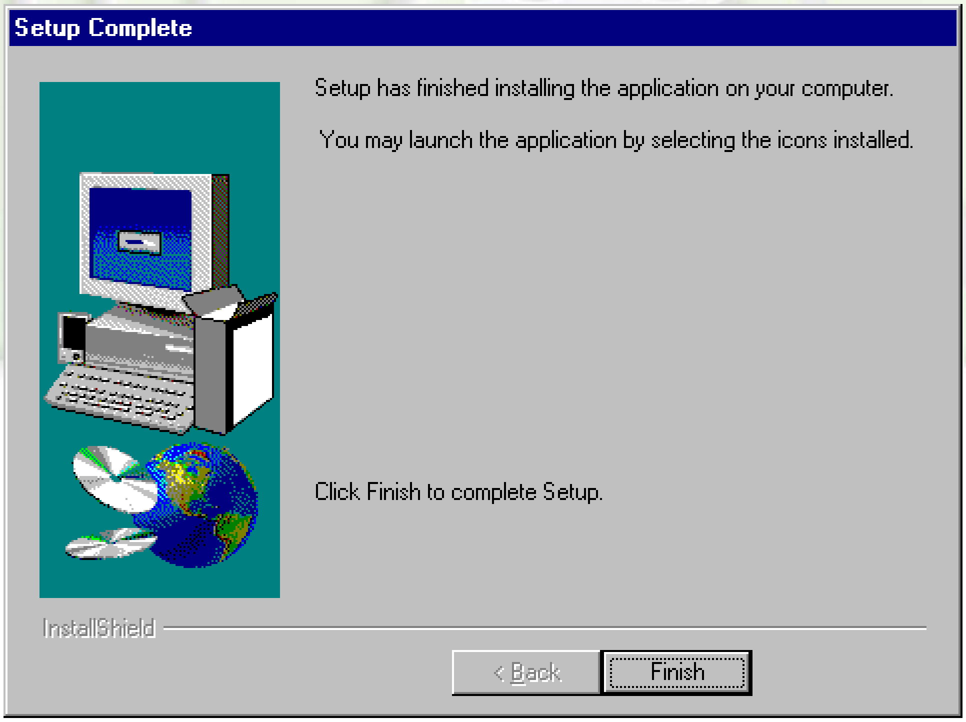
Current Settings:

```
Setup Type:
     Complete

Target Folder
     C:\Program Files\Runtime Software\DriveLook


User Information
     Name:  Student
     Company:  Washtenaw Community College
```

Click on Next.



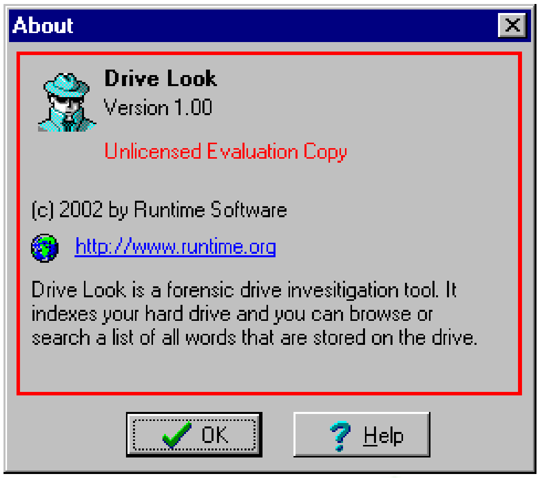
Setup Complete

Setup has finished installing the application on your computer.

You may launch the application by selecting the icons installed.

Click Finish to complete Setup.

Click on Finish.



Drive Look
Version 1.00

Unlicensed Evaluation Copy

(c) 2002 by Runtime Software

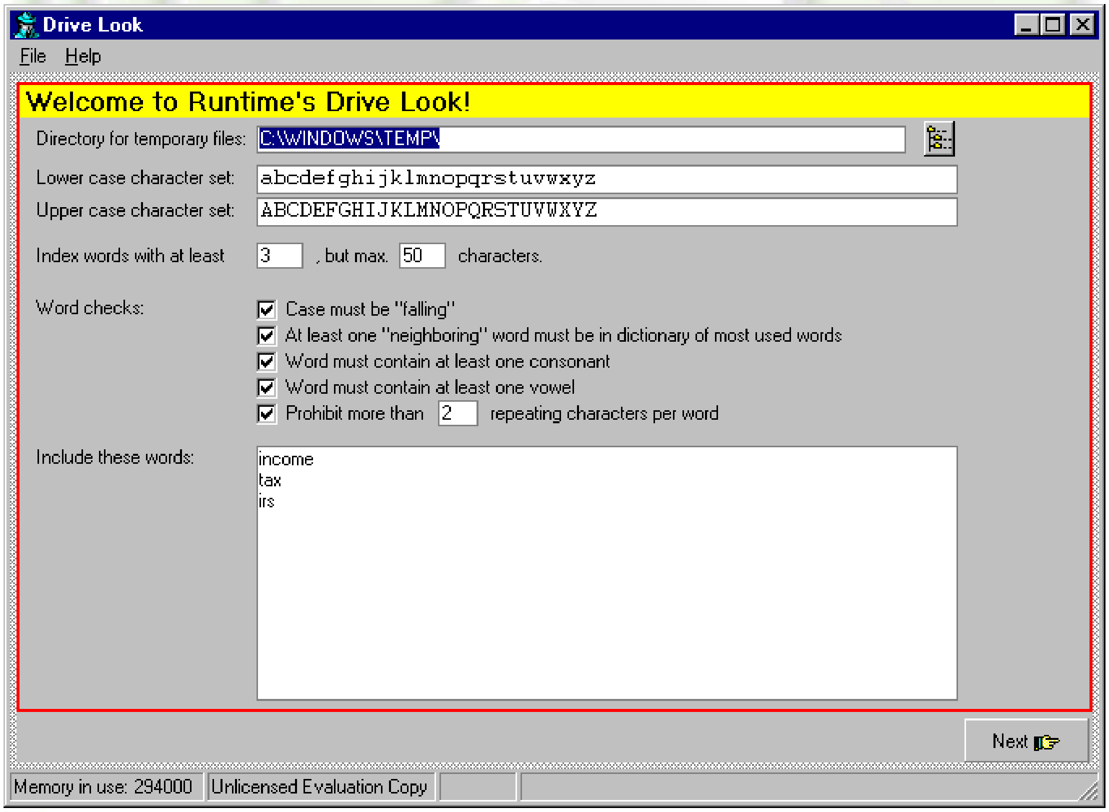
http://www.runtime.org

Drive Look is a forensic drive invesitigation tool. It indexes your hard drive and you can browse or search a list of all words that are stored on the drive.

About Drive Look from the Help Menu.

Step 2:

Start Drive Look by clicking on Start→Programs→Runtime→DriveLook



Welcome to Runtime's Drive Look!

Directory for temporary files: C:\WINDOWS\TEMP\

Lower case character set: abcdefghijklmnopqrstuvwxyz

Upper case character set: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Index words with at least 3 , but max. 50 characters.

Word checks:

☑ Case must be "falling"
☑ At least one "neighboring" word must be in dictionary of most used words
☑ Word must contain at least one consonant
☑ Word must contain at least one vowel
☑ Prohibit more than 2 repeating characters per word

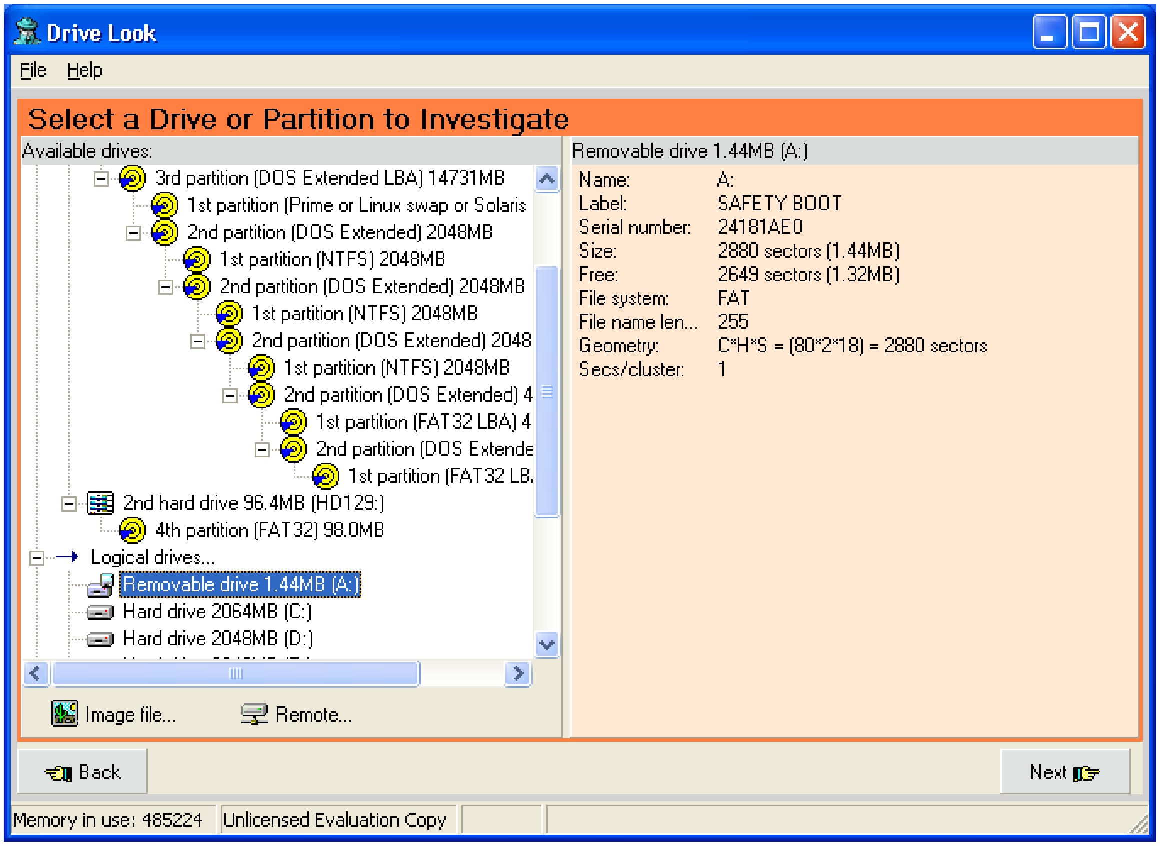
Include these words:

income
tax
irs

Memory in use: 294000 | Unlicensed Evaluation Copy

Step 3:

If you want to include specific words that might not get indexed depending on the options selected, type them into the text box and the bottom of the window. You can uncheck any of the options that you do not wish to use. We will use the defaults for this exercise. Scroll down until you see the logical drives and click on Removable drive 1.44MB(A:)



Select a Drive or Partition to Investigate

Available drives:

```
3rd partition (DOS Extended LBA) 14731MB
  1st partition (Prime or Linux swap or Solaris
  2nd partition (DOS Extended) 2048MB
    1st partition (NTFS) 2048MB
    2nd partition (DOS Extended) 2048MB
      1st partition (NTFS) 2048MB
      2nd partition (DOS Extended) 2048
        1st partition (NTFS) 2048MB
        2nd partition (DOS Extended) 4
          1st partition (FAT32 LBA) 4
          2nd partition (DOS Extende
            1st partition (FAT32 LB
2nd hard drive 96.4MB (HD129:)
  4th partition (FAT32) 98.0MB
Logical drives...
  Removable drive 1.44MB (A:)
  Hard drive 2064MB (C:)
  Hard drive 2048MB (D:)
```

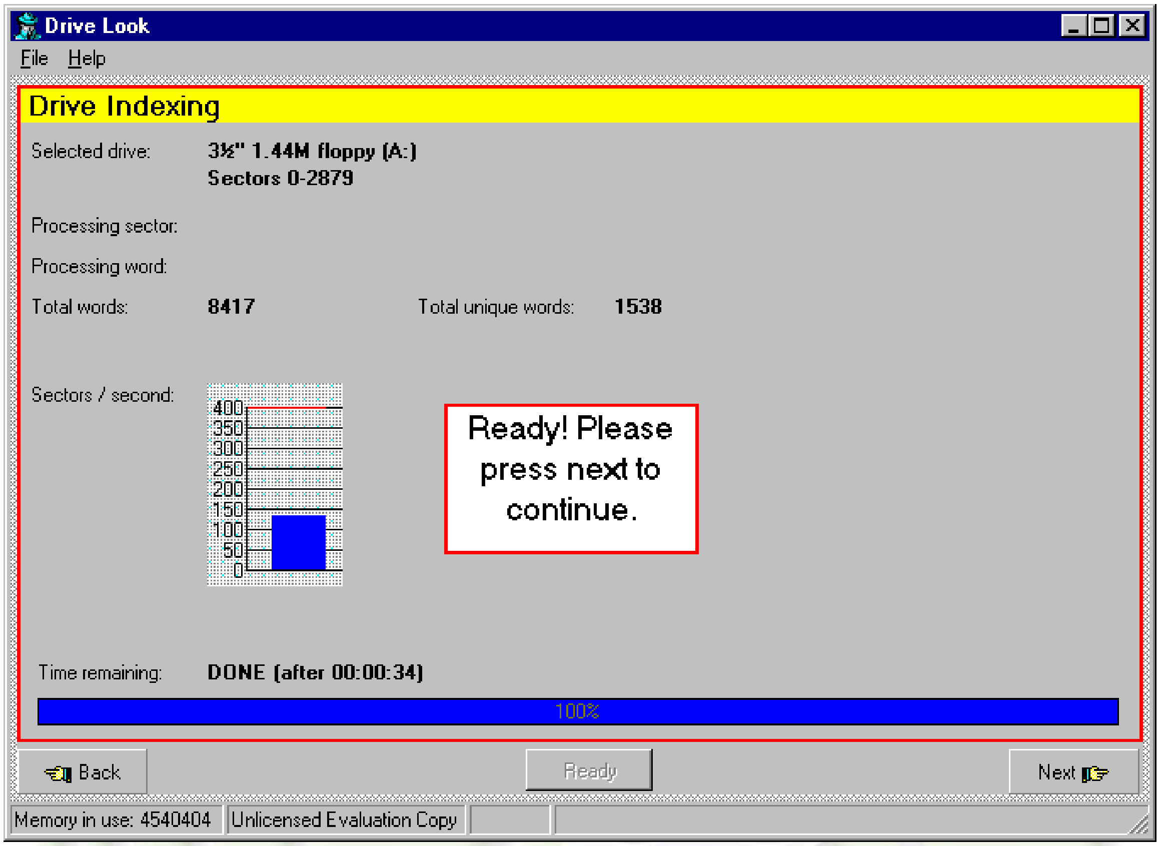
Removable drive 1.44MB (A:)

```
Name:           A:
Label:          SAFETY BOOT
Serial number:  24181AE0
Size:           2880 sectors (1.44MB)
Free:           2649 sectors (1.32MB)
File system:    FAT
File name len...  255
Geometry:       C*H*S = (80*2*18) = 2880 sectors
Secs/cluster:   1
```

Memory in use: 485224 | Unlicensed Evaluation Copy

Step 4:

To start indexing the drive click Next.



Drive Indexing

Selected drive: 3½" 1.44M floppy (A:)
Sectors 0-2879

Processing sector:

Processing word:

Total words: 8417 Total unique words: 1538

Sectors / second:

Ready! Please press next to continue.

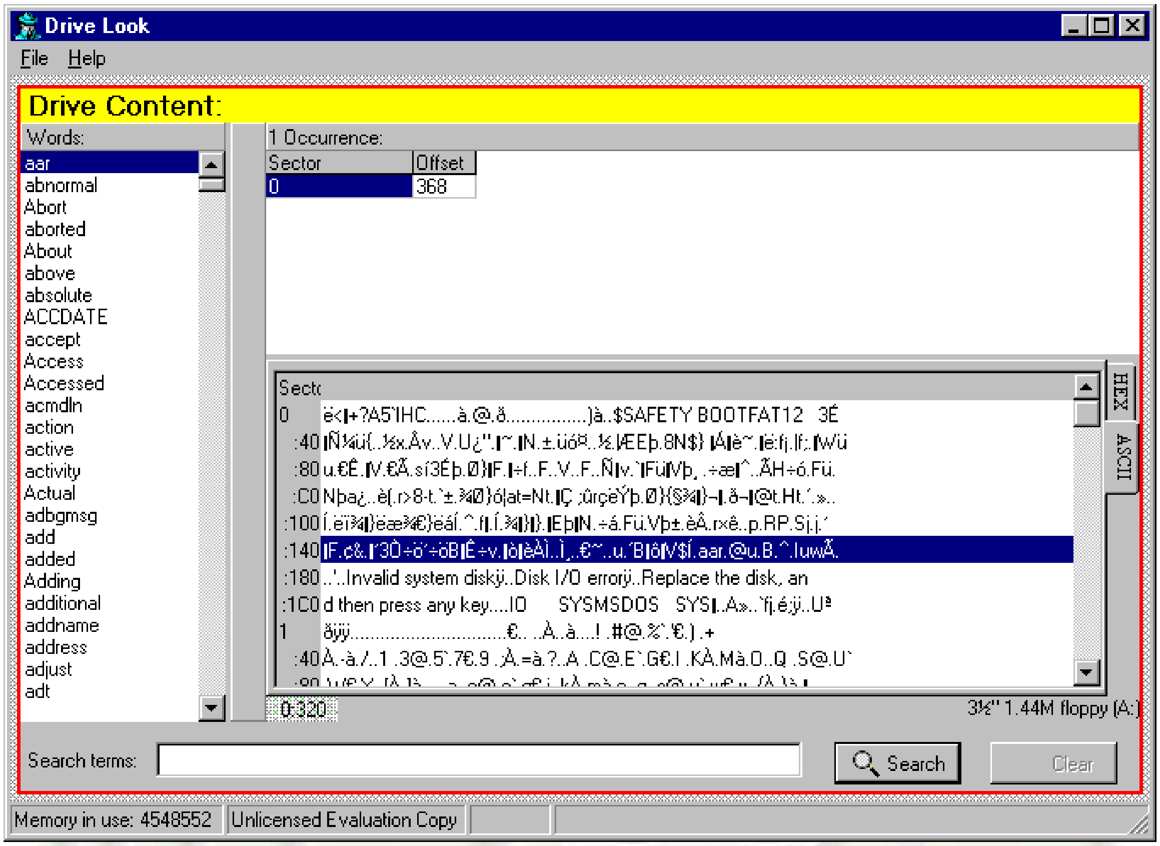
Time remaining: DONE (after 00:00:34)

Memory in use: 4540404 | Unlicensed Evaluation Copy

Click on Next.

Step 5:

The result screen looking at ASCII. Clicking on a word will highlight the location of the word on the disk, giving you the sector number and the line where it appears.



Words:

aar
abnormal
Abort
aborted
About
above
absolute
ACCDATE
accept
Access
Accessed
acmdln
action
active
activity
Actual
adbgmsg
add
added
Adding
additional
addname
address
adjust
adt

1 Occurrence:

Sector	Offset
0	368

```
Secto
0     ë<|+?A5'IHC......à.@.ð...............)à..$SAFETY BOOTFAT12   3É
  :40 |Ñ¼ü{..½x.Åv..V.U¿".|~.|N.±.üó¤..½.|ÆEþ.8N$} |Á|è~.|ë:fj.|f:.|Wü
  :80 u.€Ê.|V.€Ã.sí3Éþ.Ø}|F.|÷f..F..V..F..Ñ|v.`|Fü|Vþ¸.÷æ|^..ÃH÷ó.Fü.
  :C0 Nþa¿..è(.r>8-t.`±.¾Ø}ó|at=Nt.|Ç ;ûrçèÝþ.Ø}{§¾|}¬|.ð¬|@t.Ht.´.».
 :100 Í.ëï¾|}èæ¾€}èáÍ.^.f|.Í.¾|}|}.|Eþ|N.÷á.Fü.Vþ±.èÂ.r×ê..p.RP.Sj.j.´
 :140 |F.¢&.|'3Ò÷ö'÷öB|Ê÷v.|ò|èÀÌ..Ì¸.€~..u.´B|ô|V$Í.aar.@u.B.^.IuwÃ.
 :180 ..'..Invalid system diskÿ..Disk I/O errorÿ..Replace the disk, an
 :1C0 d then press any key....IO      SYSMSDOS   SYS|..A»..`fj.é;ÿ..Uª
1     ðÿÿ............................€.. ..À..à...! .#@.%`.€.) .+
  :40 À.-à./..1 .3@.5`.7€.9 .À.=à.?..A .C@.E`.G€.I .KÀ.Mà.O..Q .S@.U`
```

0:320

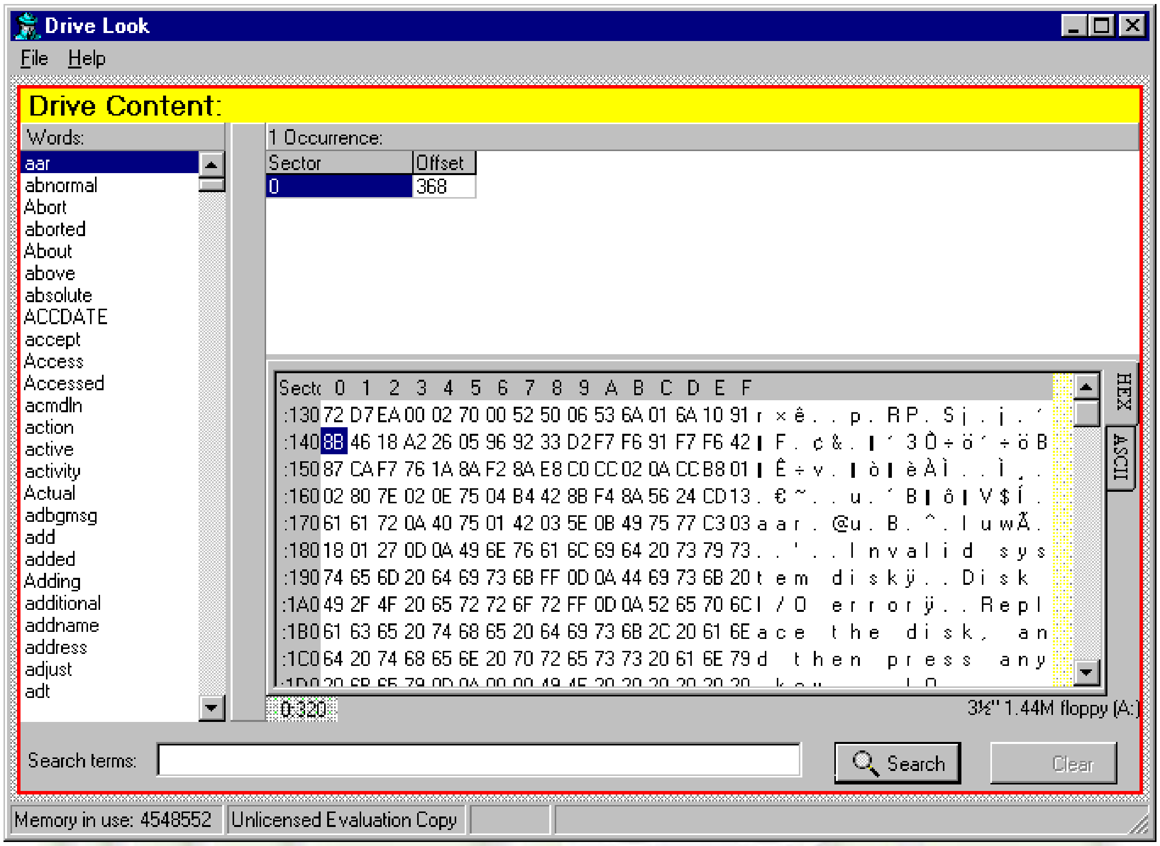
3½" 1.44M floppy (A:)

Search terms:

Memory in use: 4548552

Unlicensed Evaluation Copy

The result looking at HEX. This gives you the same information as above, but gives you the starting point of the word in Hex.



Drive Content:

Words:
aar
abnormal
Abort
aborted
About
above
absolute
ACCDATE
accept
Access
Accessed
acmdln
action
active
activity
Actual
adbgmsg
add
added
Adding
additional
addname
address
adjust
adt

1 Occurrence:

Sector	Offset
0	368

```
Sect  0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
:130 72 D7 EA 00 02 70 00 52 50 06 53 6A 01 6A 10 91 r × ê . . p . R P . S j . j . ´
:140 8B 46 18 A2 26 05 96 92 33 D2 F7 F6 91 F7 F6 42 ▌ F . ¢ & . ▌ ´ 3 Ò ÷ ö ´ ÷ ö B
:150 87 CA F7 76 1A 8A F2 8A E8 C0 CC 02 0A CC B8 01 ▌ Ê ÷ v . ▌ ò ▌ è À Ì . . Ì ¸ .
:160 02 80 7E 02 0E 75 04 B4 42 8B F4 8A 56 24 CD 13 . € ~ . . u . ´ B ▌ ô ▌ V $ Í .
:170 61 61 72 0A 40 75 01 42 03 5E 0B 49 75 77 C3 03 a a r . @ u . B . ^ . I u w Ã .
:180 18 01 27 0D 0A 49 6E 76 61 6C 69 64 20 73 79 73 . . ' . . I n v a l i d   s y s
:190 74 65 6D 20 64 69 73 6B FF 0D 0A 44 69 73 6B 20 t e m   d i s k ÿ . . D i s k
:1A0 49 2F 4F 20 65 72 72 6F 72 FF 0D 0A 52 65 70 6C I / O   e r r o r ÿ . . R e p l
:1B0 61 63 65 20 74 68 65 20 64 69 73 6B 2C 20 61 6E a c e   t h e   d i s k ,   a n
:1C0 64 20 74 68 65 6E 20 70 72 65 73 73 20 61 6E 79 d   t h e n   p r e s s   a n y
:1D0 20 6B 65 79 0D 0A 00 00 49 4F 20 20 20 20 20 20   k e y . . . . I O
```

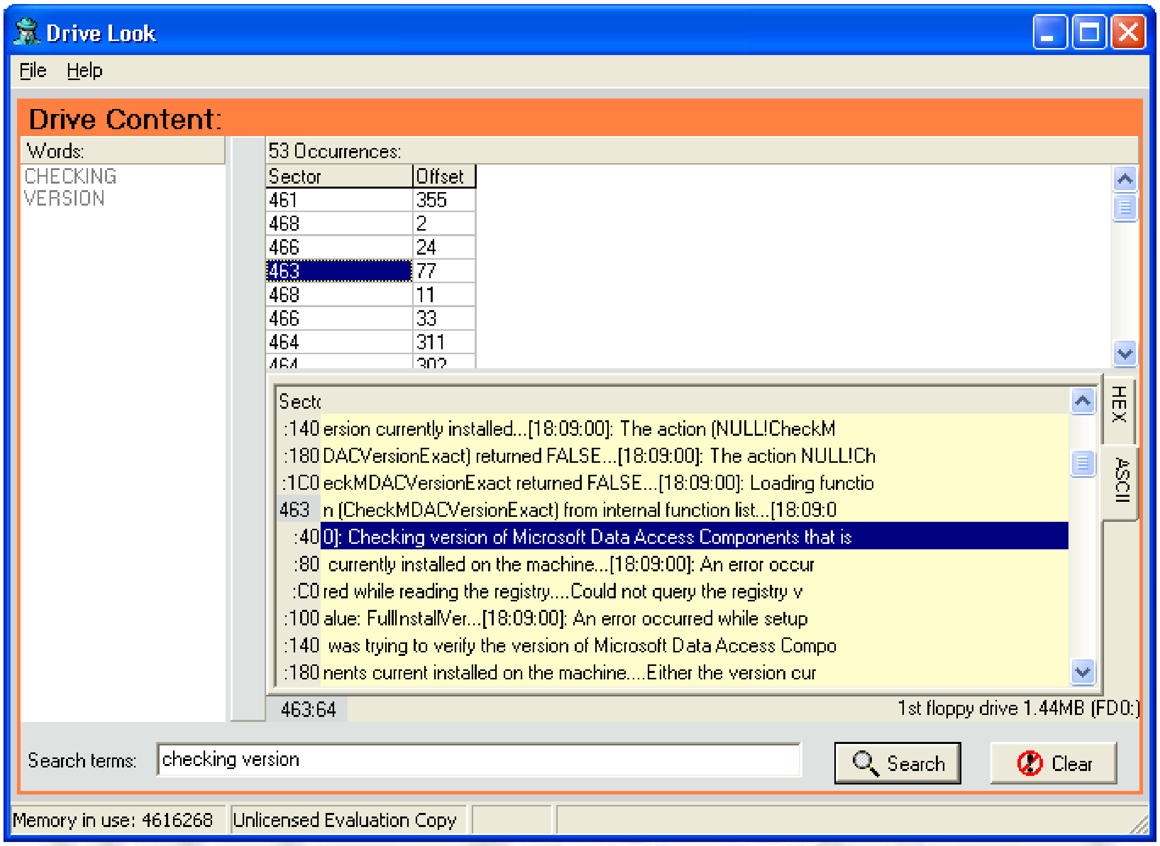
0:320 3½" 1.44M floppy (A:)

Search terms:

Memory in use: 4548552 Unlicensed Evaluation Copy

Step 6:

Once the disk drive is indexed, you can also search for a word or a group of words, just type the word(s) in the Search terms: text box and click on Search.



Words:

CHECKING
VERSION

53 Occurrences:

Sector	Offset
461	355
468	2
466	24
463	77
468	11
466	33
464	311
464	302

```
Secto
    :140 ersion currently installed...[18:09:00]: The action (NULL!CheckM
    :180 DACVersionExact) returned FALSE...[18:09:00]: The action NULL!Ch
    :1C0 eckMDACVersionExact returned FALSE...[18:09:00]: Loading functio
463      n (CheckMDACVersionExact) from internal function list...[18:09:0
     :40 0]: Checking version of Microsoft Data Access Components that is
     :80  currently installed on the machine...[18:09:00]: An error occur
     :C0 red while reading the registry....Could not query the registry v
    :100 alue: FullInstallVer...[18:09:00]: An error occurred while setup
    :140  was trying to verify the version of Microsoft Data Access Compo
    :180 nents current installed on the machine....Either the version cur
```

463:64

1st floppy drive 1.44MB (FD0:)

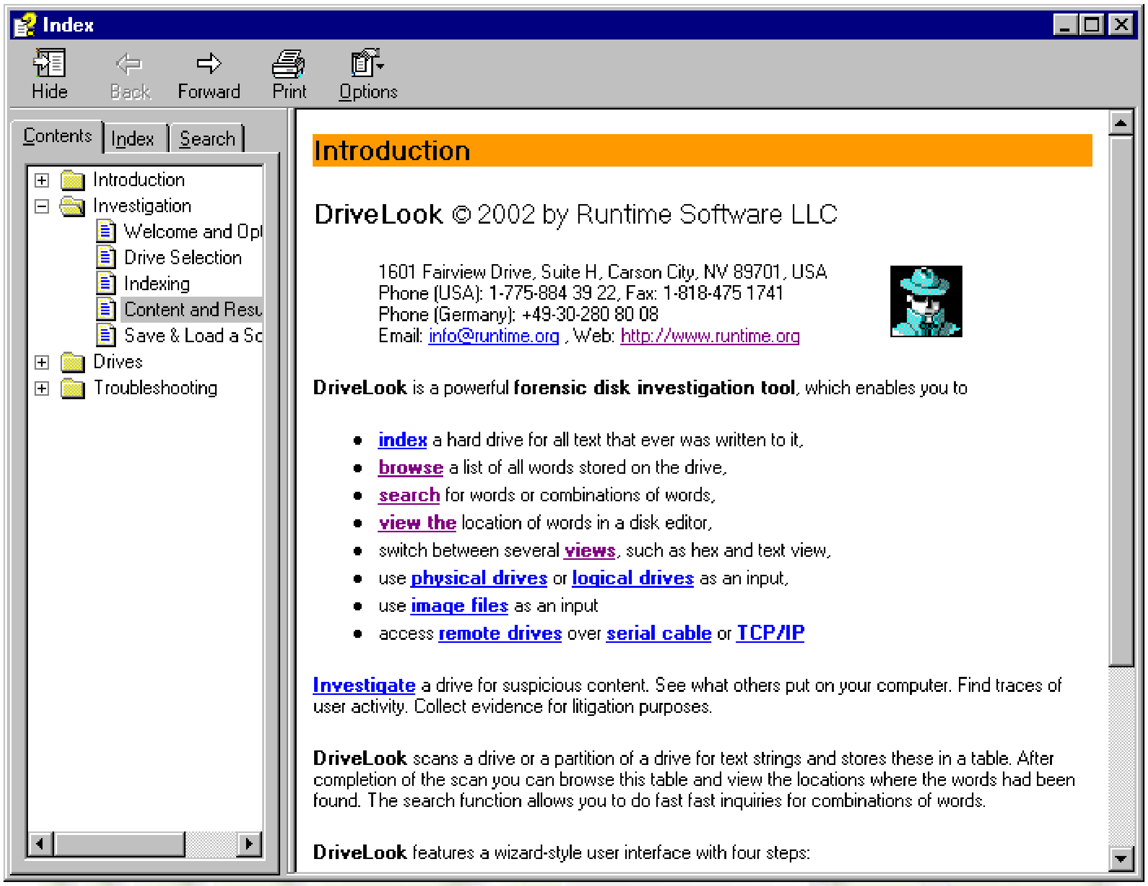
Search terms: checking version

Memory in use: 4616268

Unlicensed Evaluation Copy

Step 7:

The Help menu can give you more information about what other features are available in the program. Look at it and try some of the other features.



Introduction

DriveLook © 2002 by Runtime Software LLC

1601 Fairview Drive, Suite H, Carson City, NV 89701, USA
Phone (USA): 1-775-884 39 22, Fax: 1-818-475 1741
Phone (Germany): +49-30-280 80 08
Email: info@runtime.org , Web: http://www.runtime.org

DriveLook is a powerful **forensic disk investigation tool**, which enables you to

- **index** a hard drive for all text that ever was written to it,
- **browse** a list of all words stored on the drive,
- **search** for words or combinations of words,
- **view the** location of words in a disk editor,
- switch between several **views**, such as hex and text view,
- use **physical drives** or **logical drives** as an input,
- use **image files** as an input
- access **remote drives** over **serial cable** or **TCP/IP**

Investigate a drive for suspicious content. See what others put on your computer. Find traces of user activity. Collect evidence for litigation purposes.

DriveLook scans a drive or a partition of a drive for text strings and stores these in a table. After completion of the scan you can browse this table and view the locations where the words had been found. The search function allows you to do fast fast inquiries for combinations of words.

DriveLook features a wizard-style user interface with four steps:

The help-->content screen.

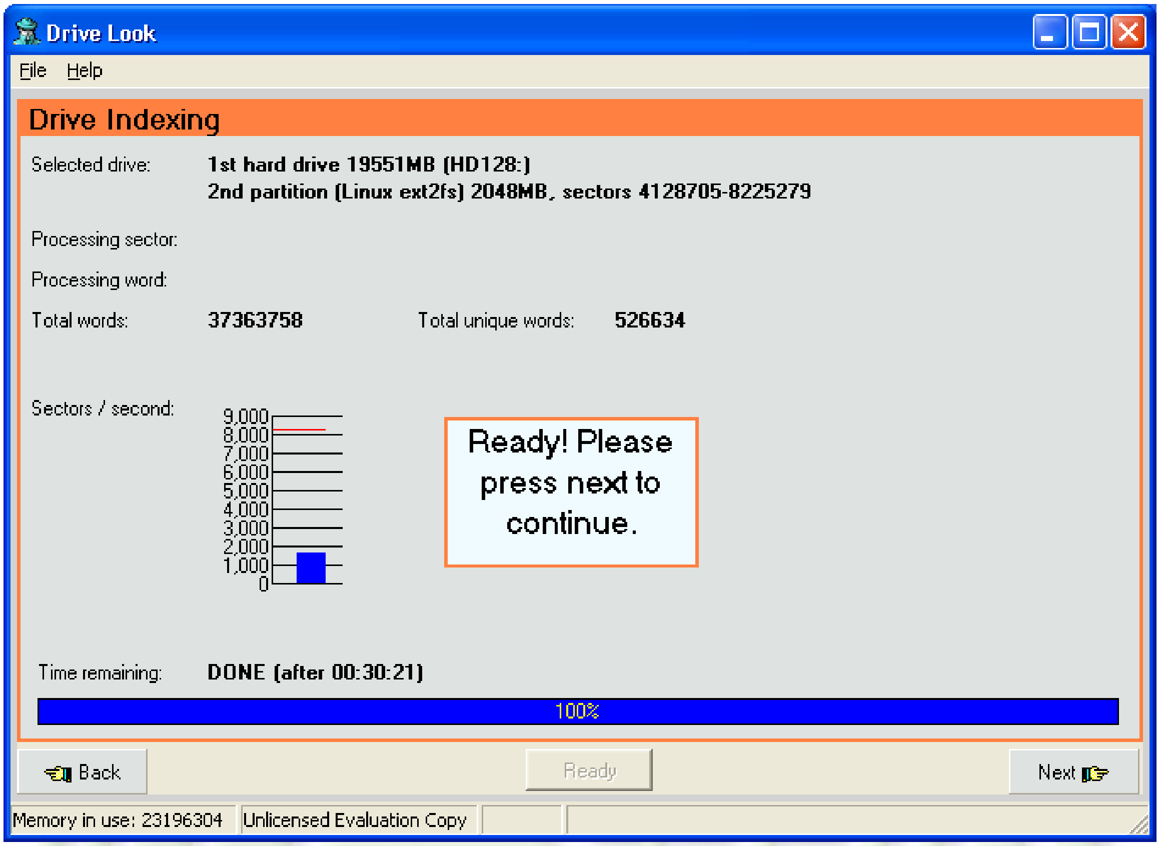
Step 8:

Exit the program and restart it. Look at one or more of the hard drive partitions. Do the smallest partition(s) you have. The larger the partition, the longer it will take to index. A 20 GB drive/partition will take almost 3 hours to index and another hour to process before you can look at it.

Make sure you have plenty of free space on the drive that you will be putting the temporary file. For this part of the lab, I installed the program on my WindowsXP partition, ran the indexing on the Linux partition, and had to store the temporary files on the Windows98 partition as there wasn’t enough free space to store them on the XP partition.

Indexing the hard drive partition will take a while, so be patient. Your instructor may have you do something else while it indexes, or start the index before he starts the lecture for this class period. Once it is indexed, repeat the steps you used looking at the floppy drive.

Some of the views on a Linux partition.



Drive Look

Drive Indexing

Selected drive: 1st hard drive 19551MB (HD128:)
2nd partition (Linux ext2fs) 2048MB, sectors 4128705-8225279

Processing sector:

Processing word:

Total words: 37363758 Total unique words: 526634

Sectors / second:

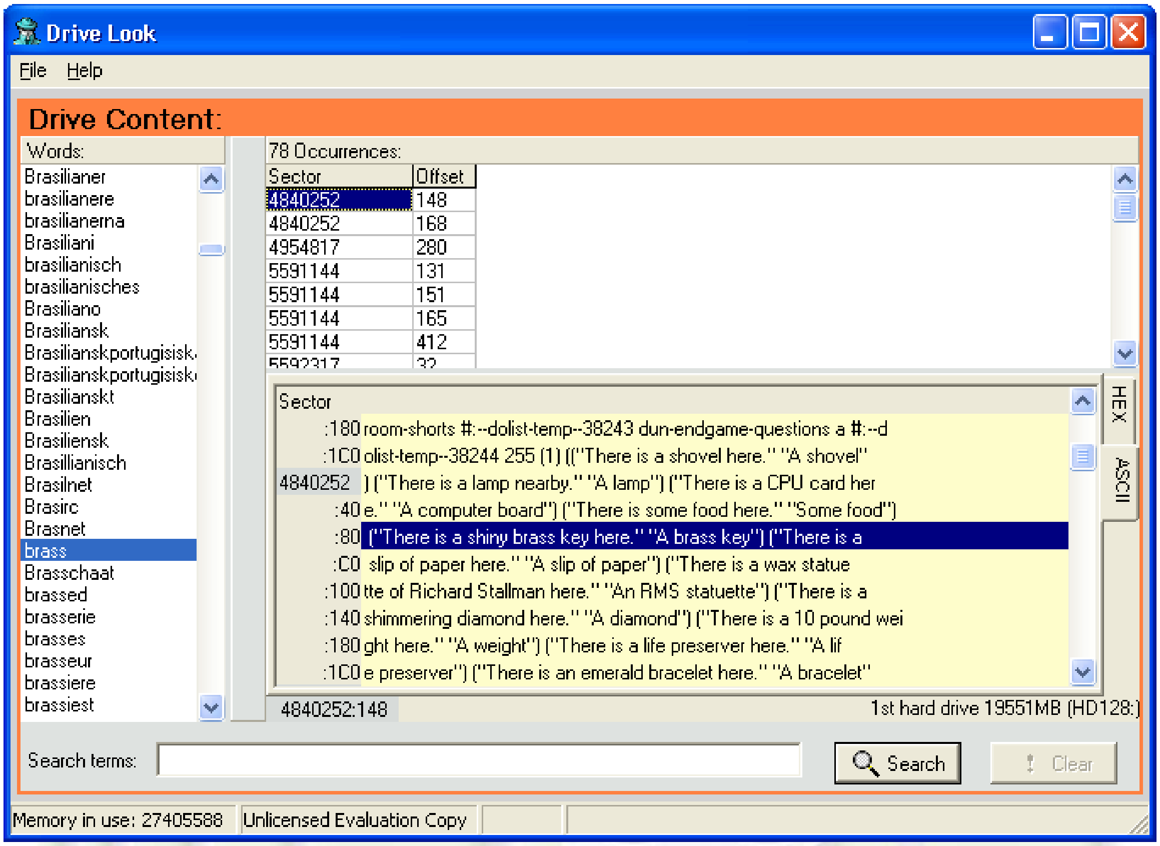
Ready! Please press next to continue.

Time remaining: DONE (after 00:30:21)

100%

Memory in use: 23196304 Unlicensed Evaluation Copy

Done indexing.



Words:

Brasilianer
brasilianere
brasilianerna
Brasiliani
brasilianisch
brasilianisches
Brasiliano
Brasiliansk
Brasilianskportugisisk
Brasilianskportugisisk
Brasilianskt
Brasilien
Brasiliensk
Brasillianisch
Brasilnet
Brasirc
Brasnet
brass
Brasschaat
brassed
brasserie
brasses
brasseur
brassiere
brassiest

78 Occurrences:

Sector	Offset
4840252	148
4840252	168
4954817	280
5591144	131
5591144	151
5591144	165
5591144	412
5592317	32

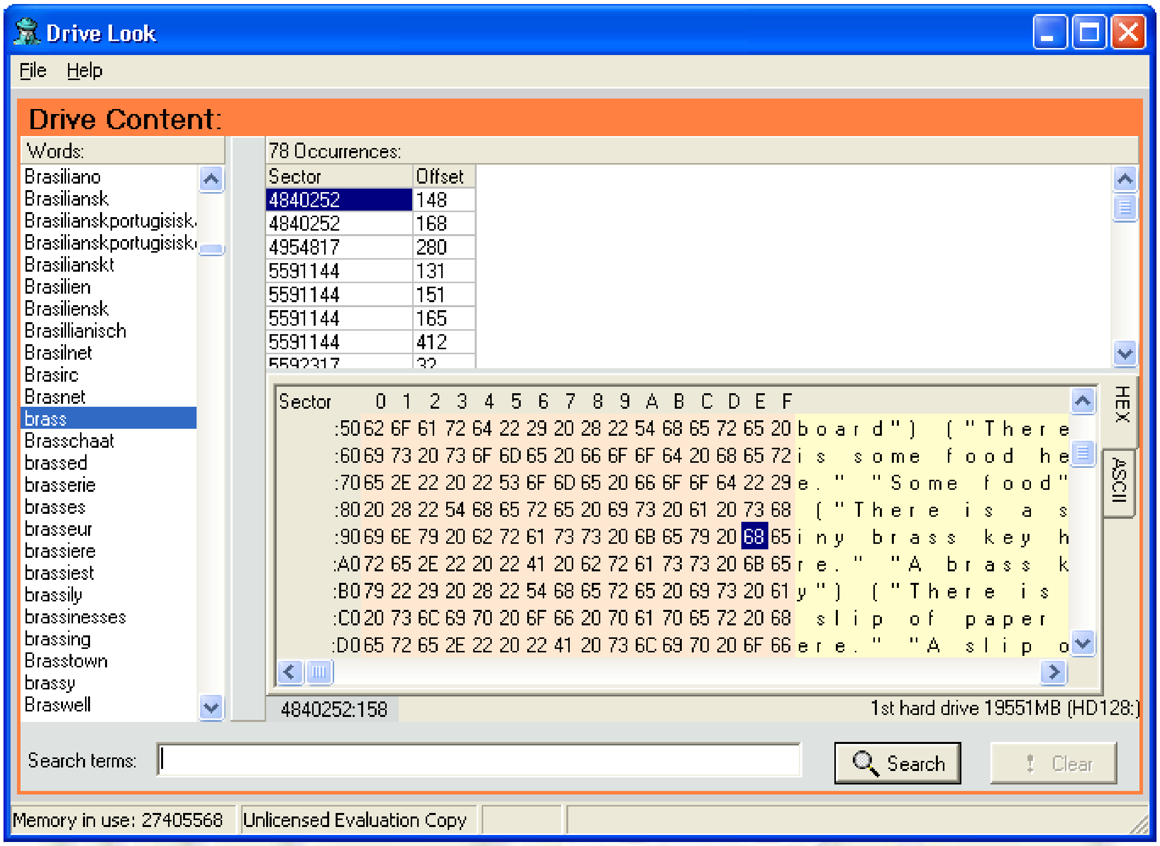
```
Sector
       :180 room-shorts #:--dolist-temp--38243 dun-endgame-questions a #:--d
       :1C0 olist-temp--38244 255 (1) (("There is a shovel here." "A shovel"
4840252     ) ("There is a lamp nearby." "A lamp") ("There is a CPU card her
        :40 e." "A computer board") ("There is some food here." "Some food")
        :80  ("There is a shiny brass key here." "A brass key") ("There is a
        :C0  slip of paper here." "A slip of paper") ("There is a wax statue
       :100 tte of Richard Stallman here." "An RMS statuette") ("There is a
       :140 shimmering diamond here." "A diamond") ("There is a 10 pound wei
       :180 ght here." "A weight") ("There is a life preserver here." "A lif
       :1C0 e preserver") ("There is an emerald bracelet here." "A bracelet"
```

4840252:148   1st hard drive 19551MB (HD128:)

Search terms:

Memory in use: 27405588   Unlicensed Evaluation Copy

ASCII result view.



Drive Content:

Words:

Brasiliano
Brasiliansk
Brasilianskportugisisk
Brasilianskportugisisk
Brasilianskt
Brasilien
Brasiliensk
Brasillianisch
Brasilnet
Brasirc
Brasnet
brass
Brasschaat
brassed
brasserie
brasses
brasseur
brassiere
brassiest
brassily
brassinesses
brassing
Brasstown
brassy
Braswell

78 Occurrences:

Sector	Offset
4840252	148
4840252	168
4954817	280
5591144	131
5591144	151
5591144	165
5591144	412
5592317	32

```
Sector    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
      :50 62 6F 61 72 64 22 29 20 28 22 54 68 65 72 65 20 board") ("There 
      :60 69 73 20 73 6F 6D 65 20 66 6F 6F 64 20 68 65 72 is some food her
      :70 65 2E 22 20 22 53 6F 6D 65 20 66 6F 6F 64 22 29 e." "Some food")
      :80 20 28 22 54 68 65 72 65 20 69 73 20 61 20 73 68  ("There is a sh
      :90 69 6E 79 20 62 72 61 73 73 20 6B 65 79 20 68 65 iny brass key he
      :A0 72 65 2E 22 20 22 41 20 62 72 61 73 73 20 6B 65 re." "A brass ke
      :B0 79 22 29 20 28 22 54 68 65 72 65 20 69 73 20 61 y") ("There is a
      :C0 20 73 6C 69 70 20 6F 66 20 70 61 70 65 72 20 68  slip of paper h
      :D0 65 72 65 2E 22 20 22 41 20 73 6C 69 70 20 6F 66 ere." "A slip of
```

4840252:158

1st hard drive 19551MB (HD128:)

Search terms:

Memory in use: 27405568

Unlicensed Evaluation Copy

Hex result view.

Step 9: Analysis

1) Why would you want to index a disk drive?

2) After working with this utility, what about Drive Look do you feel you should study further? Why?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Try out some of the other features found on the menu toolbar or found by looking at the help menu.

Go to http://www.runtime.org for further information on the software and on other software they offer.

Research software with similar functionality.

Appendix

This lab was written using Runtime's Drive Look Version 1.00 which may be found at

www.runtime.org

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).

A floppy drive is recommended.