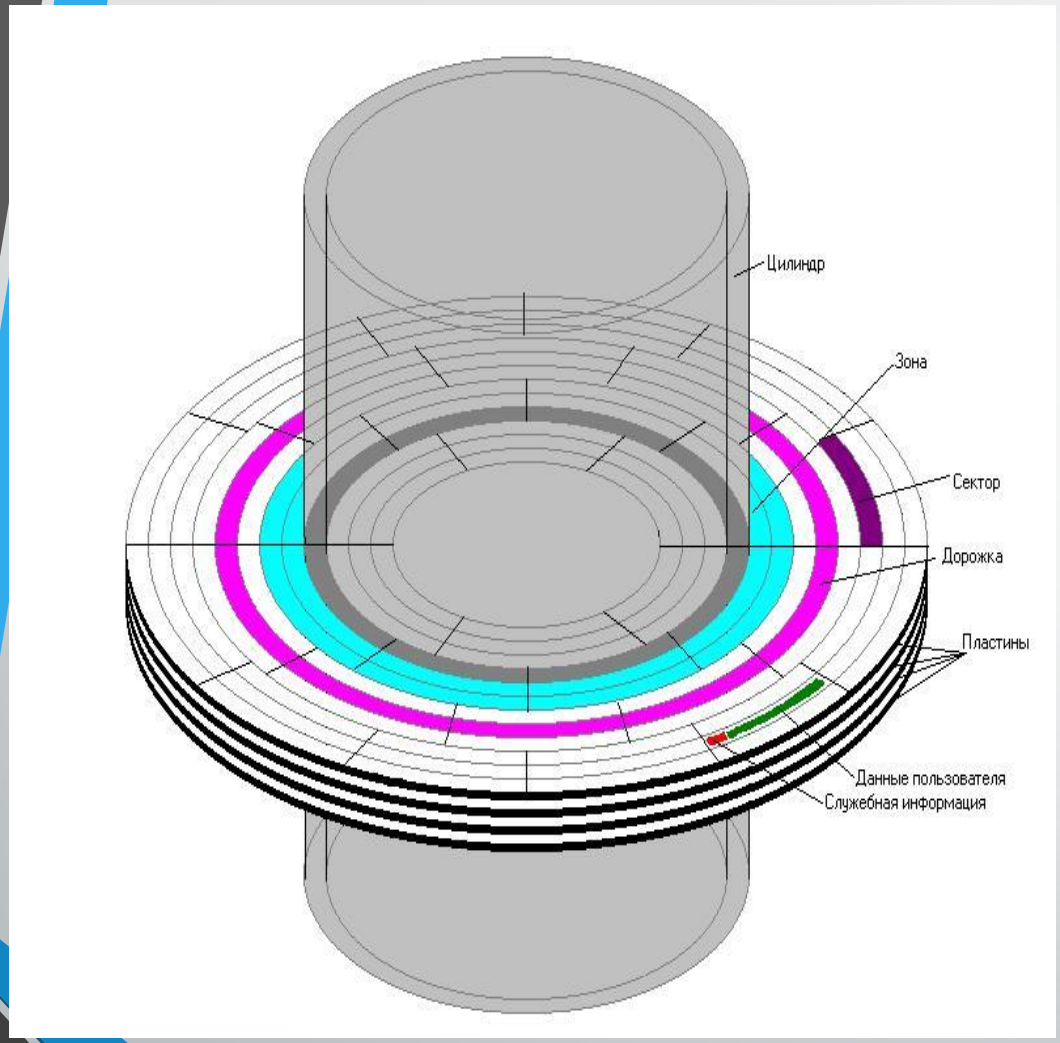
Фиксация остаточных данных при расследовании компьютерных преступлений

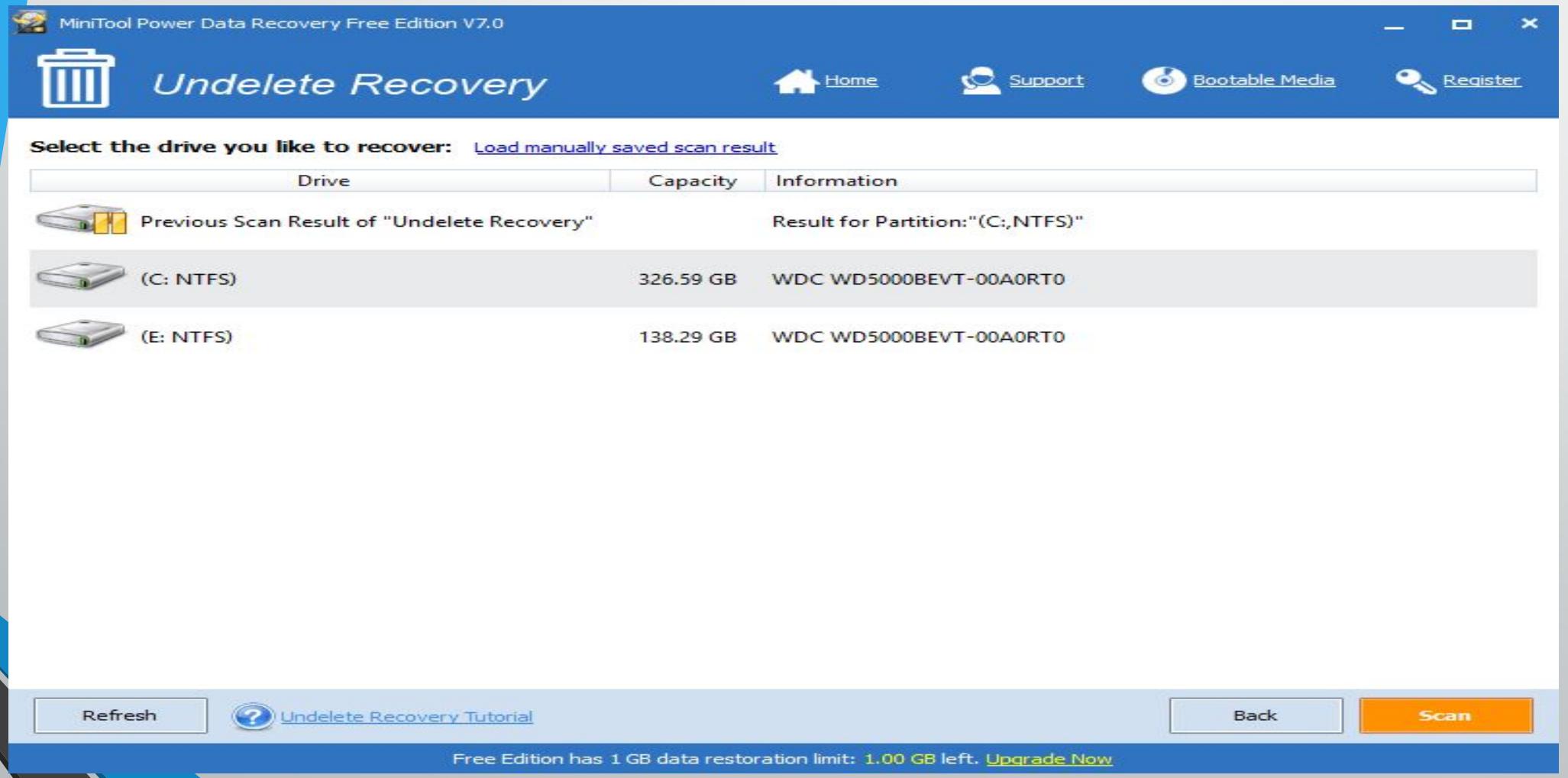


- Остаточные данные – информация на записывающем устройстве, оставшаяся после ее формального удаления.

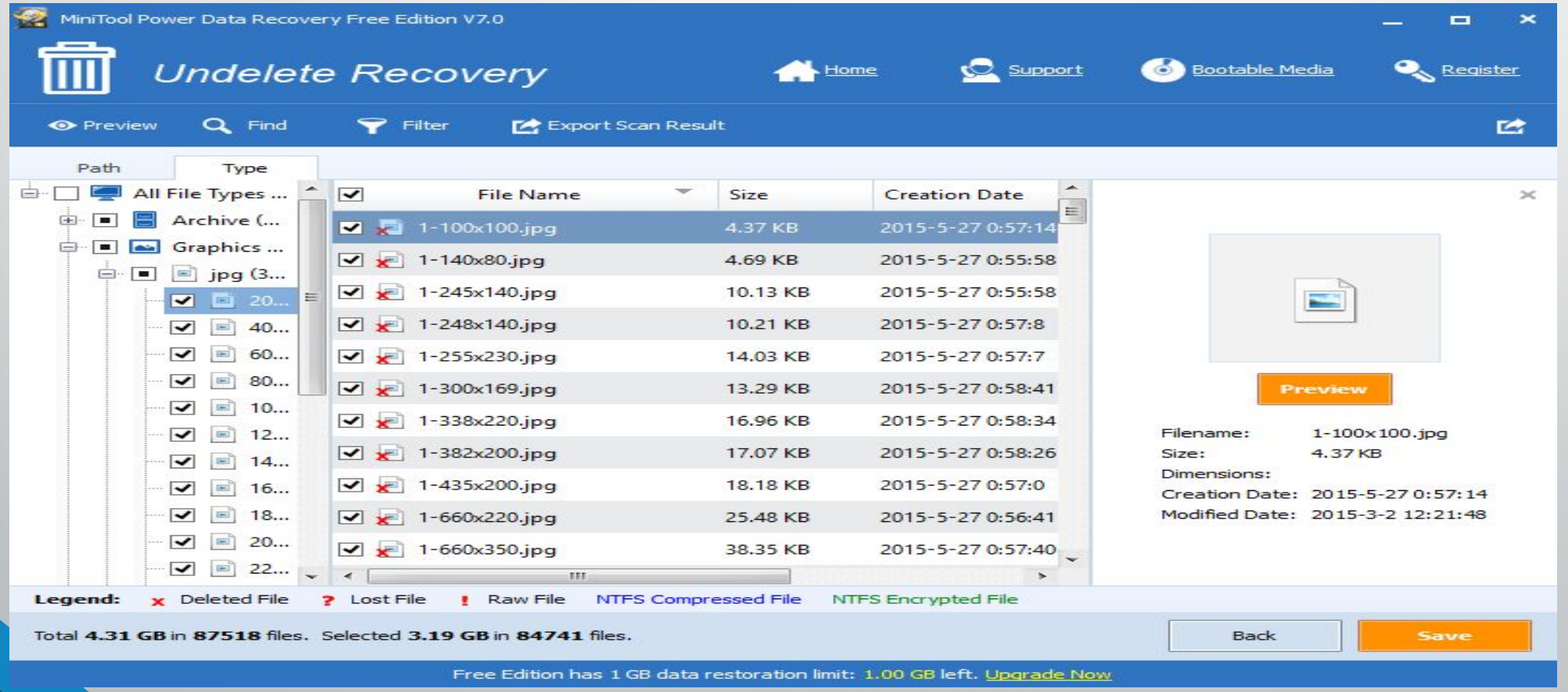
Minitool Power Data Recovery

- используется при восстанов-лении данных на повреждённых, неисправных жёстких дисках, отличается наиболее полным сканированием.

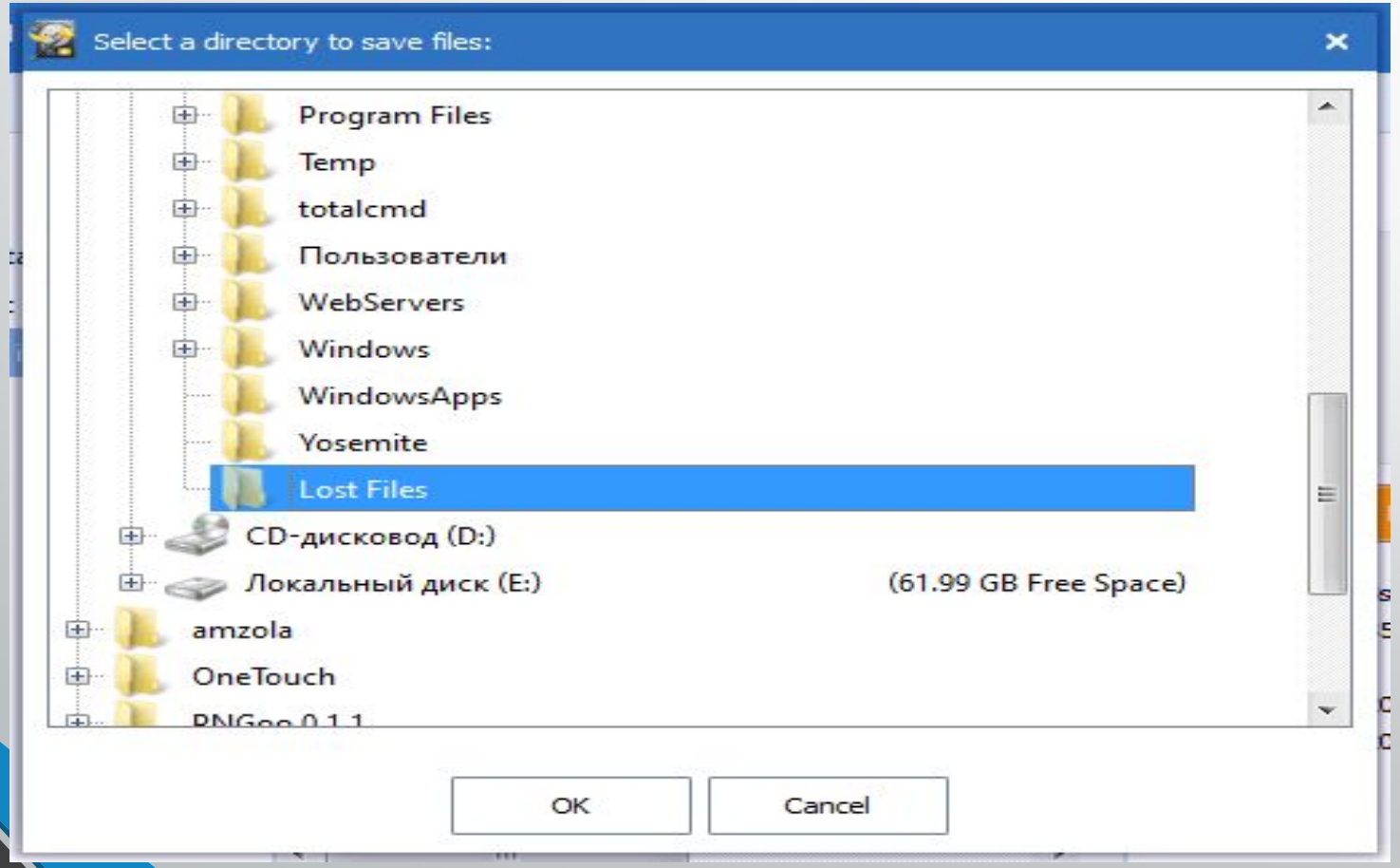
- На странице «Undelete Recovery» содержится список всех дисков, подключенных к компьютеру. Чтобы начать процесс восстановления, нужно выбрать диск и нажать «Scan».



- 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».

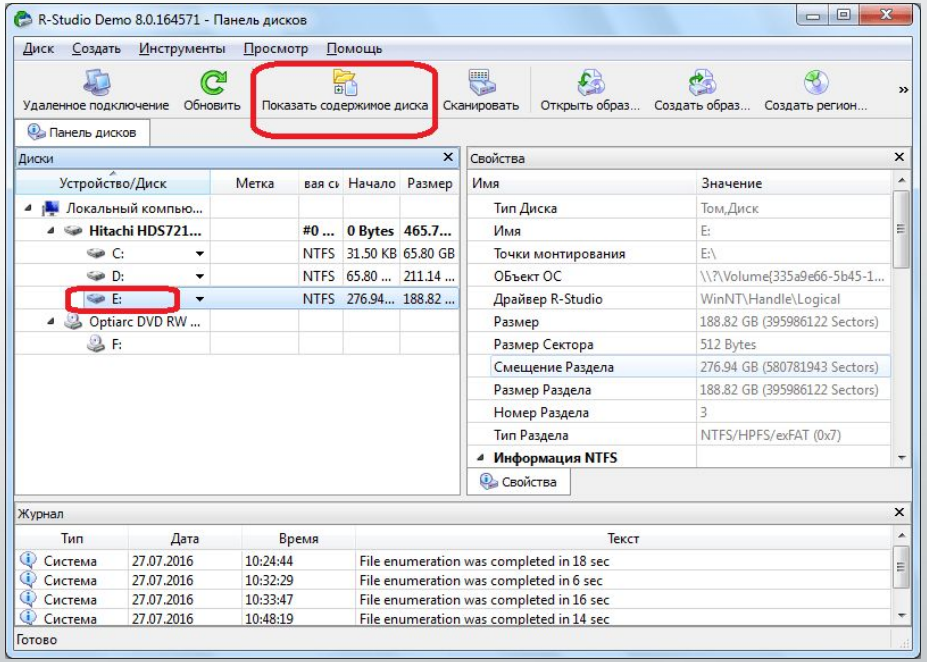


- Диалоговое окно «Save Files» предложит выбрать место для сохранения восстанавливаемых файлов. Для этого я создал папку «Lost Files» в корне диска C. Чтобы продолжить восстановление, нужно нажать «OK». В результате файлы были успешно восстановлены и сохранены в указанной папке на жестком диске.

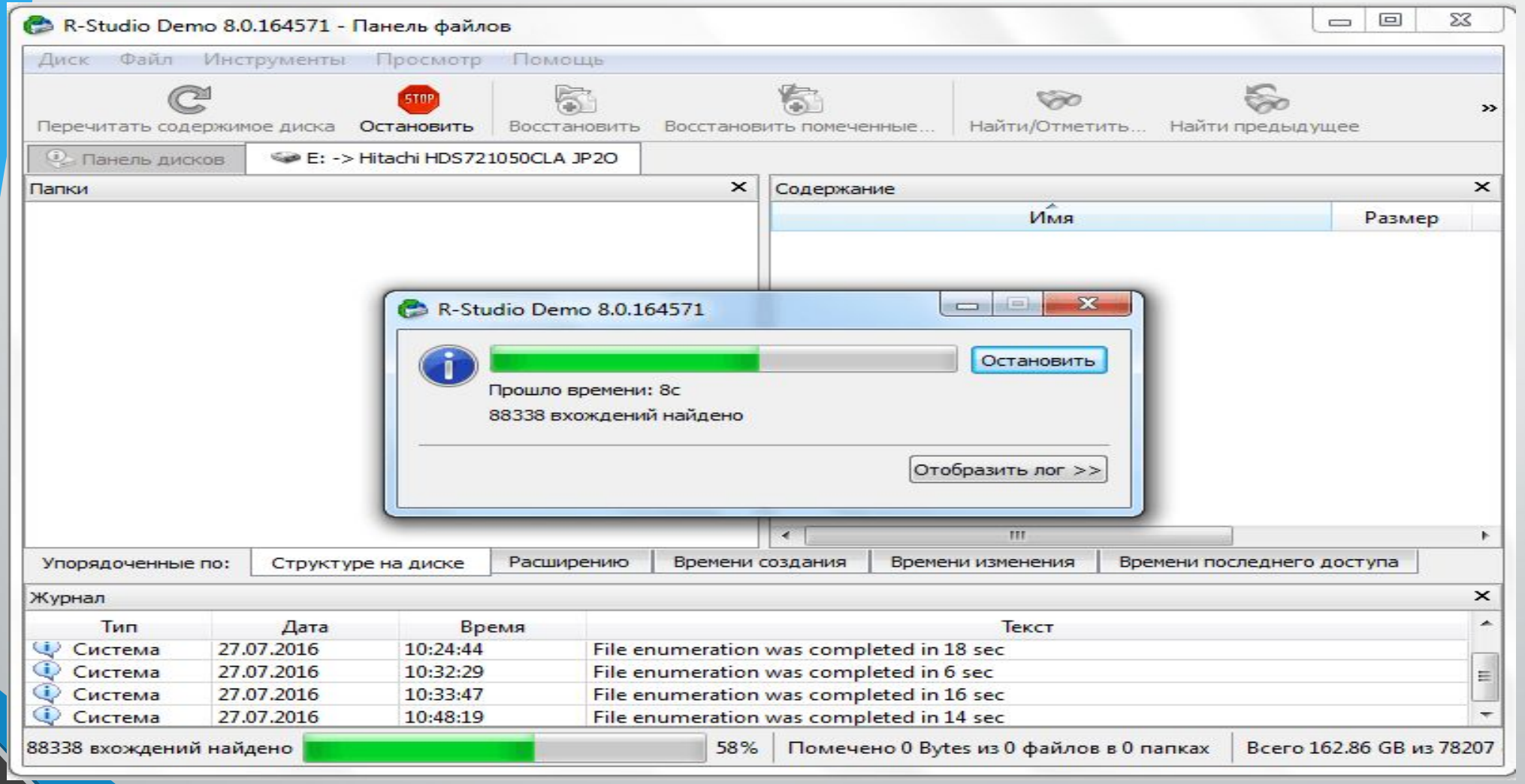


R-Studio

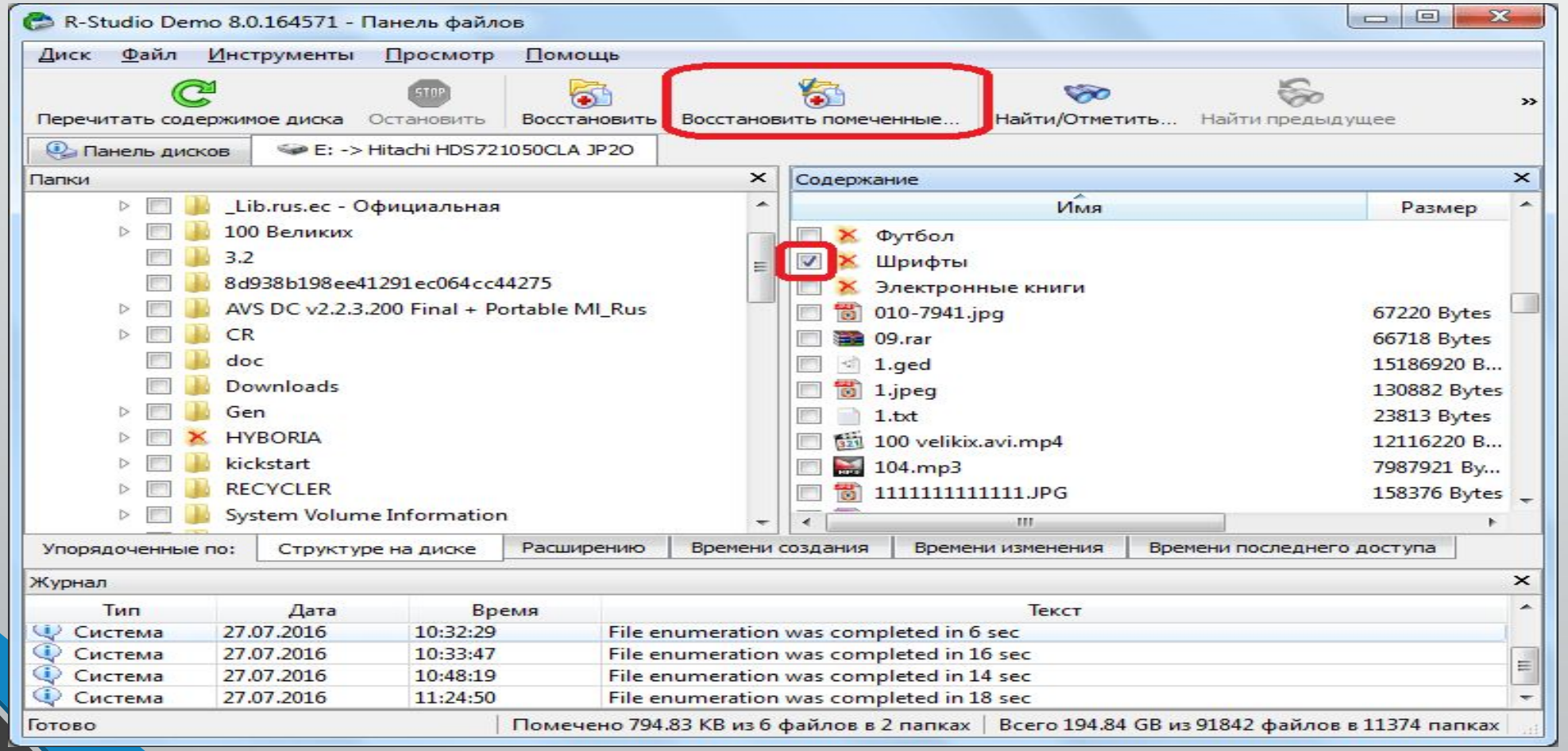
- программа восстановления данных с жесткого диска, способна восстанавливать поврежденные вредоносными программами файлы. Используется в ОС Windows XP, Windows 7 и старше. Чтобы найти удаленный файл, можно сначала просмотреть содержимое раздела диска, где он раньше размещался. Для этого, кликаем по наименованию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



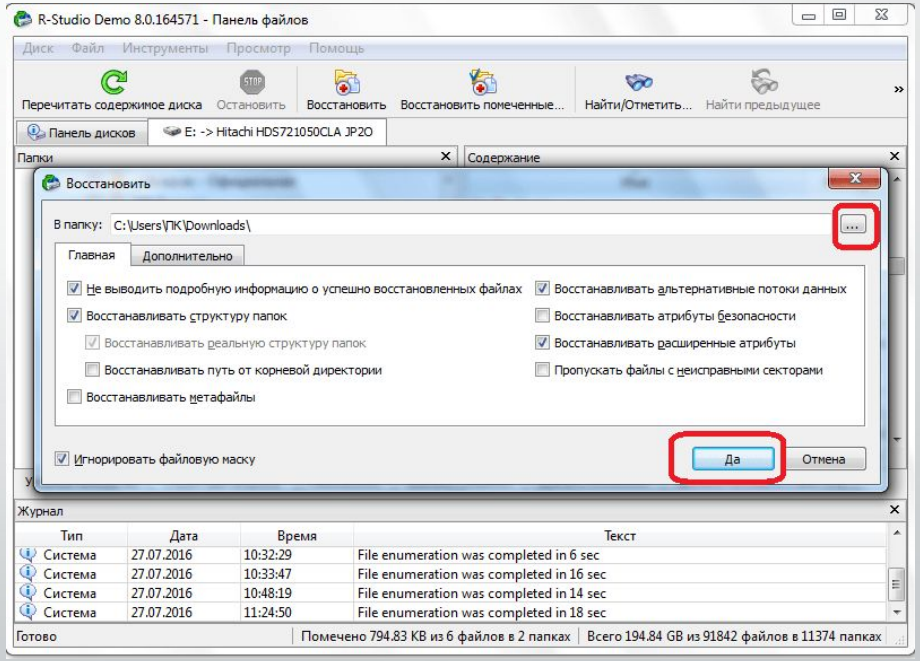
- Начинается обработка информации с диска программой Р-Студио.



- После того, как процесс обработки произошел, 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».

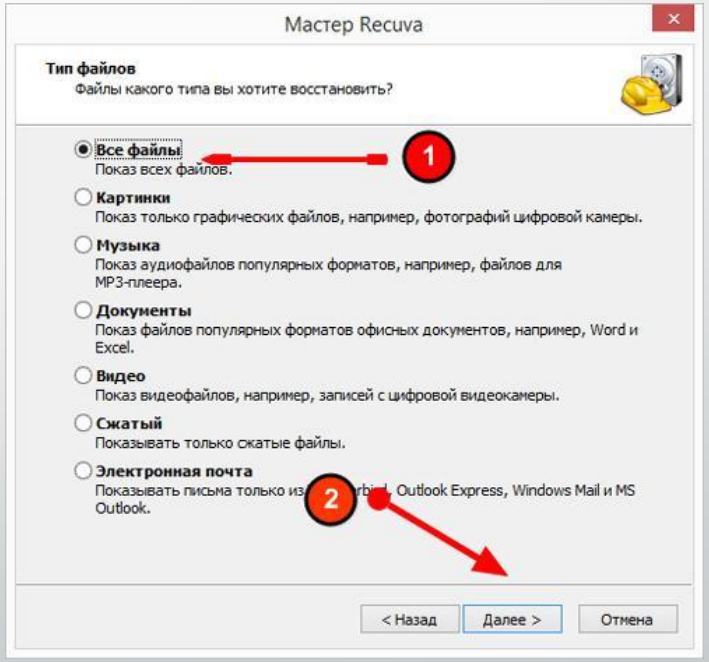


- После этого, отрывается окно, в котором мы должны указать параметры восстановления. Самым важным является указание директории, куда будет восстановлена папка или файл. После того, как мы выбрали каталог сохранения, и при желании произвели другие настройки, жмем на кнопку «Да». После этого, файл восстанавливается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

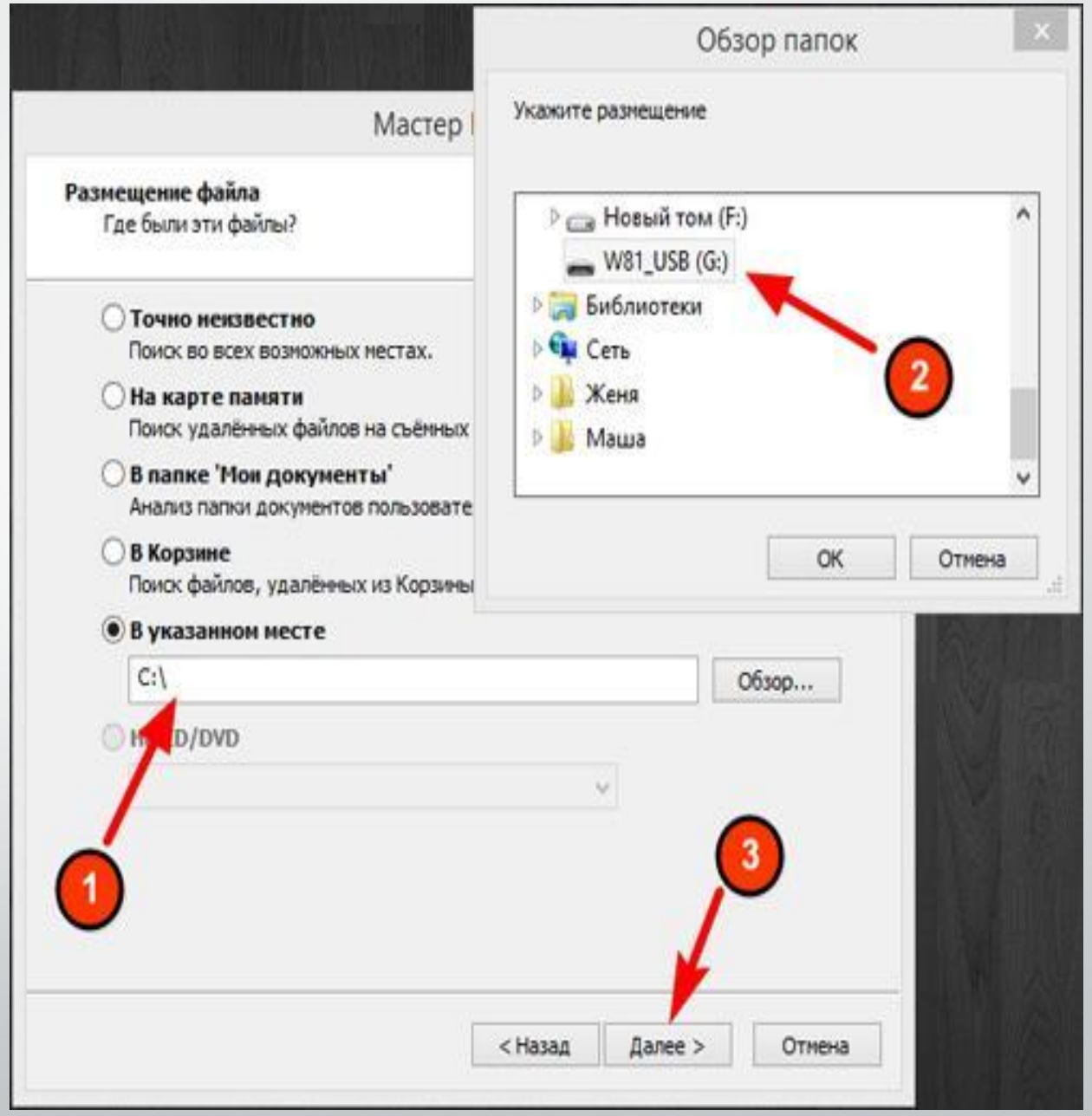


Recuva

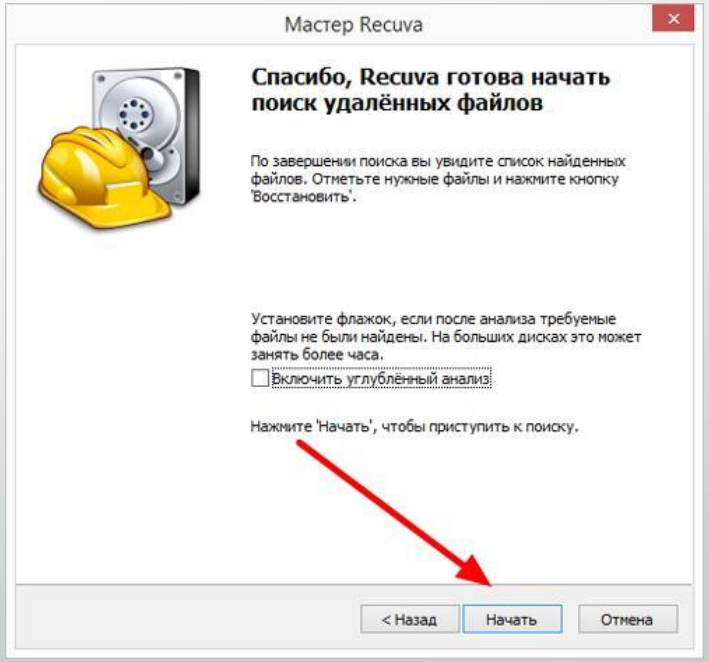
- бесплатная утилита позволяет восстановления дан-ных после очистки корзины и сбоев файловой. Можно выбрать восстановление только музыки, документов, изображений, видео файлов, архивированных файлов или почтовых файлов.



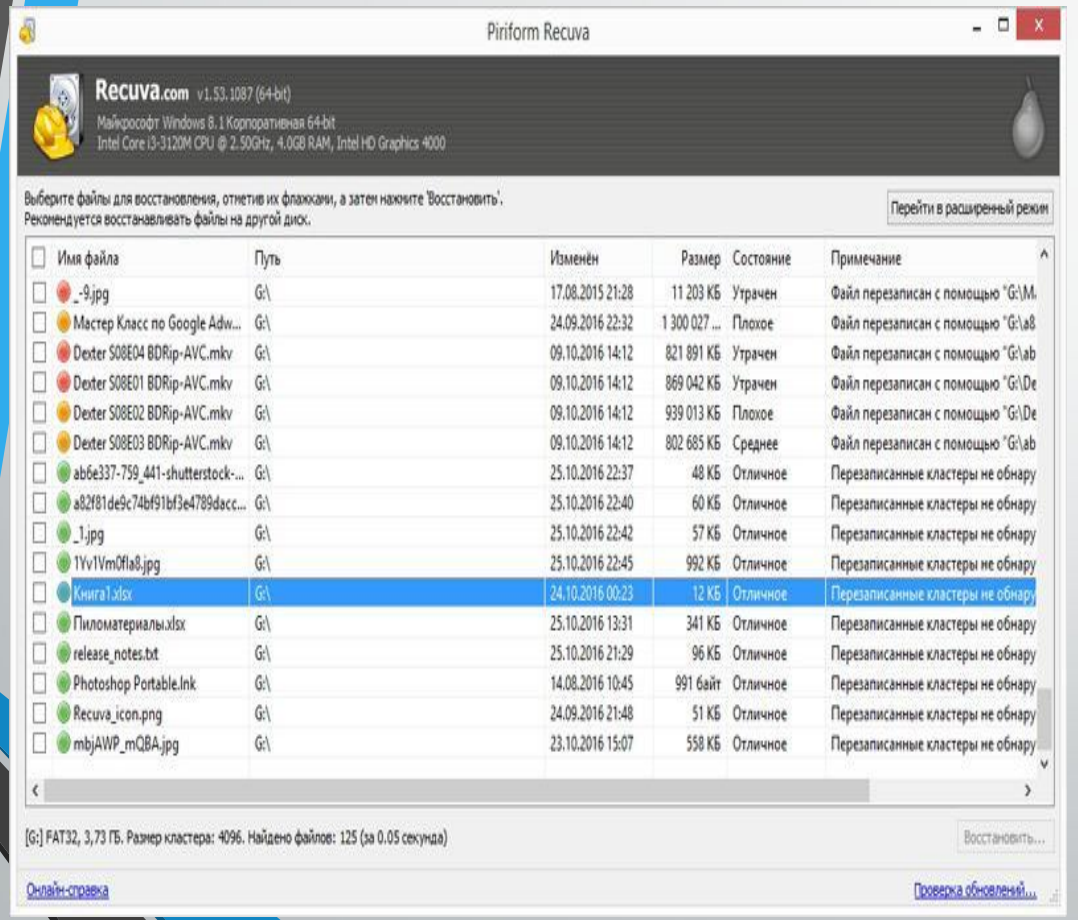
- Если вы точно знаете месторасположение удаленных файлов (в нашем примере — это флешка), выбирайте пятый пункт *«В указанном месте»*, отмечайте двойным кликом в появившемся списке нужный диск/папку и нажимайте *«Далее».*

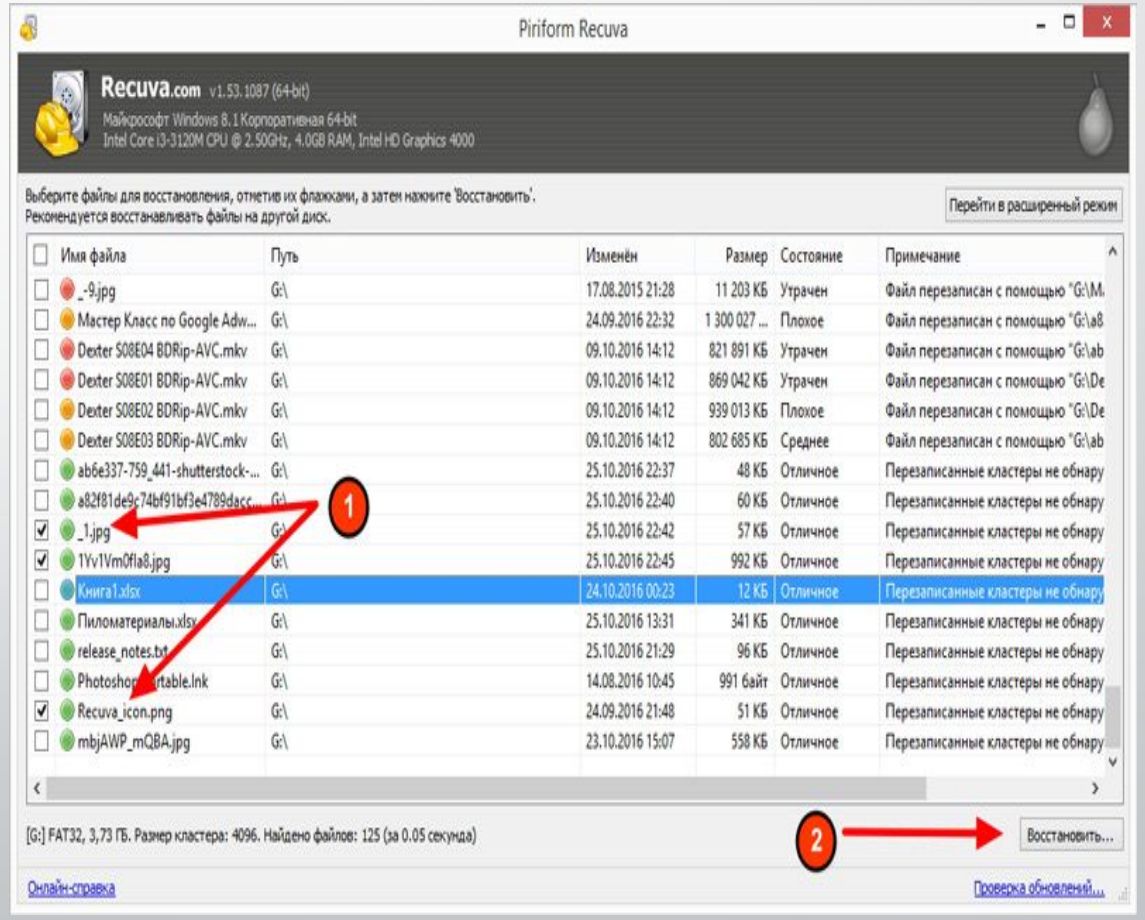


Recuva позволяет провести углубленный анализ



- 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.



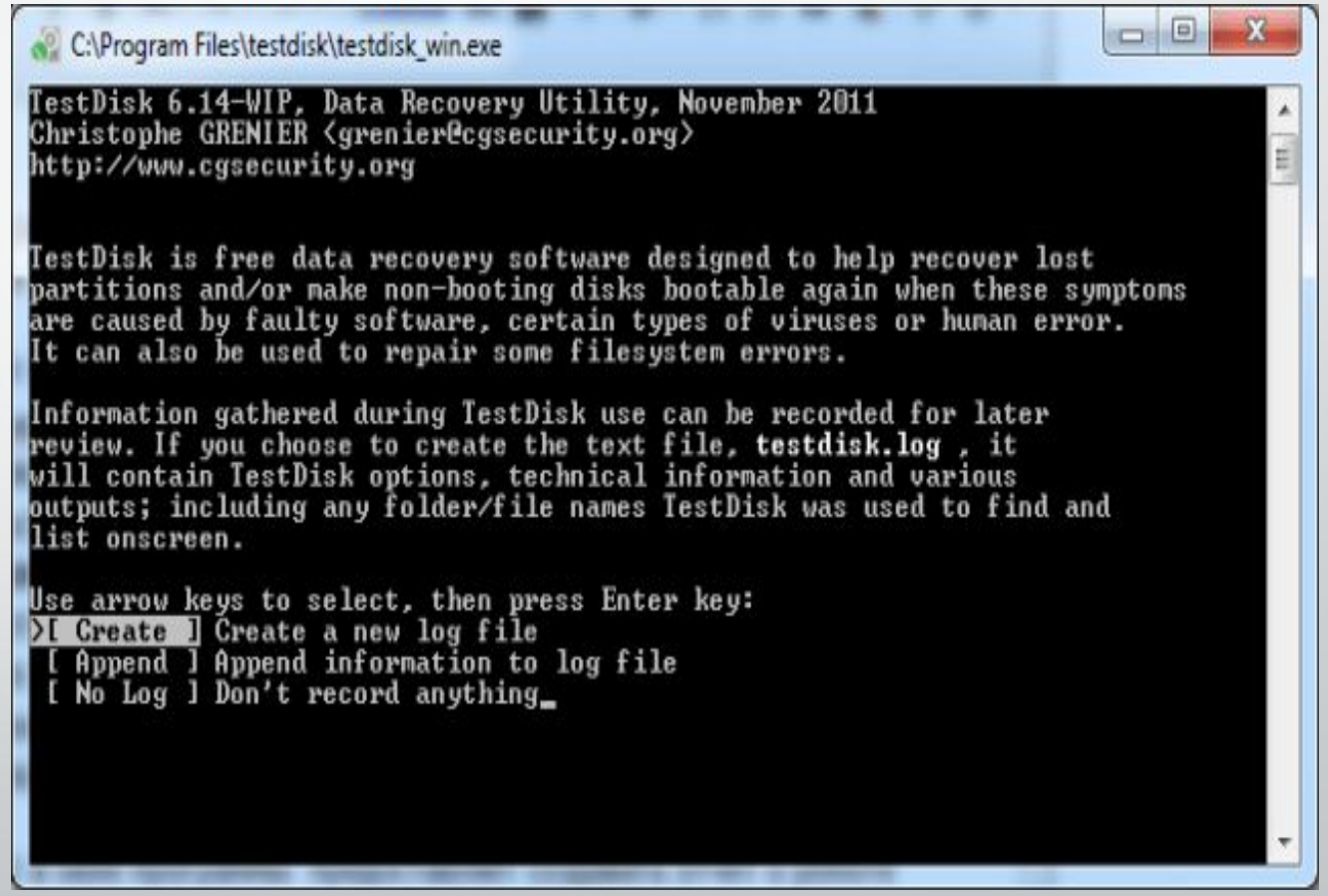


TestDisk и PhotoRec

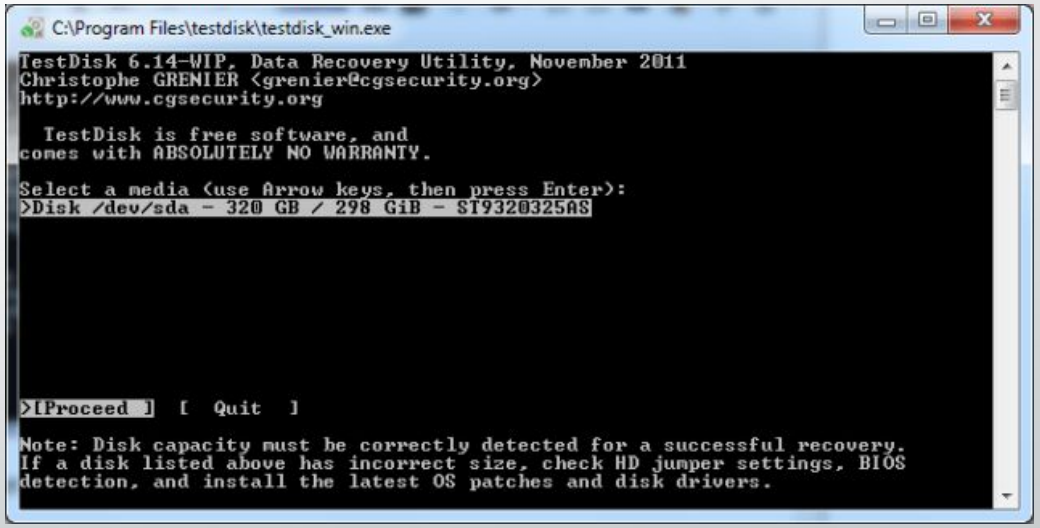
- TestDisk —поддерживает огромное количество файловых форматов, позволяет восстановить данные с диска, на котором не загружается операционная система. Утилита может восстановить повреждённый загрузочный сектор или потерянные данные. В комплекте с ней используется программа PhotoRec для восстановления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

Testdisk

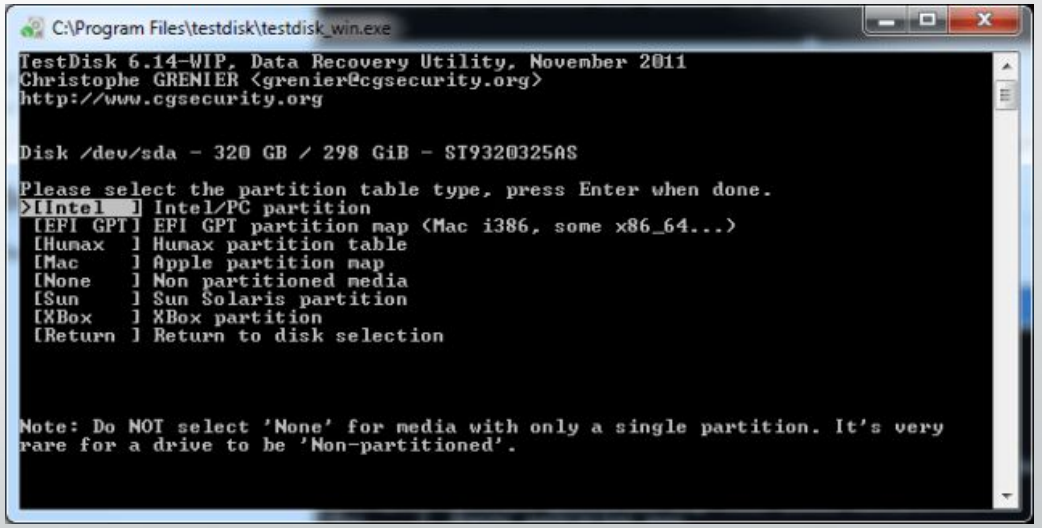
- Программа позволяет восстановить поврежденный загрузочный сектор.
- Create a new log file - создать новый файл
- Append information to log file - добавить информацию в файл
- Dont record anytihng - ничего не записывать



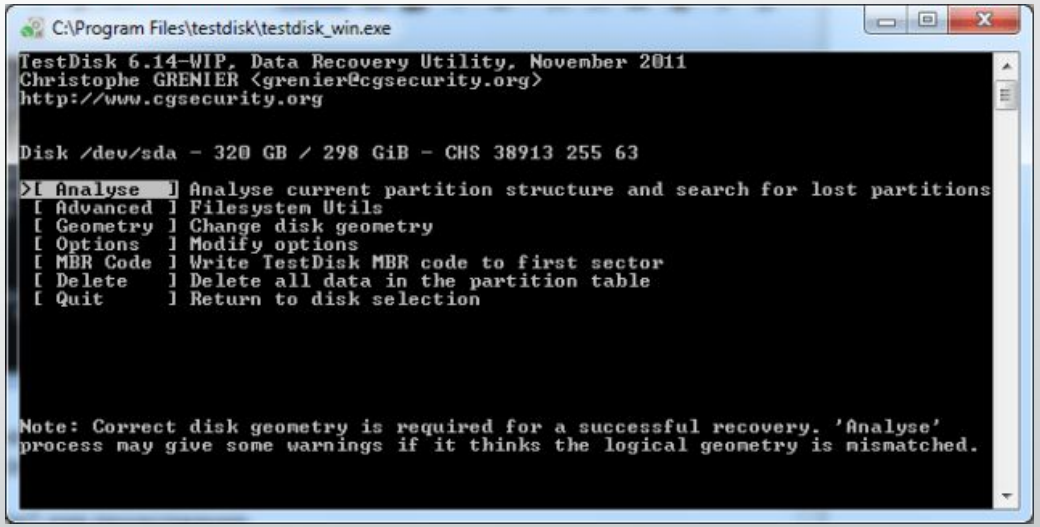
- Осуществляется выбор диска (не только винчестеры, но и на съемных носителях)



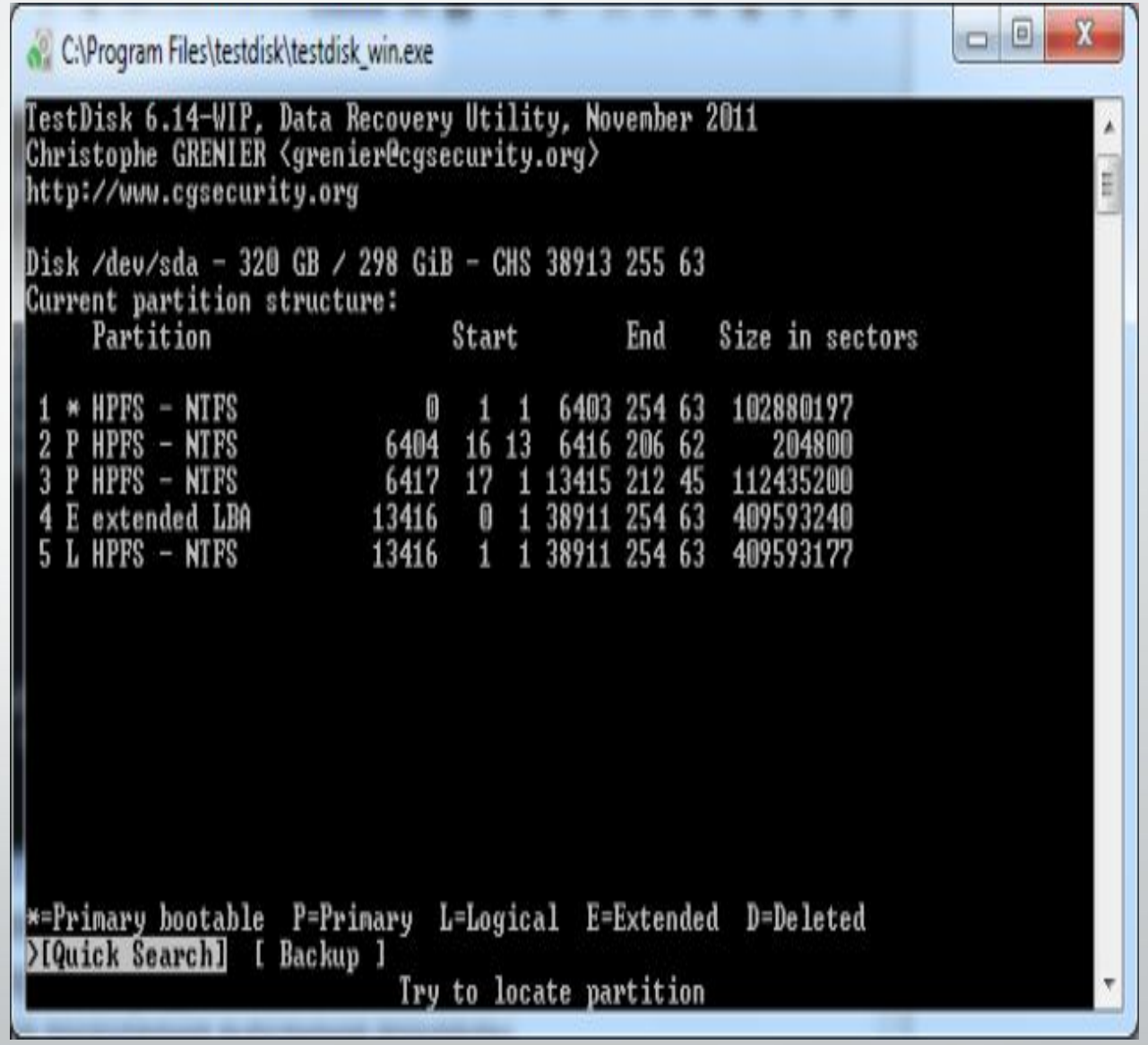
- Программа предоставляет Таблицу разделов.



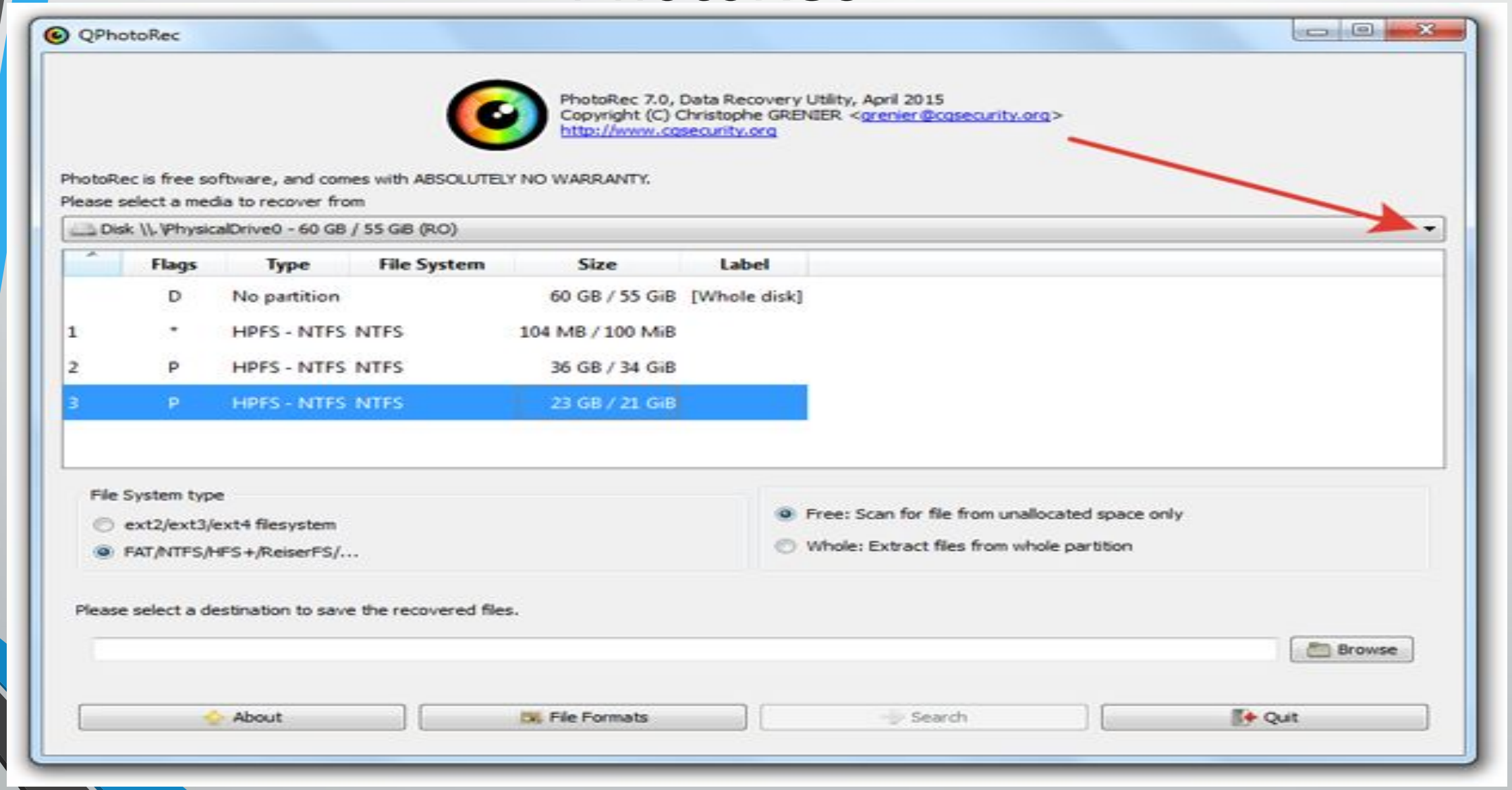
- Чтобы произвести тест структуры разделов выбранного носителя информации, а также поиска пропавших файлов, следует выбрать пункт «Analyse». Когда появится результат, вы увидите информацию о диске. Теперь нужно в меню, расположенном в нижней части экрана выбрать Quick Search. Сразу после этого программа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



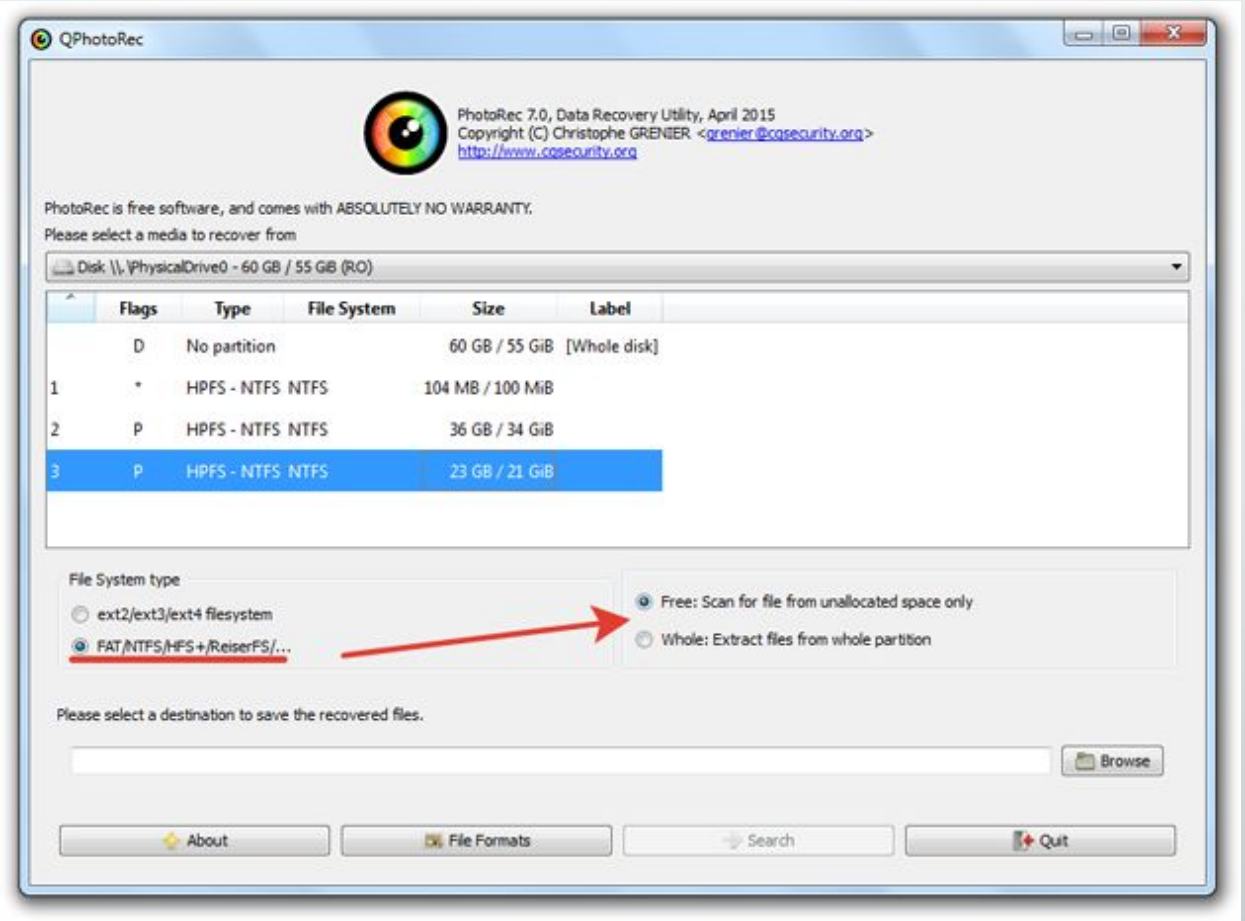
- Особенность этой программы - каталоги с русским наименованием изображаются некорректно.
- После восстановления одного из разделов необходимо перезагрузить компьютер.



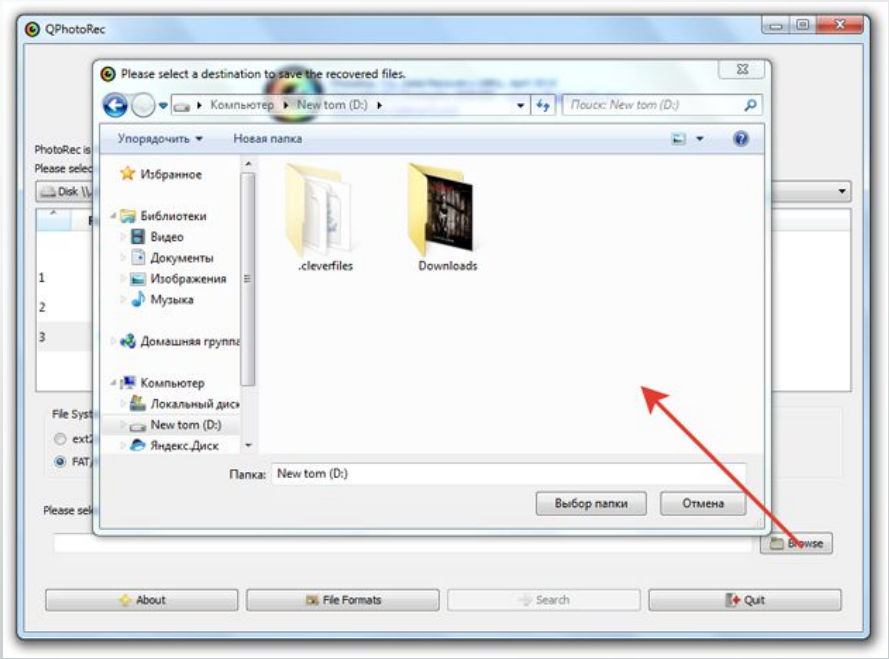
PhotoRec


QPhotoRec
PhotoRec 7.0, Data Recovery Utility, April 2015
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.
Please select a media to recover from
Disk \\.\PhysicalDrive0 - 60 GB / 55 GiB (RO)
Flags Type File System Size Label
D No partition 60 GB / 55 GiB [Whole disk]
1 * HPFS - NTFS NTFS 104 MB / 100 MiB
2 P HPFS - NTFS NTFS 36 GB / 34 GiB
3 P HPFS - NTFS NTFS 23 GB / 21 GiB
File System type
ext2/ext3/ext4 filesystem
FAT/NTFS/HFS+/ReiserFS/...
Free: Scan for file from unallocated space only
Whole: Extract files from whole partition
Please select a destination to save the recovered files.
Browse
About
File Formats
Search
Quit

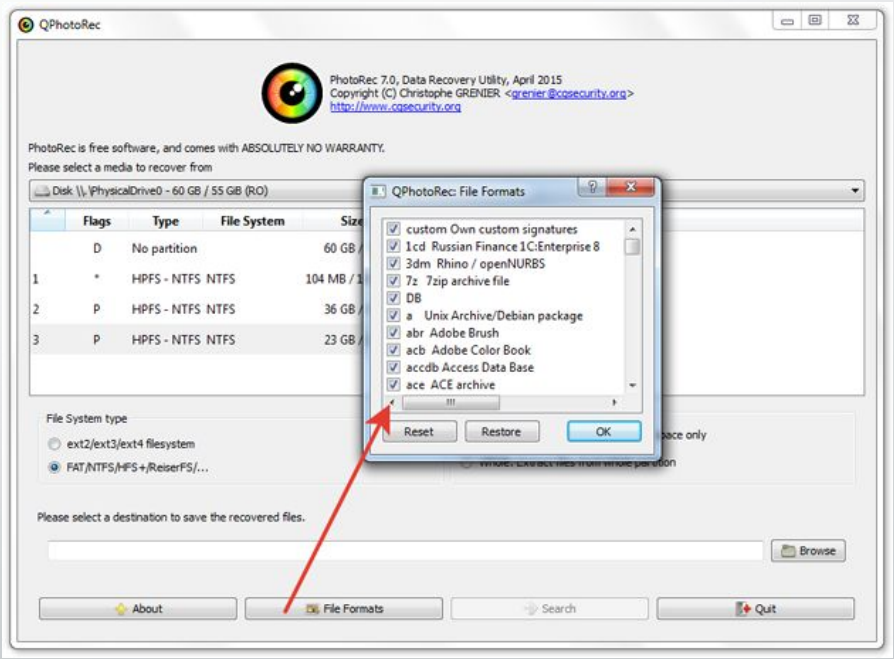
- Рядом выберите режим сканирования – Free или Whole. Полное сканирование (Whole) займет намного больше времени, эффективность восстановления будет выше.



- 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.