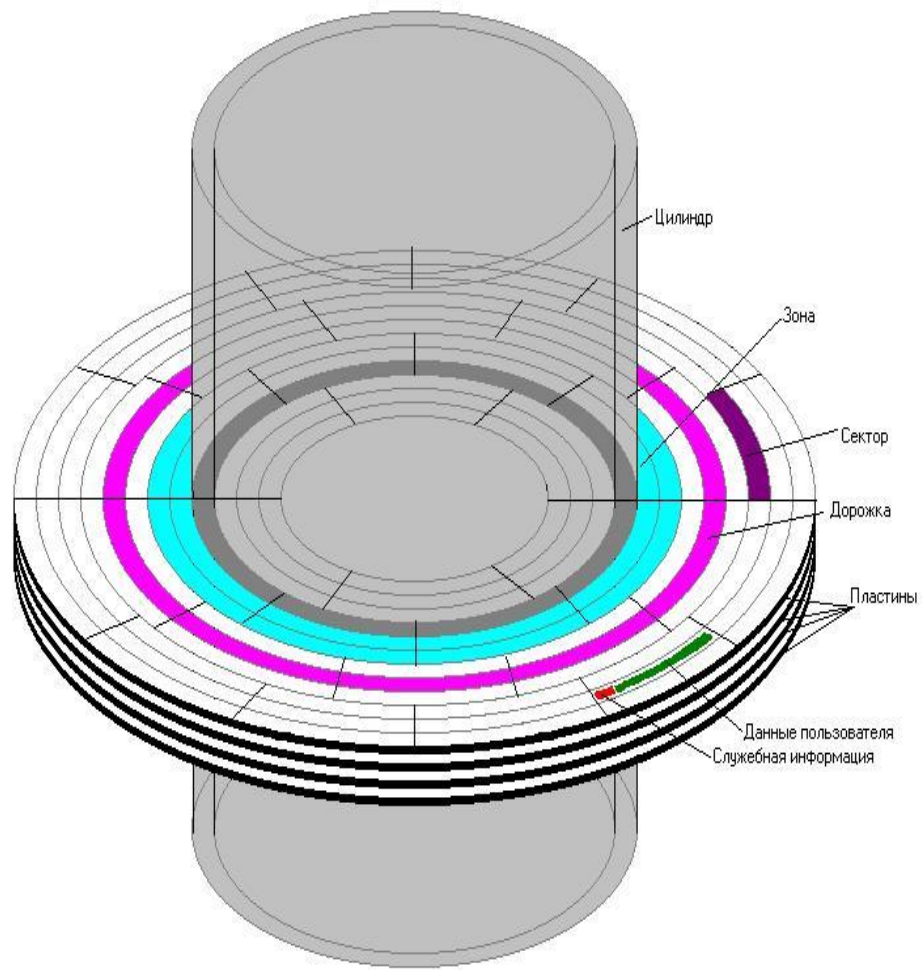


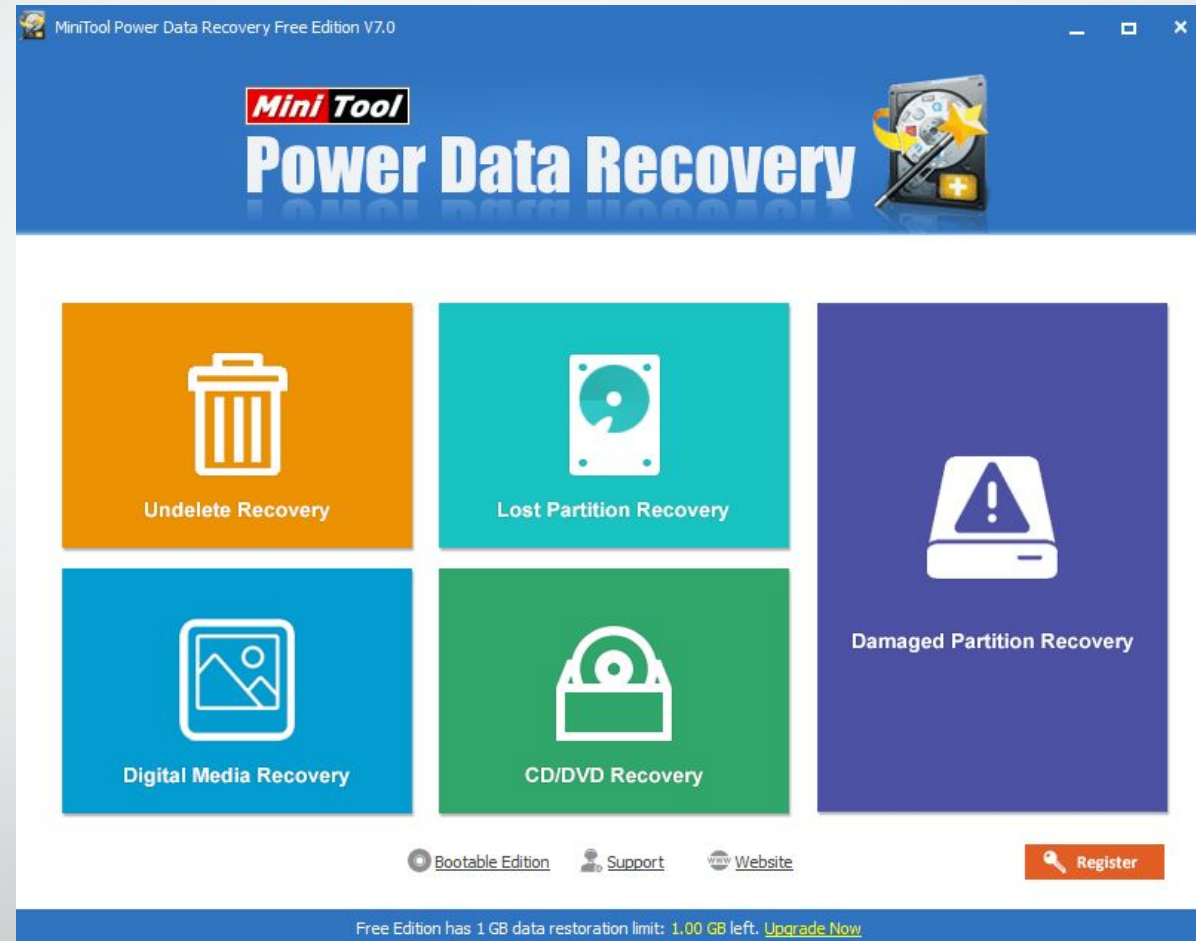
Фиксация остаточных данных при расследовании компьютерных преступлений



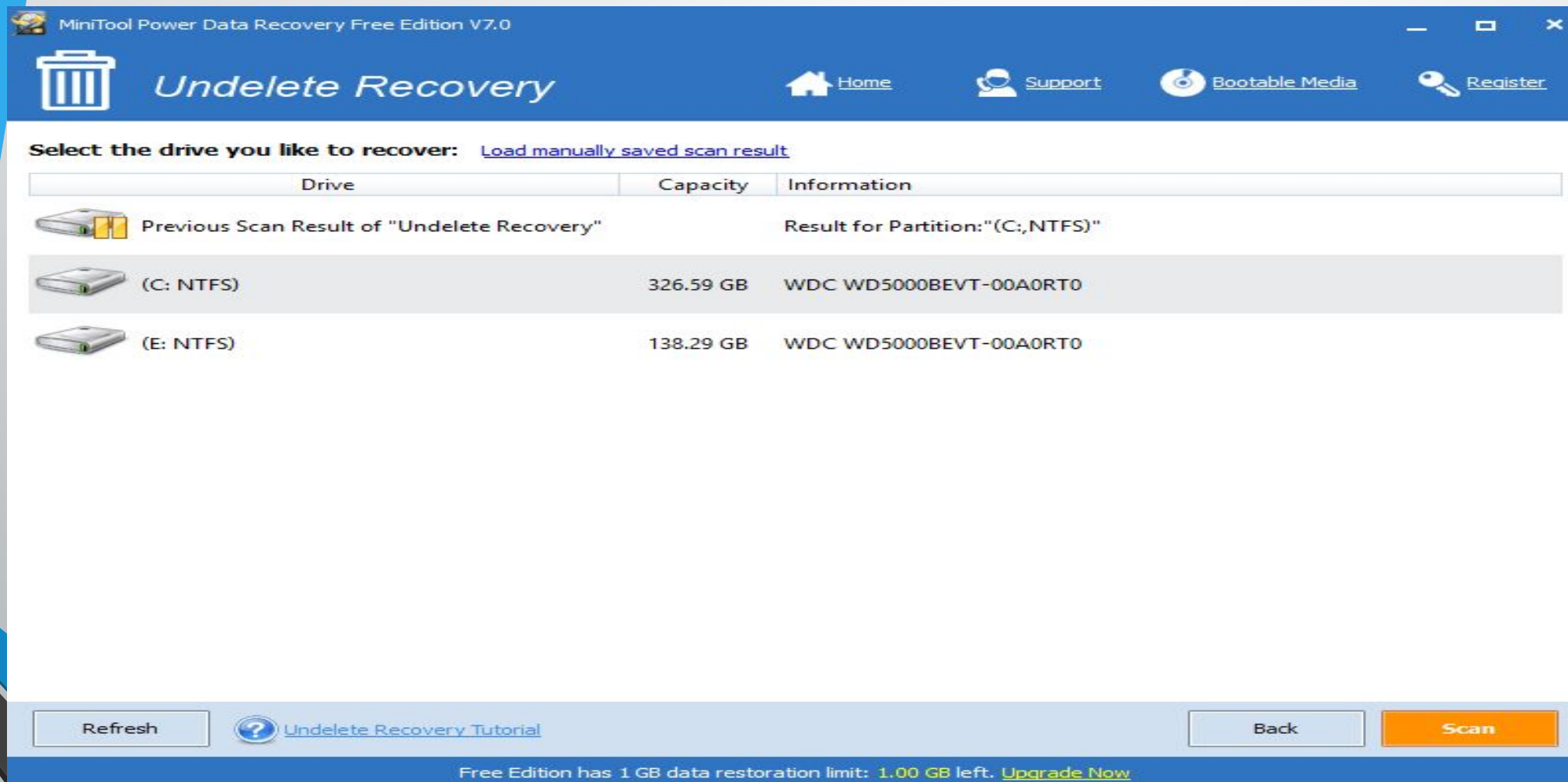
- Остаточные данные – информация на записывающем устройстве, оставшаяся после ее формального удаления.

Minitool Power Data Recovery

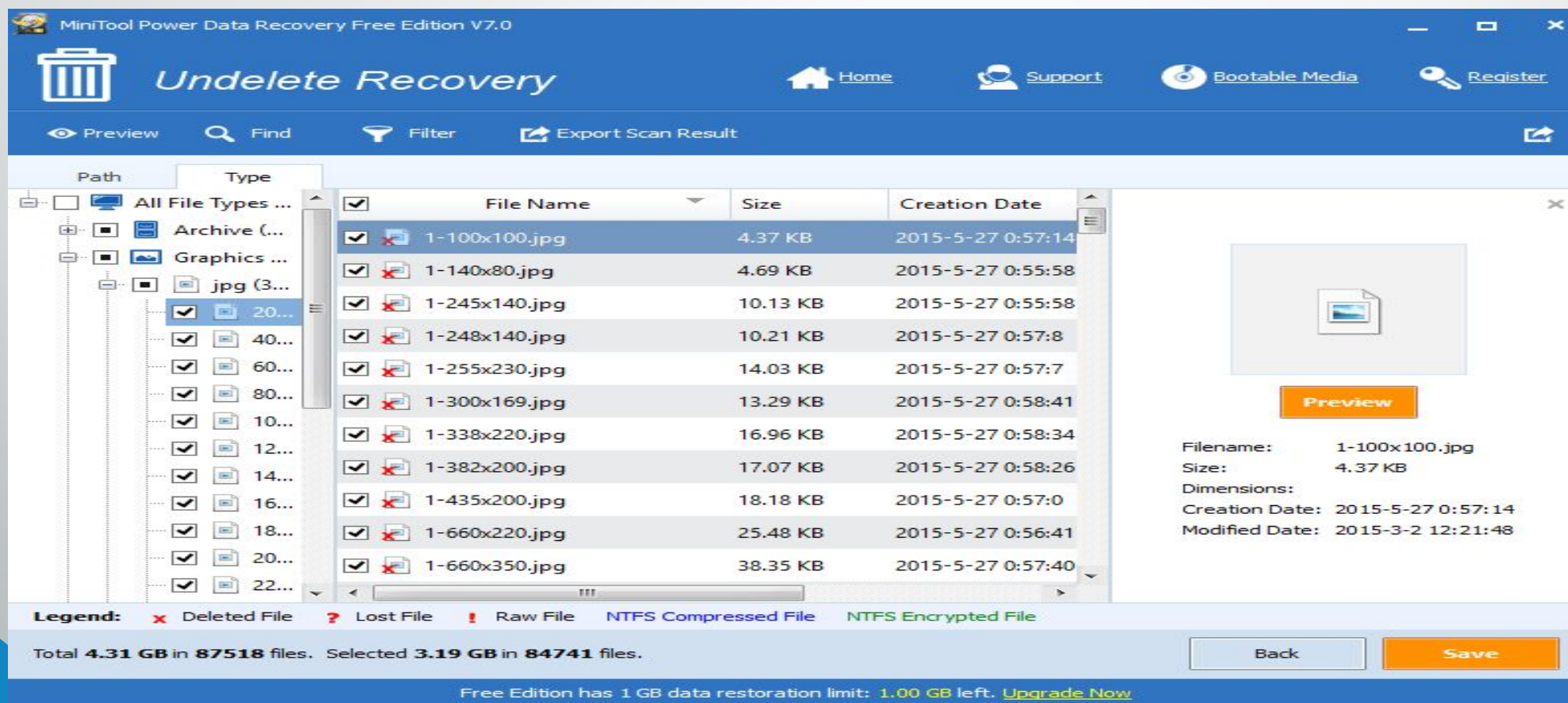
используется при
восстановлении данных на
повреждённых, жёстких
неисправных дисках, отличается
наиболее полным
сканированием.



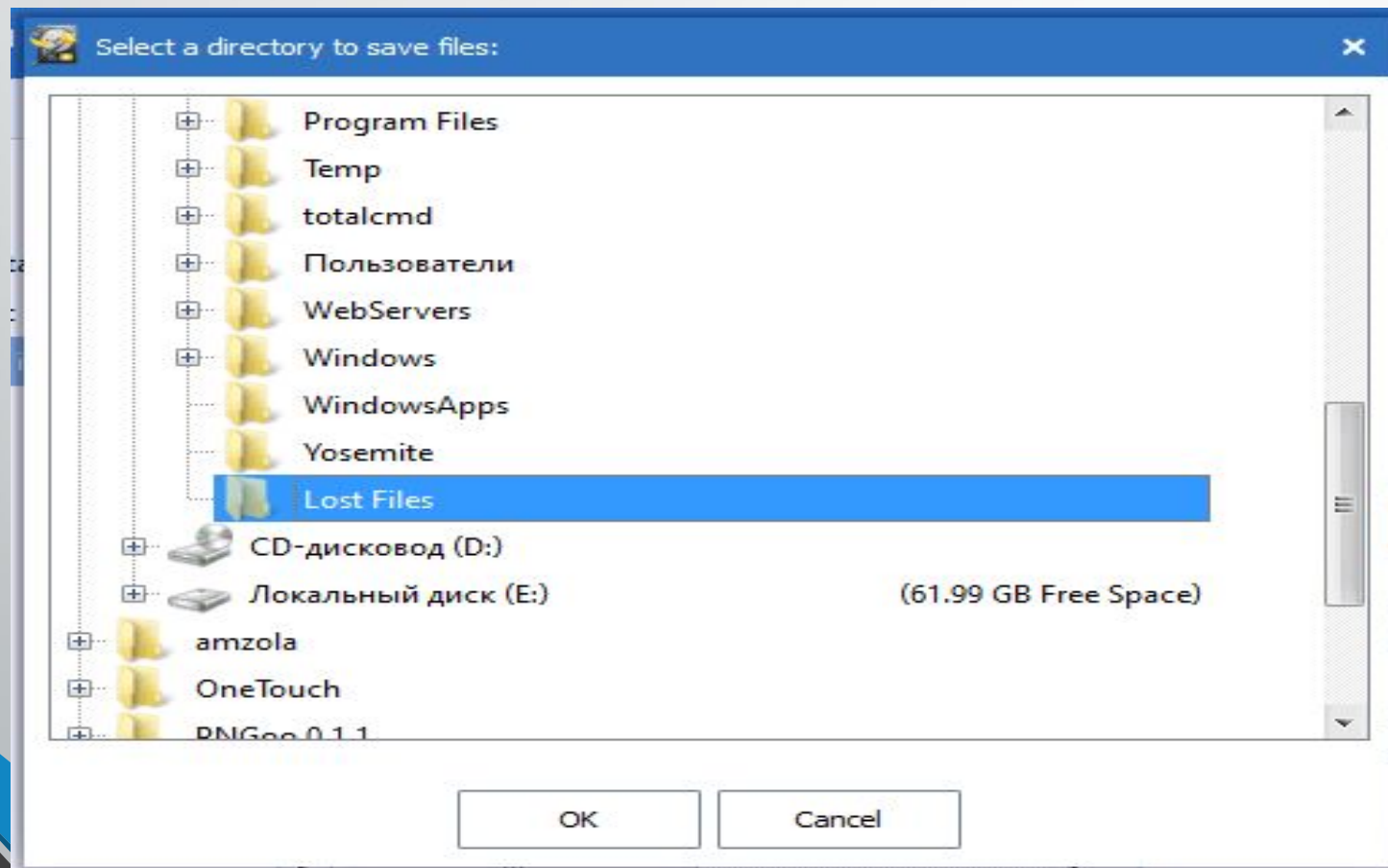
- На странице «Undelete Recovery» содержится список всех дисков, подключенных к компьютеру. Чтобы начать процесс восстановления, нужно выбрать диск и нажать «Scan».



- Удаленные папки и файлы будут отмечены красным X, как показано на изображении ниже. Для восстановления нужно отметить соответствующую папку (или файл) и нажать кнопку «Save».

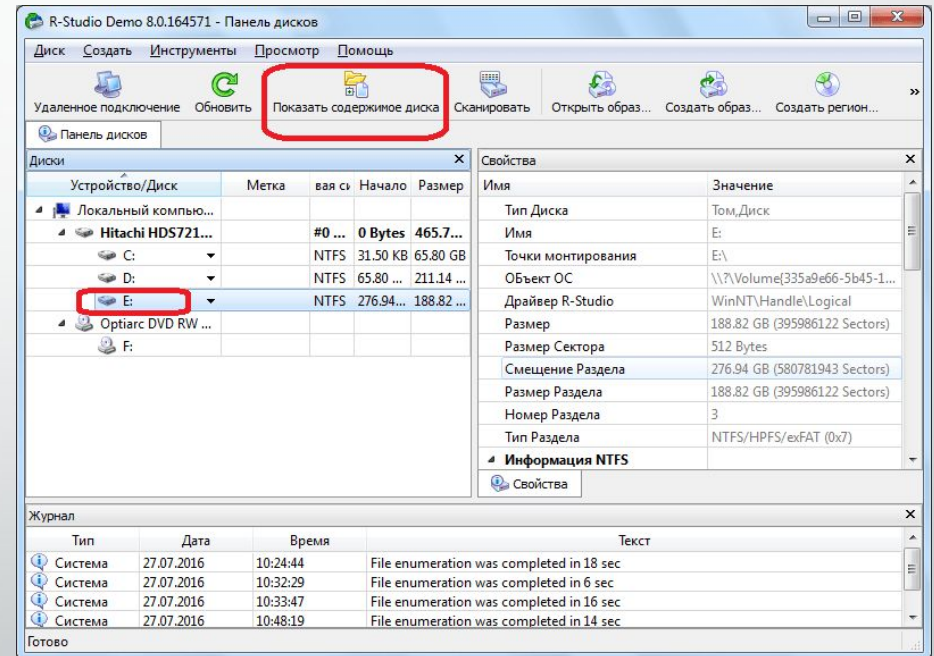


- Диалоговое окно «Save Files» предложит выбрать место для сохранения восстанавливаемых файлов. Для этого я создал папку «Lost Files» в корне диска C. Чтобы продолжить восстановление, нужно нажать «ОК». В результате файлы были успешно восстановлены и сохранены в указанной папке на жестком диске.

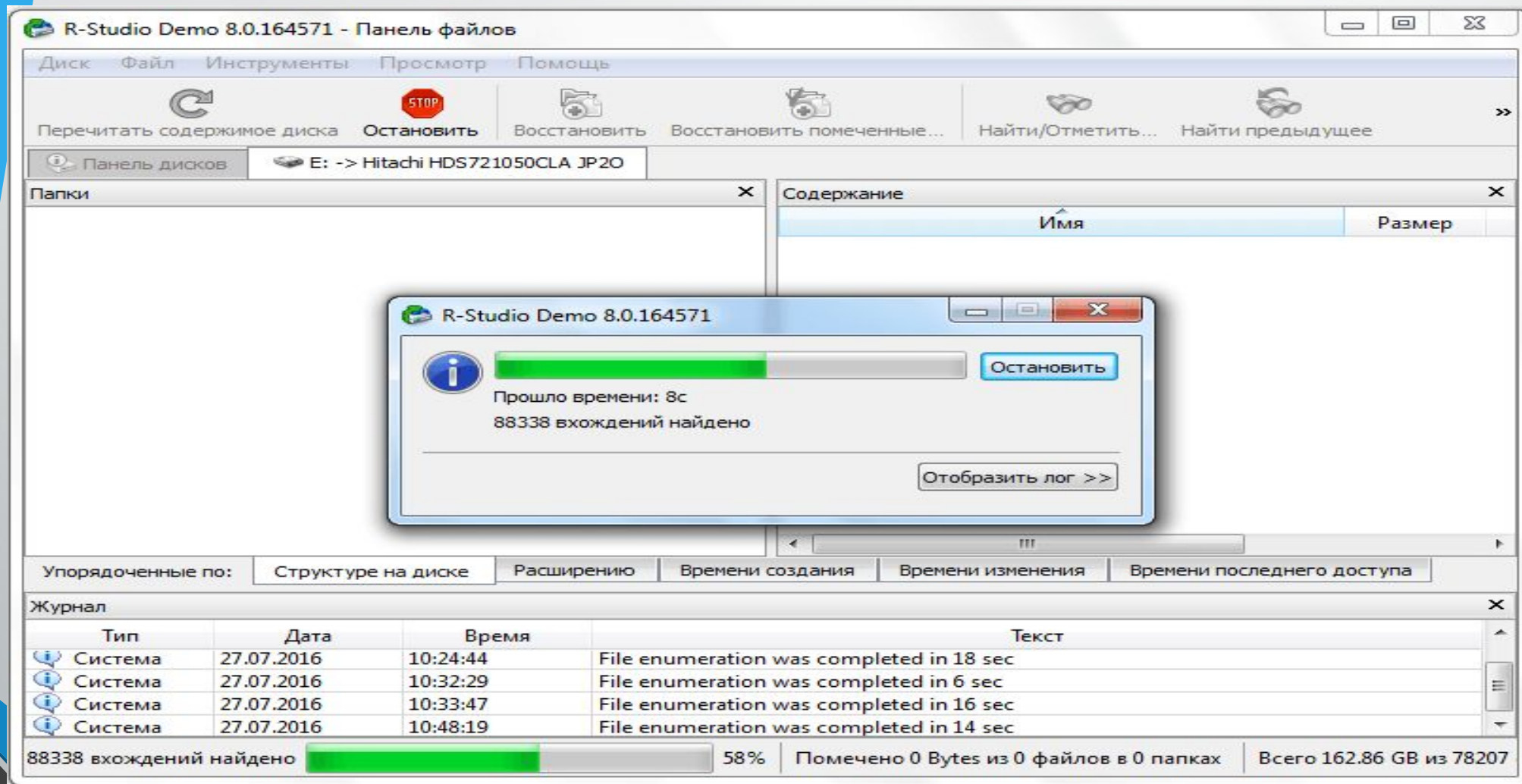


R-Studio

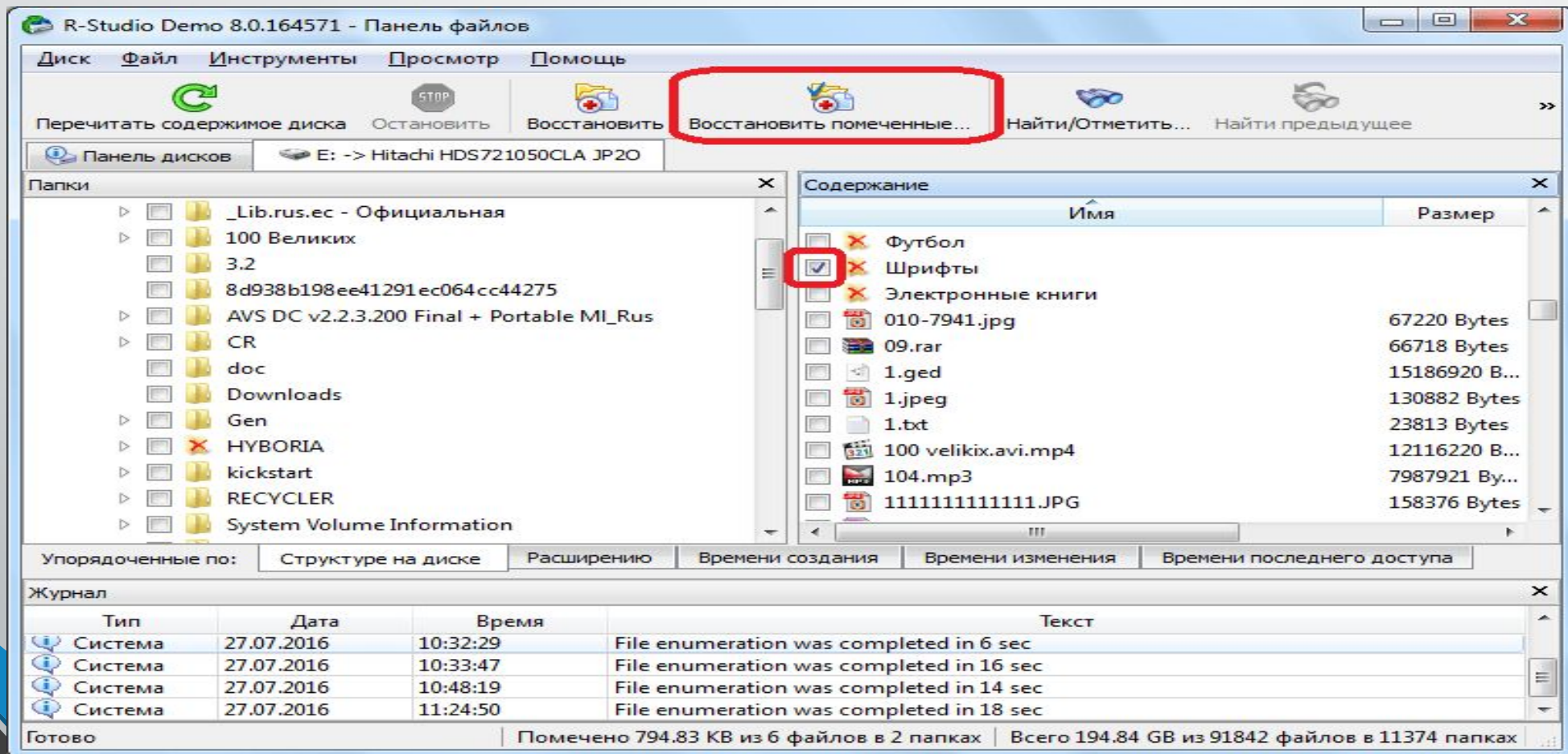
программа восстановления данных с жесткого диска, способна восстанавливать поврежденные вредоносными программами файлы. Используется в ОС Windows XP, Windows 7 и старше. Чтобы найти удаленный файл, можно сначала просмотреть содержимое раздела диска, где он раньше размещался. Для этого, кликаем по наименованию раздела диска, и жмем на кнопку в верхней панели «Показать содержимое диска».



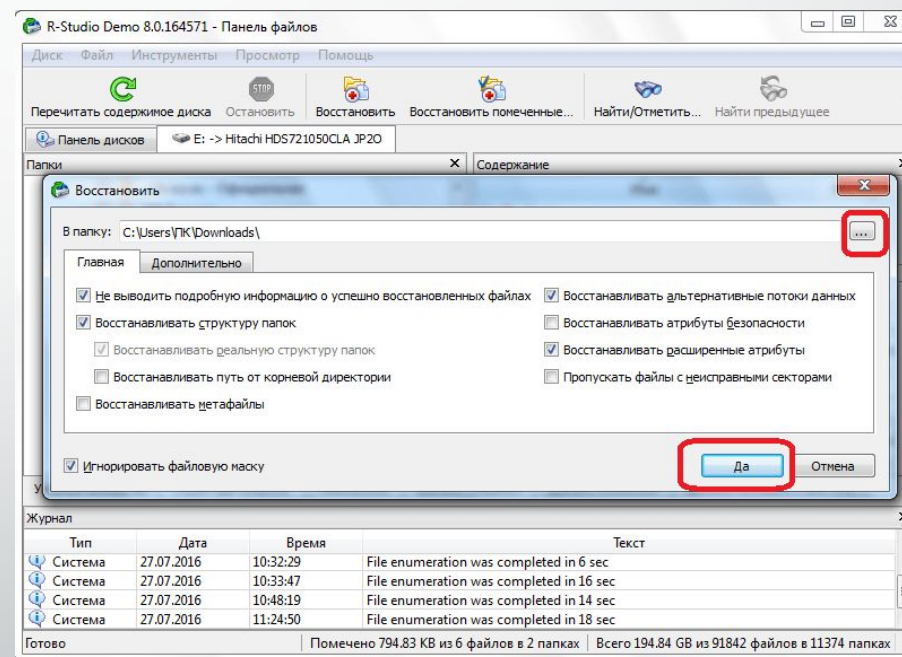
- Начинается обработка информации с диска программой R-Студิโอ.



- После того, как процесс обработки произошёл, мы можем наблюдать файлы и папки расположенные в данном разделе диска, в том числе и удаленные. Удаленные папки и файлы помечены красным крестиком.
- Для того, чтобы восстановить нужную папку или файл, помечаем его галочкой, и жмем кнопку на панели инструментов «Восстановить помеченные».

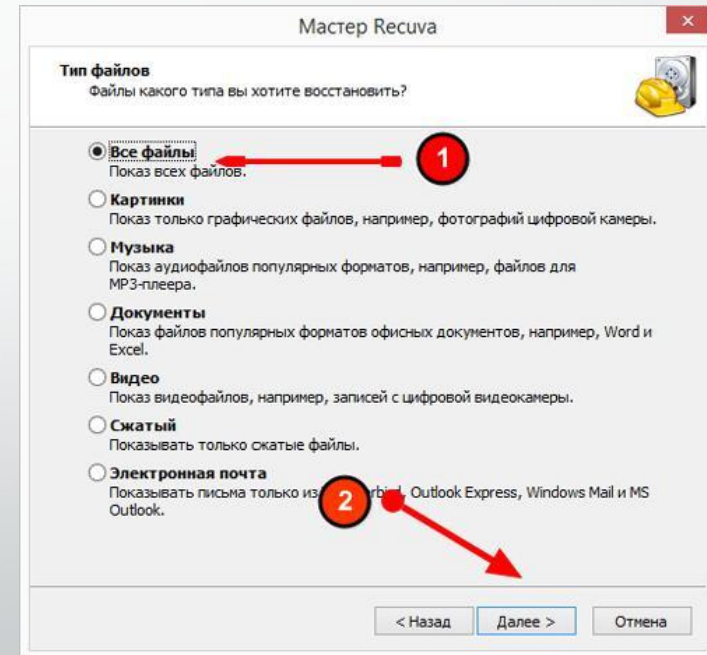


- После этого, отрывается окно, в котором мы должны указать параметры восстановления. Самым важным является указание директории, куда будет восстановлена папка или файл. После того, как мы выбрали каталог сохранения, и при желании произвели другие настройки, жмем на кнопку «Да». После этого, файл восстанавливается в ту директорию, которую мы указали ранее.

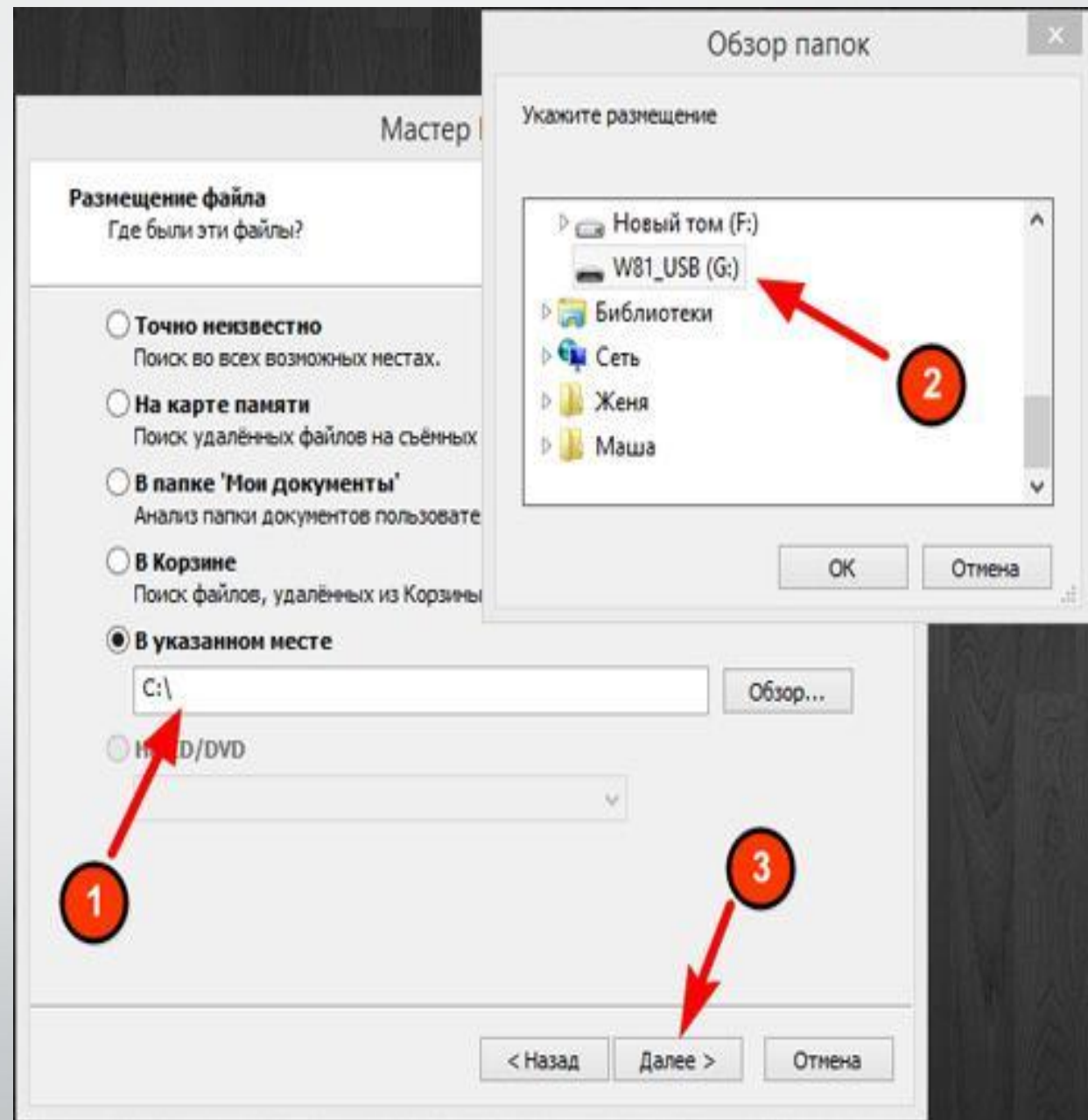


Recuva

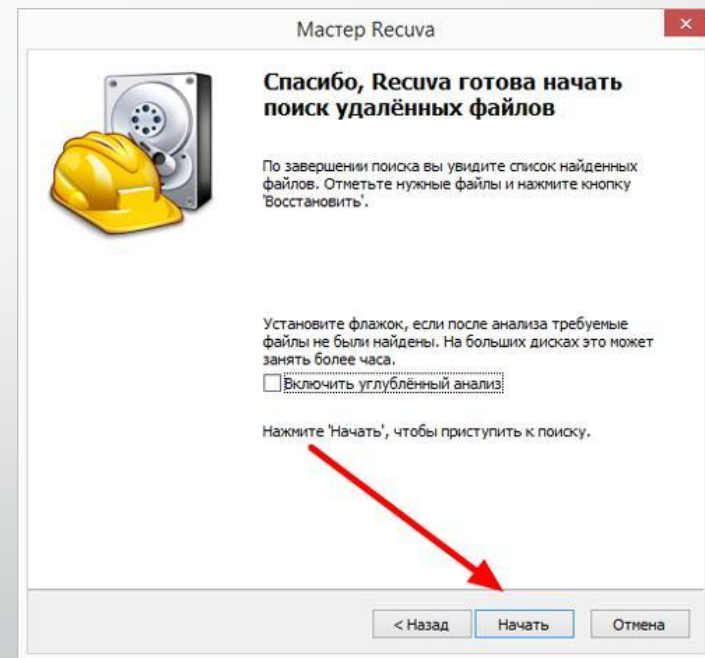
- бесплатная утилита позволяет восстановления дан-ных после очистки корзины и сбоя файловой. Можно выбрать восстановление только музыки, документов, изображений, видео файлов, архивированных файлов или почтовых файлов.



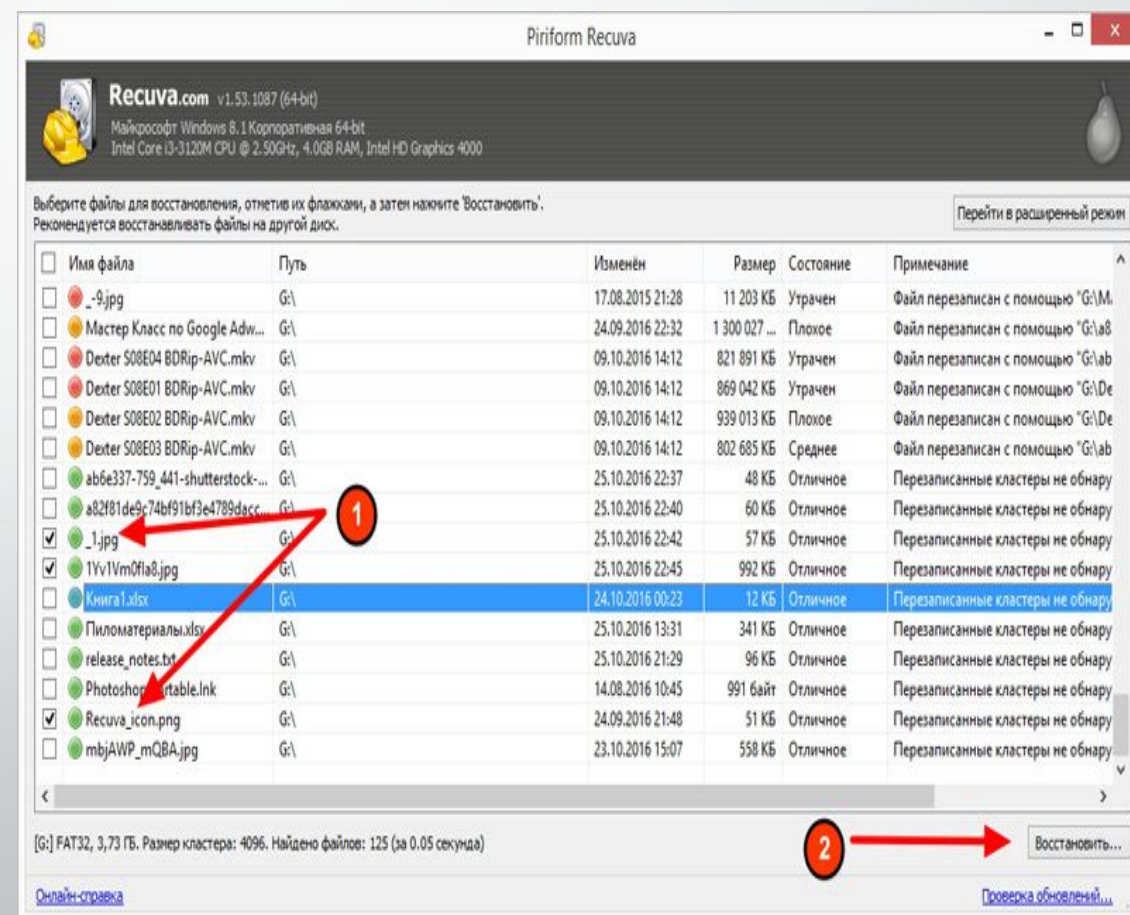
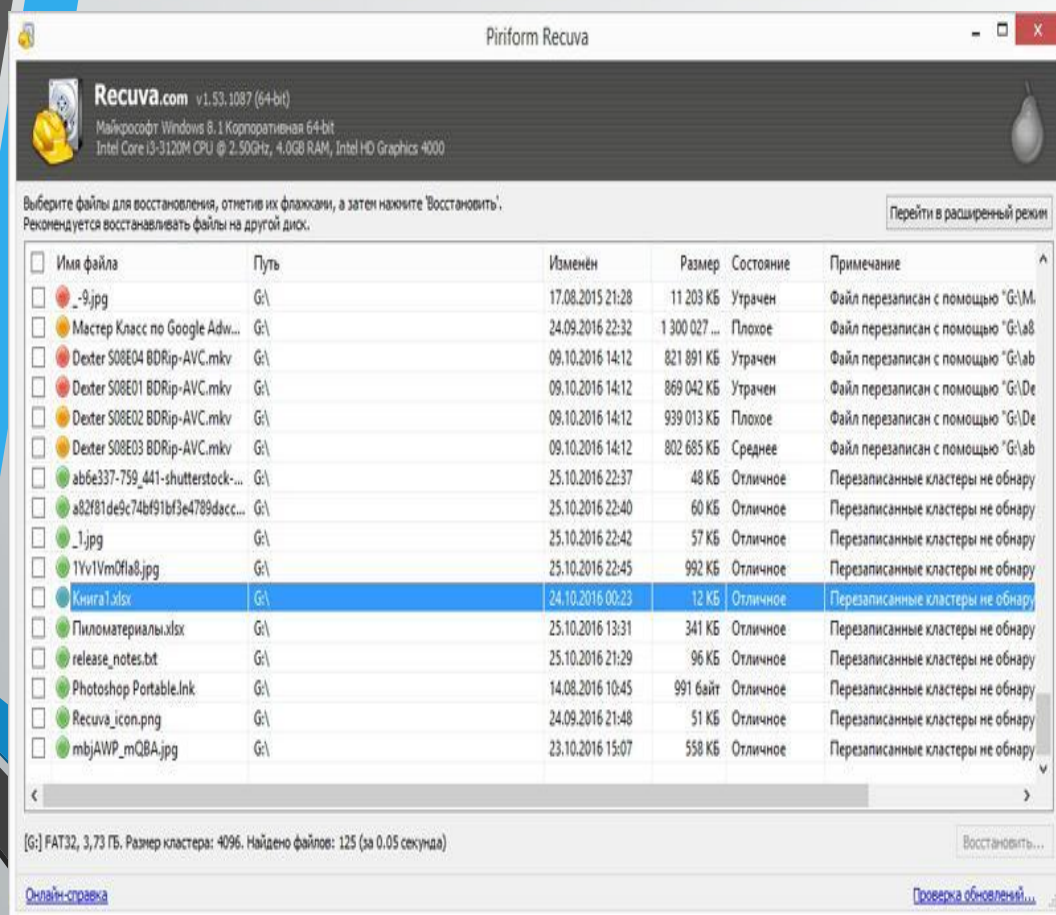
- Если вы точно знаете месторасположение удаленных файлов (в нашем примере — это флешка), выбирайте пятый пункт «В указанном месте», отмечайте двойным кликом в появившемся списке нужный диск/папку и нажимайте «Далее».



Recuva позволяет провести углубленный анализ



- После анализа помечаются группы файлов — красные (восстановить не получится), желтые (возможно частичное восстановление) и зеленые (могут быть восстановлены полностью).
- Отмечайте искомые файлы, нажимайте «Восстановить...» и выбирайте папку, куда будут помещены восстановленные файлы.

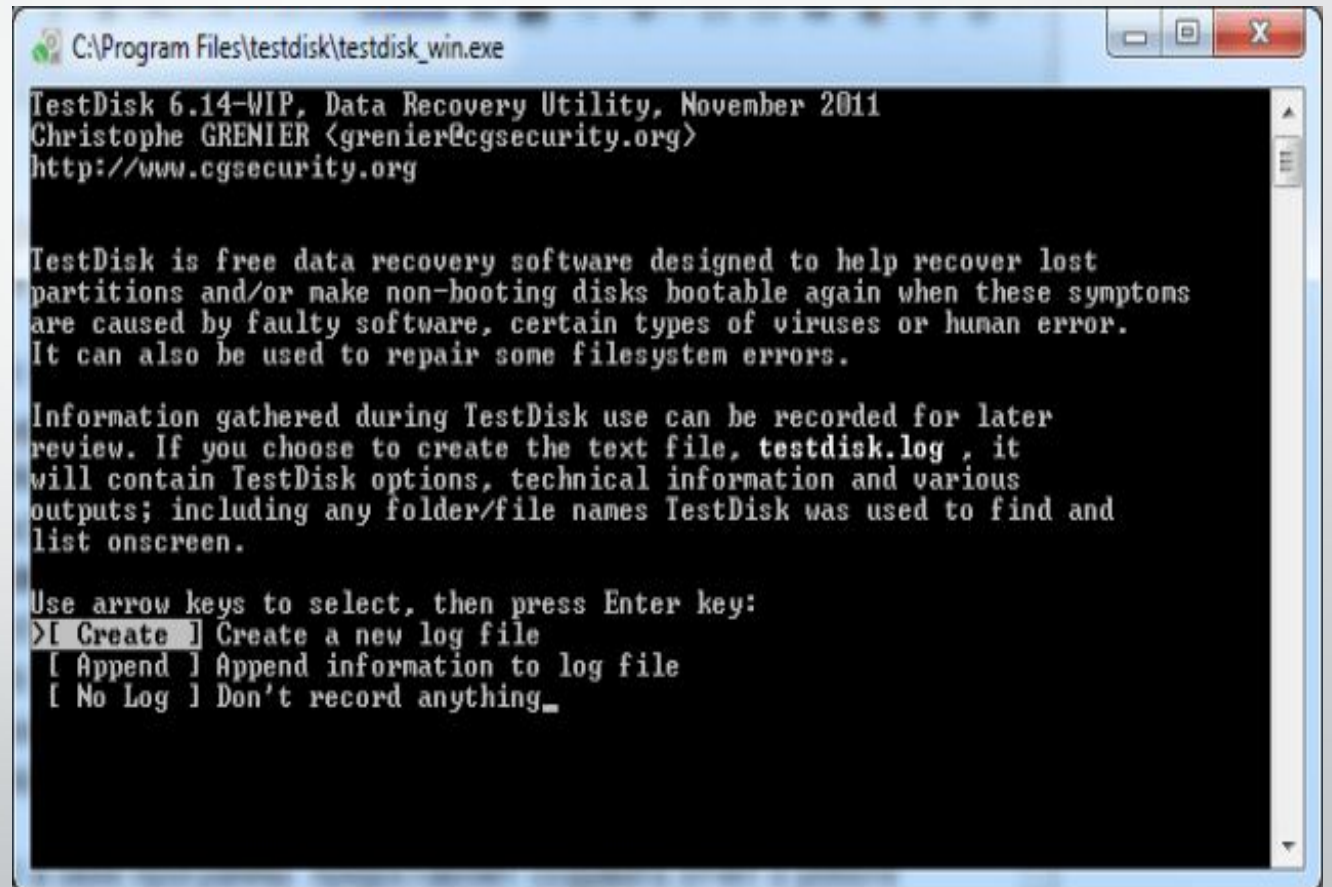


TestDisk и PhotoRec

- TestDisk —поддерживает огромное количество файловых форматов, позволяет восстановить данные с диска, на котором не загружается операционная система. Утилита может восстановить повреждённый загрузочный сектор или потерянные данные. В комплекте с ней используется программа PhotoRec для восстановления удаленных текстовых, графических и мультимедийных файлов.

Testdisk

- Программа позволяет восстановить поврежденный загрузочный сектор.
- Create a new log file - создать новый файл
- Append information to log file - добавить информацию в файл
- Dont record anything - ничего не записывать



```
C:\Program Files\testdisk\testdisk_win.exe

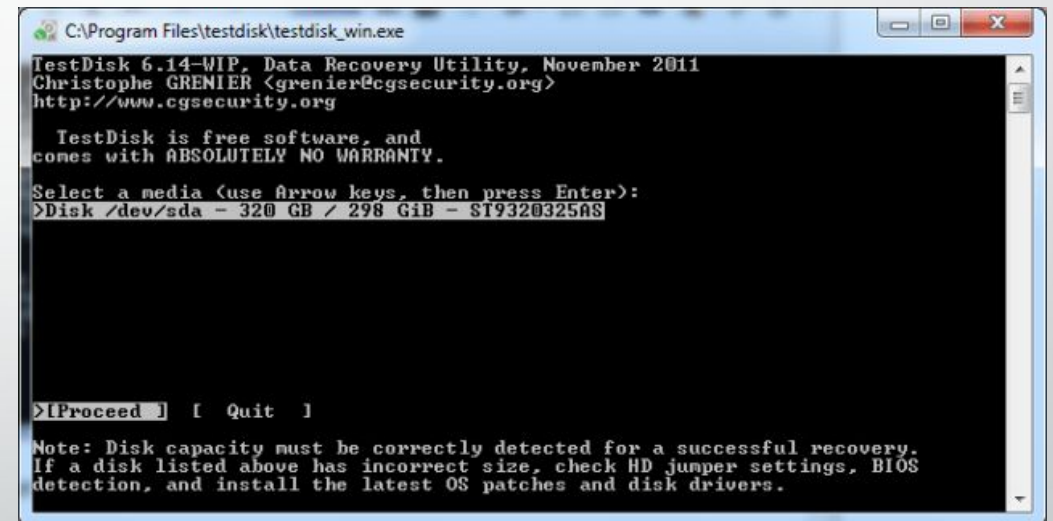
TestDisk 6.14-WIP, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

TestDisk is free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
>[ Create ] Create a new log file
[ Append ] Append information to log file
[ No Log ] Don't record anything_
```

- Осуществляется выбор диска (не только винчестеры, но и на съемных носителях)



```
C:\Program Files\testdisk\testdisk_win.exe
TestDisk 6.14-WIP, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

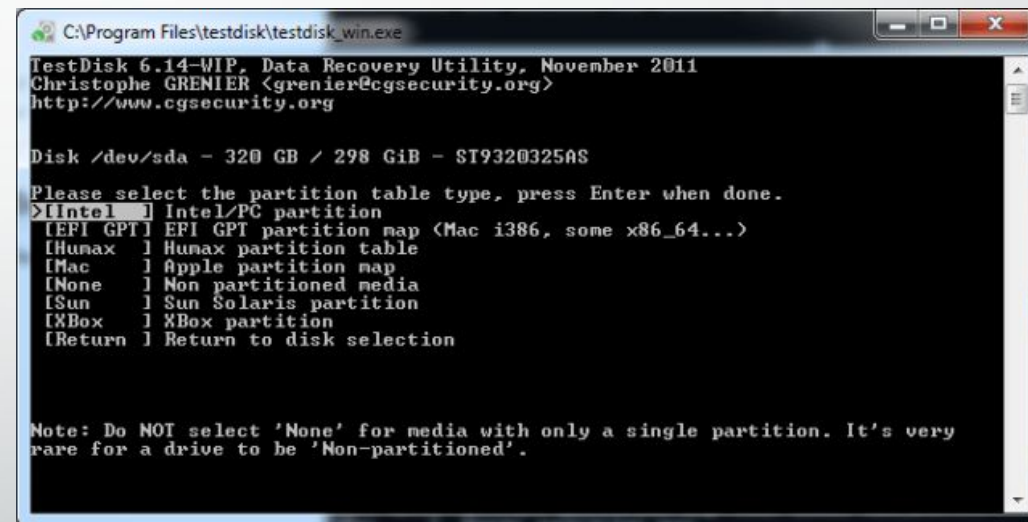
TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk /dev/sda - 320 GB / 298 GiB - ST9320325AS

>[Proceed] [Quit]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

- Программа предоставляет Таблицу разделов.



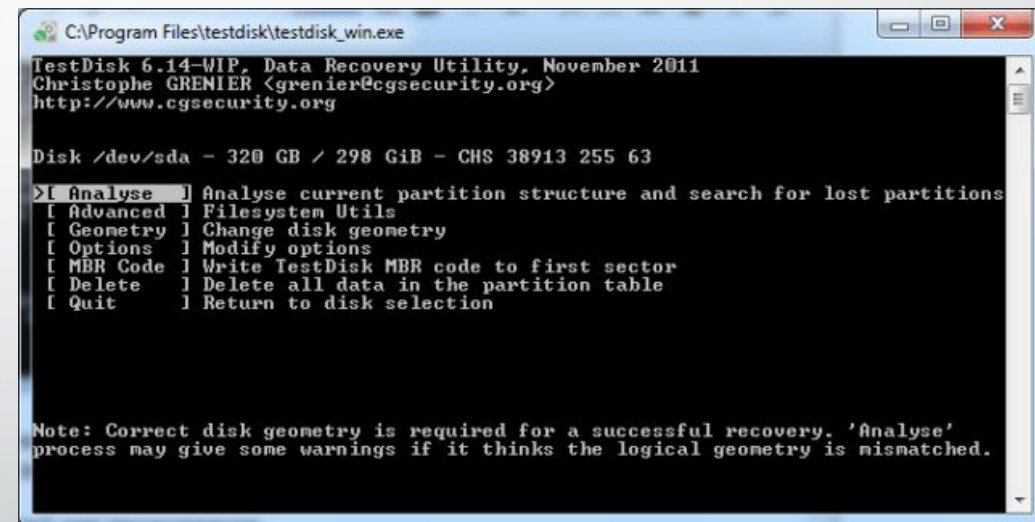
```
C:\Program Files\testdisk\testdisk_win.exe
TestDisk 6.14-WIP, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 320 GB / 298 GiB - ST9320325AS

Please select the partition table type, press Enter when done.
>[Intel] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Humax ] Humax partition table
[Mac ] Apple partition map
[None ] Non partitioned media
[Sun ] Sun Solaris partition
[XBox ] Xbox partition
[Return] Return to disk selection

Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.
```


- Чтобы произвести тест структуры разделов выбранного носителя информации, а также поиска пропавших файлов, следует выбрать пункт «Analyse». Когда появится результат, вы увидите информацию о диске. Теперь нужно в меню, расположенном в нижней части экрана выбрать Quick Search. Сразу после этого программа спросит, нужно ли осуществлять поиск разделов, созданных под Vista. Лучше всего согласиться и нажать кнопку «Y», что означает «Да».



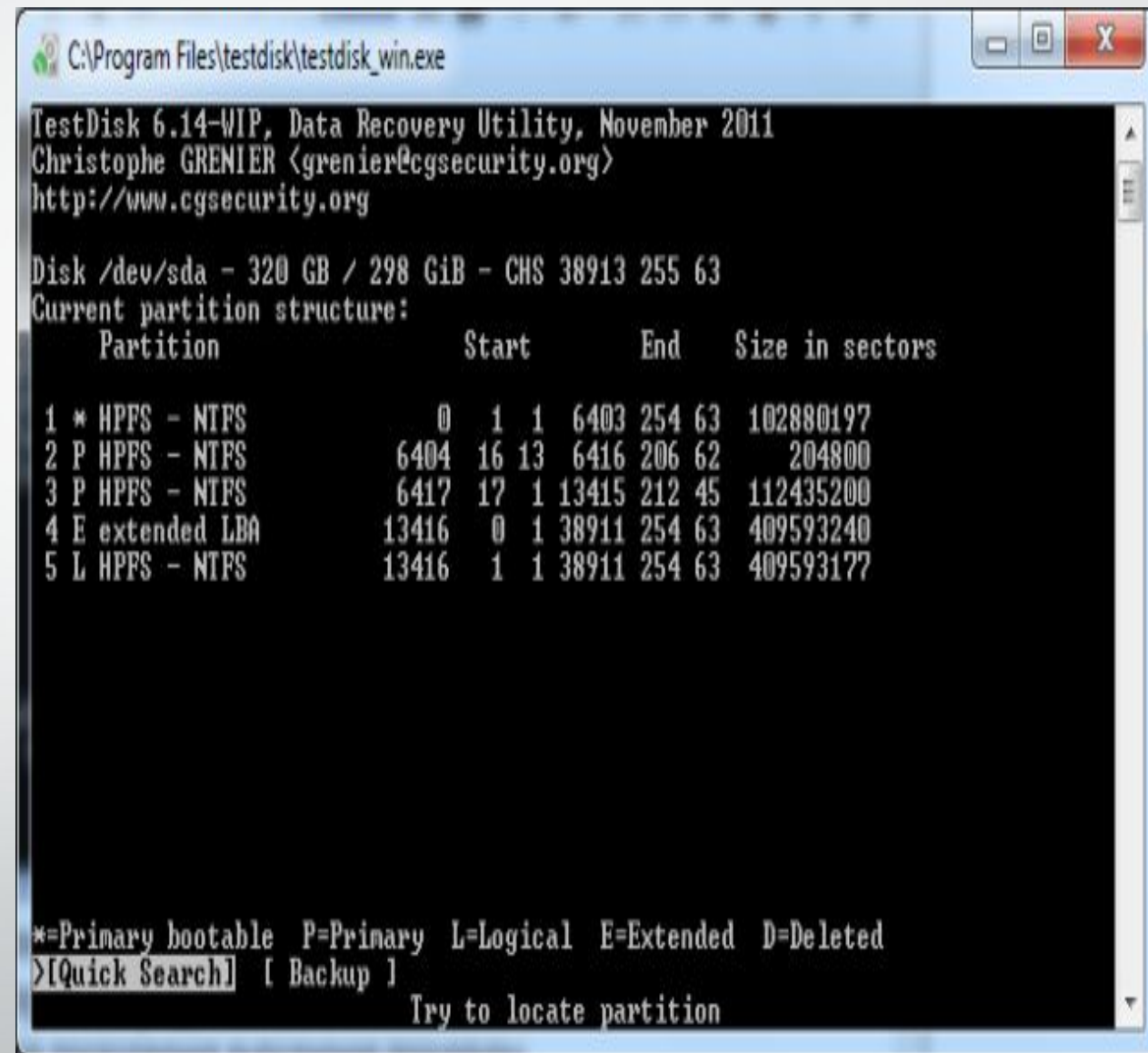
The screenshot shows a Windows-style window titled "C:\Program Files\testdisk\testdisk_win.exe". The window contains a black terminal-like area with white text. At the top, it says "TestDisk 6.14-WIP, Data Recovery Utility, November 2011" followed by "Christophe GRENIER <grenier@cgsecurity.org>" and "http://www.cgsecurity.org". Below this, it displays "Disk /dev/sda - 320 GB / 298 GiB - CHS 38913 255 63". A menu is shown with "Analyse" selected and highlighted. The menu options are: "Analyse" (Analyse current partition structure and search for lost partitions), "Advanced" (Filesystem Utils), "Geometry" (Change disk geometry), "Options" (Modify options), "MBR Code" (Write TestDisk MBR code to first sector), "Delete" (Delete all data in the partition table), and "Quit" (Return to disk selection). At the bottom, a note states: "Note: Correct disk geometry is required for a successful recovery. 'Analyse' process may give some warnings if it thinks the logical geometry is mismatched."

```
C:\Program Files\testdisk\testdisk_win.exe
TestDisk 6.14-WIP, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 320 GB / 298 GiB - CHS 38913 255 63
> [ Analyse ] Analyse current partition structure and search for lost partitions
[ Advanced ] Filesystem Utils
[ Geometry ] Change disk geometry
[ Options ] Modify options
[ MBR Code ] Write TestDisk MBR code to first sector
[ Delete ] Delete all data in the partition table
[ Quit ] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

- Особенность этой программы - каталоги с русским наименованием изображаются некорректно.
- После восстановления одного из разделов необходимо перезагрузить компьютер.



The screenshot shows the TestDisk 6.14-WIP interface. The title bar indicates the file path: C:\Program Files\testdisk\testdisk_win.exe. The main window displays the following information:

```
TestDisk 6.14-WIP, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

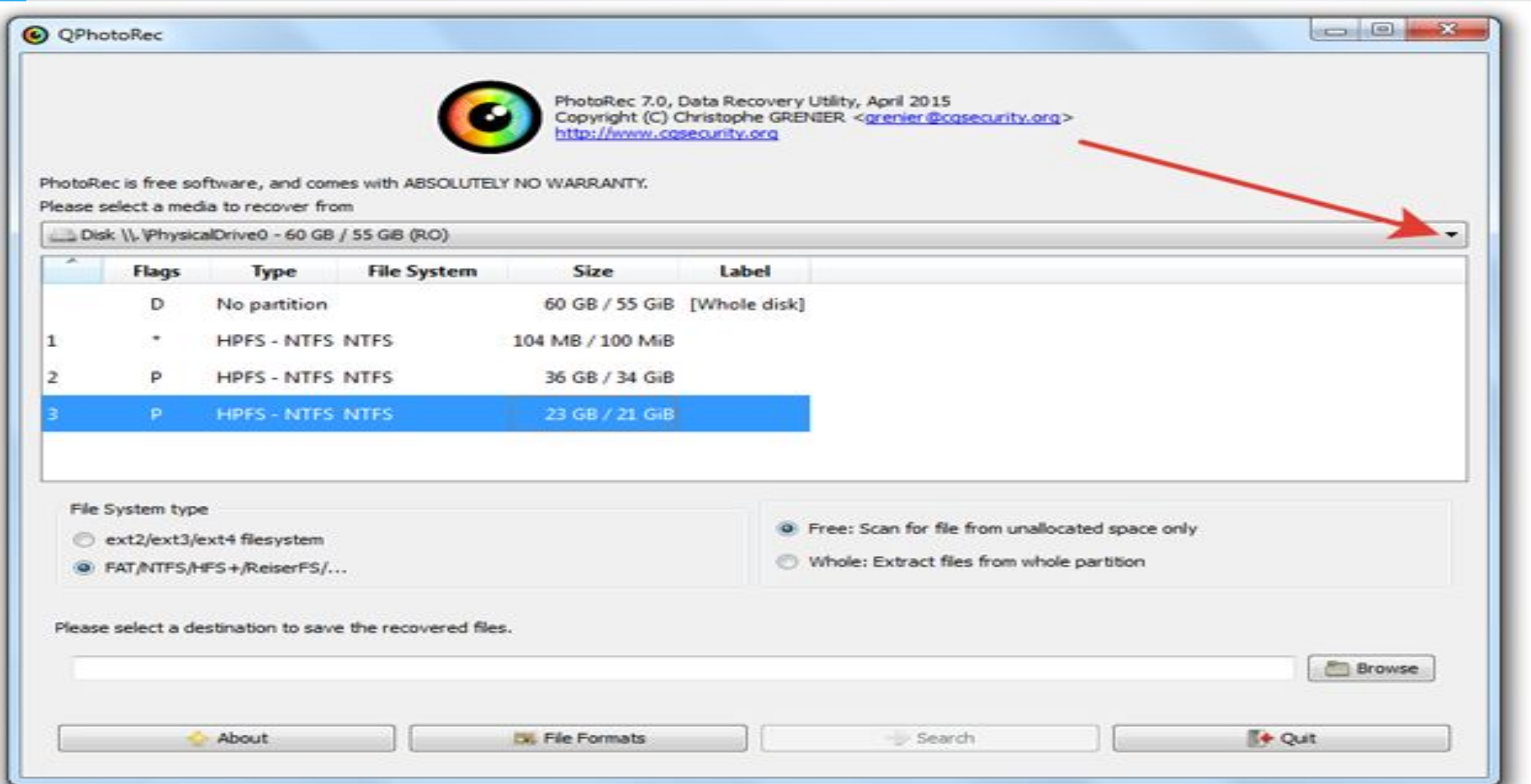
Disk /dev/sda - 320 GB / 298 GiB - CHS 38913 255 63
Current partition structure:
```

Partition	Start	End	Size in sectors
1 * HPFS - NTFS	0 1 1 6403 254 63		102880197
2 P HPFS - NTFS	6404 16 13 6416 206 62		204800
3 P HPFS - NTFS	6417 17 1 13415 212 45		112435200
4 E extended LBA	13416 0 1 38911 254 63		409593240
5 L HPFS - NTFS	13416 1 1 38911 254 63		409593177

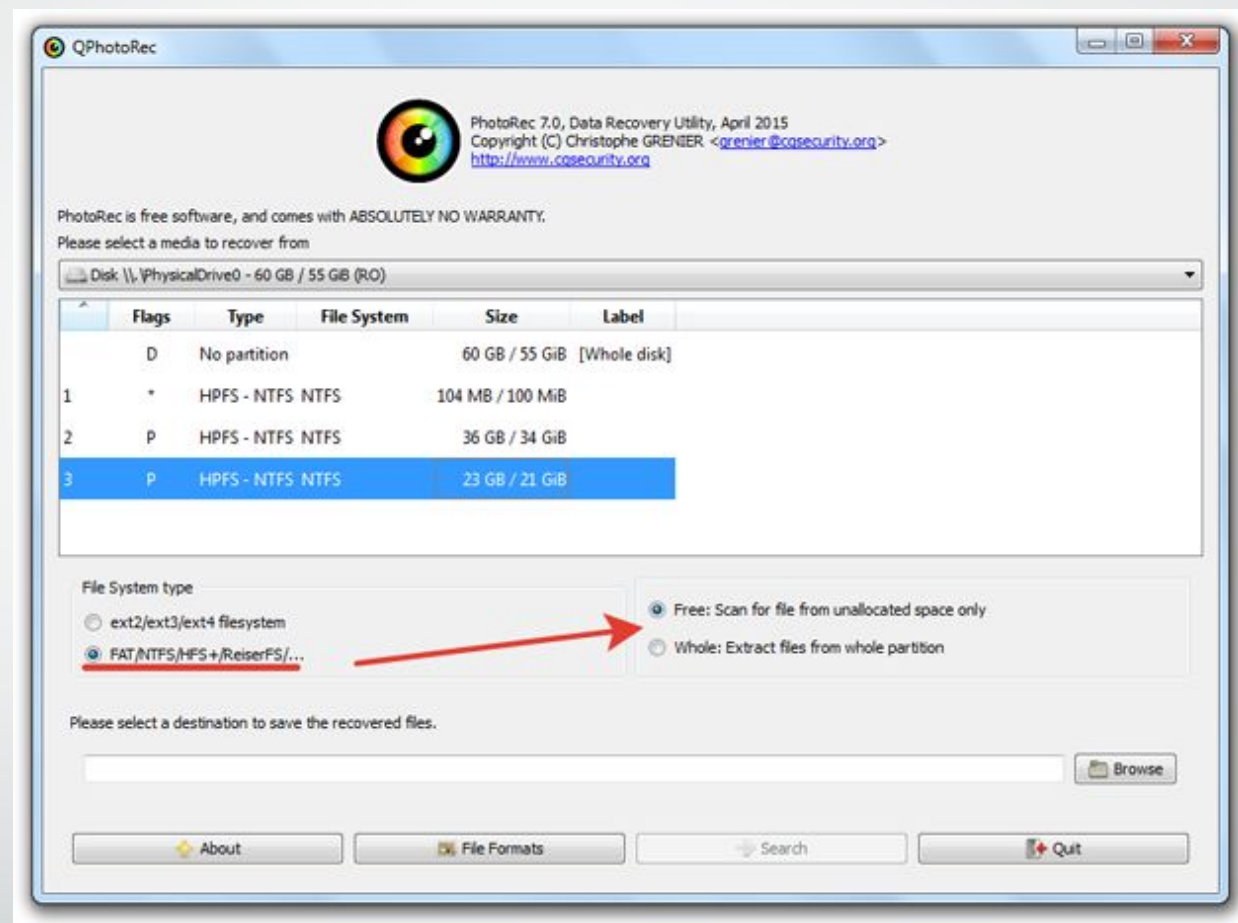
At the bottom, there is a legend and navigation options:

```
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
>[Quick Search] [Backup]
Try to locate partition
```

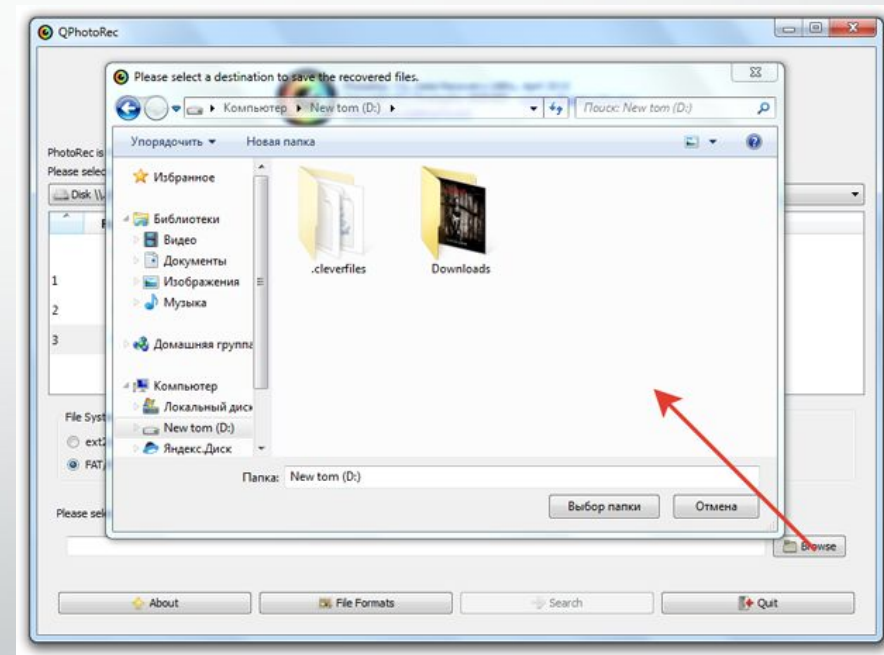
PhotoRec



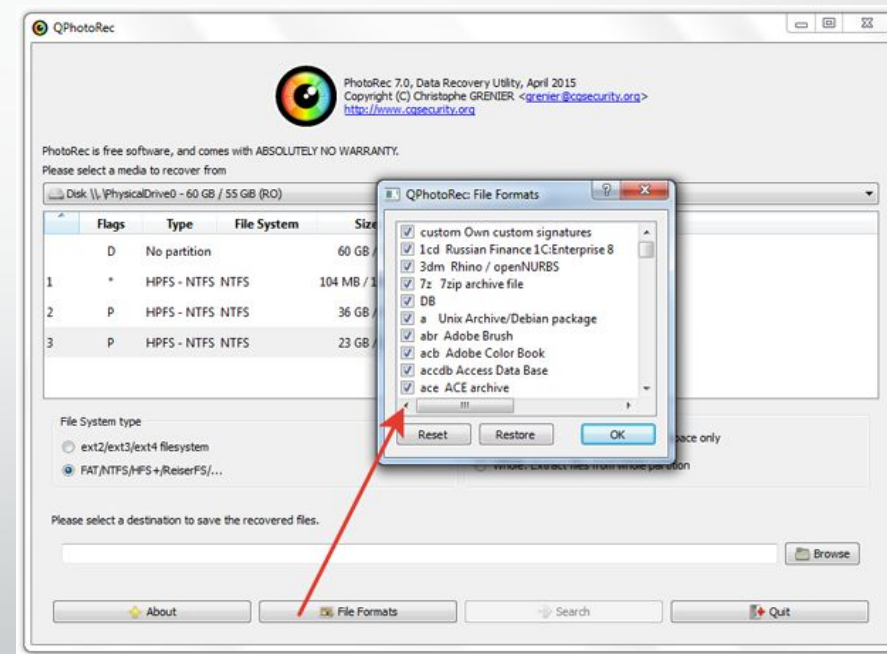
- Рядом выберите режим сканирования – Free или Whole. Полное сканирование (Whole) займет намного больше времени, эффективность восстановления будет выше.



- Нажмите «Browse» и укажите папку, в которую следует сохранять найденные файлы.



- Программа позволяет восстанавливать данные по формату.



- Нажмите «Search», чтобы запустить поиск файлов. Программа найдет и восстановит данные в ту папку, которую вы указали. Вы не можете выбирать, какие файлы следует сохранить, как в других программах.

