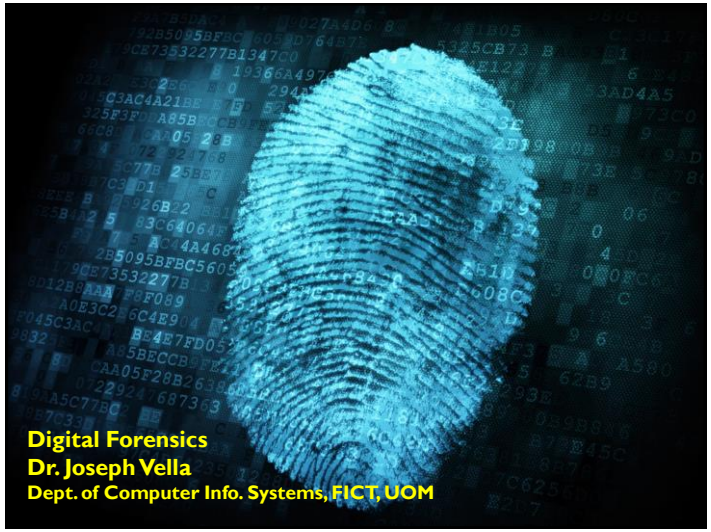


DELETED FILES & PARTITIONS

Undeleting & Recovering files (including folders & partitions) is an important forensic activity.

Although a number of tools exists it's very OS/FS related and therefore *ad hoc* techniques are required.

J Vella – Digital Forensics Deleted Files

Introduction

- An obvious action, and reaction, of a perpetrator is to delete digital content, traces and signatures. This is to conceal:
  - Evidence of event;
  - The perpetrator.
- Scope of this session:
  - Data stored in
    - Files &
    - Partitions.
  - Operating systems
    - MS Windows &
    - Linux.
  - Operation(s)
    - Undelete files & folders (using undelete) – filing system features;
    - Retrieve files & folders (using recovery) – having a backup repository.

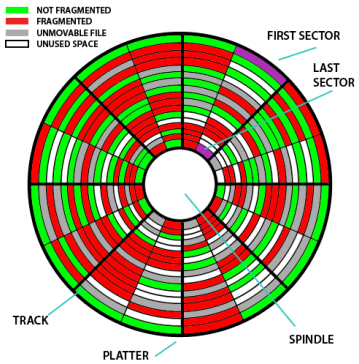
J Vella – Digital Forensics Deleted Files

undeletion

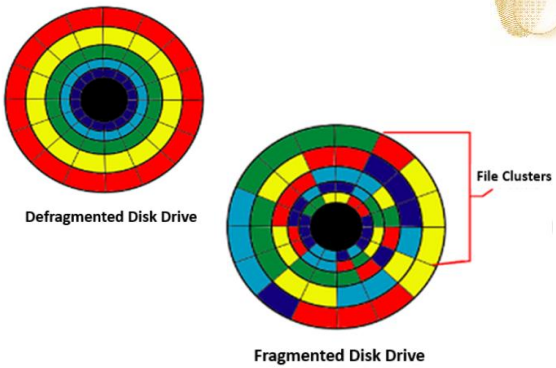
- Undelete restores files from a file system through an OS facility (e.g. delete CLI command in MSDOS and Windows).
  - Not all OS provide undelete capabilities and applicability is strongly tied to the OS filing system.
    - Microsoft have had it from MS DOS 5 up to 6.2;
    - In Unix and Linux it's a add-on to ext2 and ext3. ext4 has undelete as a feature (but not universally implemented).
      - Many GUI shells have implemented undelete as part of the Trash (and Recycle) where files are moved to a temporary area.
- Approaches for enabling undelete (and recovery):
  - File-system entries in its directories and files;
  - Holding area as in Trash & Recycle;
  - Copy deleted files to an archive;
  - File versioning (e.g. as in the defunct DEC OpenVMS / Files-11).
- Undelete will not always work!
  - Because of file fragmentation and space management, undelete has better probability of success the sooner it is attempted.

J Vella – Digital Forensics Deleted Files

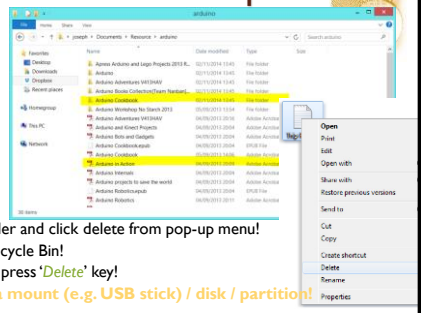
File allocation onto a fs – file frag



File allocation onto a fs – file frag



Deleting files & folders in Explorer

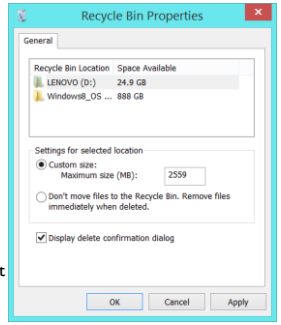


- How?
  - *Right Click* on file and or folder and click delete from pop-up menu!
  - *Drag* file and or folder to Recycle Bin!
  - Select file and or folder and press '*Delete*' key!
  - Let's ignore formatting a mount (e.g. USB stick) / disk / partition!
- Then What?
  - If
    Not a mount
    And shift key not pressed
    Not in use
  - Then
    - "Deleted" files / folders are actually moved to the Recycle Bin.

Knowledge of Recycle Bin Behaviour

- Huge files are never recycled.
- If data size allocation is reached then deleted files start overwriting older items.
- One can side-track the Recycle bin by:
  - Use of shift key with the delete key; or
  - Setting "Don't move files to Recycle bin …".
- Items bin might have their folder name appended with Windows security identifier (SID).
  - Recycle Bin is located in a hidden directory named `\$Recycle.Bin\%SID%` where %SID% is the SID of the user that requested the deletion.

Windows 8.1



What happens at the Recycle Bin?

- Files and folders are moved to Recycle Bin because they have been selected for deletion.
  - i.e. files and folders are not deleted!
    - Also one is only moving file descriptors as file data (i.e. disk pages are not really moved).
  - Can delete files and folder and maintain the structure in the bin.
- On moving a file or folder into the Recycle Bin the following happens (i.e. MS Windows 7 & 8):
  - File (or folder) are moved to the Recycle Bin;
  - Each file (or folder) has the original location and date deleted attached to it;

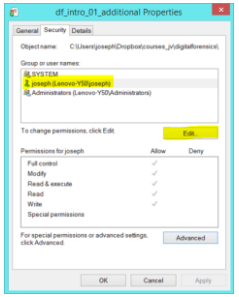
Once in the Bin (not pushed out or moved out):

One can browse the bin;

Undelete at will.

Set, View, Change, or Remove Permissions on Files and Folders

- When a file or folder is created, Windows assigns default permissions to that object.
  - **Modify** is the minimum permission required to complete this procedure. Review the details in "Additional considerations" in this topic.
    - To set, view, change, or remove permissions on files and folders
    - Right-click the file or folder for which you want to set permissions, click **Properties**, and then click the **Security** tab.



Undelete in FAT (MS DOS / FS)

- On delete the directory entry remains unchanged.
  - Preserving the "deleted" file's name, time stamp, file length and its physical location on the disk.
  - The list of disk clusters occupied by the file will be erased from the File Allocation Table (FAT), marking those sectors available.
- For undelete success the following must hold:
  - The entry of the deleted file must still exist in the directory, meaning that it must not yet be overwritten by a new file;
  - The sectors formerly used by the deleted file must not be overwritten yet by other files.
    - Even if the new file has already got deleted and returning sectors to FAT!
      - Consequently it is imperative to *check* the undelete file integrity.
- Note:
  - Recovery of fragmented files (after the first fragment) is therefore not possible by automatic processes, but only by manual examination of each (unused) block of the disk. This requires detailed knowledge of the file system, as well as the binary format of the file type being recovered, and is therefore only done by recovery specialists.
  - **Undelete works up to MS DOS version 6.22!?**

Undelete in Linux

```
$ rm -rf /path/to/myfile
```

- Use debugfs to view a filesystems log

```
$ debugfs -w /dev/mapper/wks01-root
```

- At the debugfs prompt

```
debugfs: lsdel
```

- Sample output

```
Inode  Owner  Mode    Size    Blocks   Time deleted
23299      0 120777      3    1/   1 Tue Mar 13 16:17:30 2012
7536655    0 120777      3    1/   1 Tue May  1 06:21:22 2012
2 deleted inodes found.
```

- Run the command in debugfs

```
debugfs: logdump -i <7536655>
```

- Adopted from:

http://www.cyberciti.biz/tips/linux-ext3-ext4-deleted-files-recovery-howto.html

- debugfs::logdump -i <7536655>

```
...
output truncated
    Fast_link_dest: bin
    Blocks:  (0+1): 7235938
  FS block 7536642 logged at sequence 38402086, journal block 26711
    (inode block for inode 7536655):
    Inode: 7536655 Type: symlink Mode: 0777 Flags: 0x0 Generation: 3532221116
    User:     0   Group:     0   Size: 3
    File ACL: 0    Directory ACL: 0
    Links: 0   Blockcount: 0 Fragment:  Address: 0    Number: 0    Size: 0
    ctime: 0x4f9fc732 -- Tue May  1 06:21:22 2012
    atime: 0x4f9fc730 -- Tue May  1 06:21:20 2012
    mtime: 0x4f9fc72f -- Tue May  1 06:21:19 2012
    dtime: 0x4f9fc732 -- Tue May  1 06:21:22 2012
    Fast_link_dest: bin
    Blocks:  (0+1): 7235938
No magic number at block 28053: end of journal.
```

- With the above inode info run the following commands

```
# dd if=/dev/mapper/wks01-root of=recovered.file.001
bs=4096 count=1 skip=7235938
```

- # file recovered.file.001
- file:ASCII text, with very long lines
- Files been recovered to recovered.file.001.

Back-up & Restore

- The process of copying files (and their properties) from source to archive and back.
  - Backups are indispensable for:
    - Data recovery;
    - Return to a point in time.
- Data owners usually implement some of their data retention policies and disaster recovery plans through backups.
- Backing up techniques include:
  - Unstructured
  - System image
  - Incremental (mixing with full backups) – save by time increments
  - Differential (with a full backup) – save files that have changed since last full backup.
    - Therefore restore needs to access at most two backup files (i.e. full and last differential).
  - A reverse delta type repository stores a recent "mirror" of the source data and a series of differences between the mirror in its current state and its previous states. This can be done through binary diff.
    - System employed by Time Machine (Mac).
    - Continuous data protection.
- Backup are stored on a variety of storage media:
  - HDs, Tapes, Optical, Solid state, Remote back-up service.

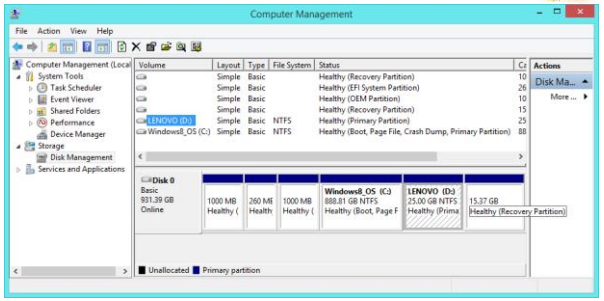
DELETING AND UNDELETING DISK PARTITIONS

Deleting a Partition

- What happens?
  - All data on that partition is lost.
  - If partition is on dynamic disk all dynamic volumes are deleted!
- How?
  - Using the Windows GUI or the CLI.

Delete a partition (GUI):

Exec Window/Control Panel/Admin Tools/Computer Management
Choose key Storage Key / Disk Management.



- Right-click the partition, logical drive, or basic volume you want to delete, and then click Delete!

Delete a partition (CLI):

command prompt (MSDOS) and invoke diskpart

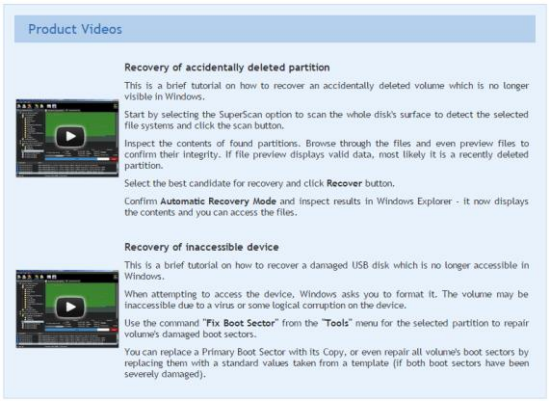
```
DISKPART> list disk
Disk ###  Status         Size     Free     Dyn  Gpt
Disk 0    Online          931 GB      0 B        *
DISKPART> select disk 0
Disk 0 is now the selected disk.
DISKPART> list partition
  Partition ###  Type              Size     Offset
  Partition 1    Recovery          1000 MB  1024 KB
  Partition 2    System             260 MB  1001 MB
  Partition 3    OEM               1000 MB  1261 MB
  Partition 4    Reserved           128 MB  2261 MB
  Partition 5    Primary            888 GB  2389 MB
  Partition 6    Primary             25 GB   891 GB
  Partition 7    Recovery            15 GB   916 GB
DISKPART> select partition 5
Partition 5 is now the selected partition.
DISKPART> delete partition
```


Undelete a partition

- The recovery of deleted partitions is the process by which a user can evaluate and extract deleted partitions.
  - The partition recovery process is important in case of data recovery.
  - This recovery helps in recovering the partitions that are lost accidentally, or due to virus, software malfunction, or even sabotage.
- There are some tools available for the recovery of deleted partitions.

Active@ Partition Recovery

- This is a freeware (and commercial) toolkit that helps you to recover deleted and damaged logical drives and partitions within DOS, Windows, & Linux (recovery LiveCD) environments.
  - Simple QuickScan easily detects and recovers recently deleted partitions, as long as they were not formatted / overwritten to after deletion.
  - Advanced low-level SuperScan may detect partitions which were deleted a long time ago, even if you have created new ones and even formatted them.
  - LastChance recovery method detects & recovers files by their signatures on volumes having severely damaged file systems, where physical volume recovery isn't possible!
  - Fixes damaged Partition Table, MBR (Master Boot Record).
  - Creates a Disk Image - sector-by-sector data backup for data recovery.
  - Restores all data from raw, compressed and VMWare Disk Images.
  - Supports Windows 7 & 8, XP & Vista, 2003 & 2008 & 2012 Servers, …
  - Recovers FAT/exFAT/NTFS/HFS+/UFS/Ext2/Ext3/Ext4/BtrFS file systems.
  - Recovers IDE, SATA, eSATA, SSD, SCSI, RAID, USB Flash Disks and Memory Cards.



Please view these at your own time:
http://www.partition-recovery.com/videos.html

Software – EnCase Remote Recovery

Advertising

- Remotely Undelete Files, Quickly and Easily
  - Reach across the network and access user file systems to restore deleted files without getting on a plane, shipping hardware or taking users offline.
  - Rapidly navigate file directories and view files to access information without data transfer, then move any number of files between shared storage or computers running Windows, Linux, OS X, Solaris, NetWare and other operating systems - EnCase Remote Recovery + covers it all.
  - Diagnose system issues and troubleshoot network connectivity of remote computers, using key system diagnostics.
  - Remote Recovery is non-disruptive to users, which means you can keep users online and productive while you undelete remote files, diagnose problems and collect data in the background.

(please view clips at your leisure)

- https://www.guidancesoftware.com/products/Pages/encase-remote-recovery/overview.aspx?cmpid=Referral-OTHER-Remote_Recovery_NA-Q414_Remote_Recovery_Launch_Press_Release-A-Landing_Page-Remote_Recovery_Overview-10-13-2014&utm_source=OTHER&utm_medium=Referral&
- These are 3 minutes promotional clips!?

Deleting files in the Cloud (example)

- http://computerforensicsblog.champlain.edu/2012/08/10/dropbox-forensics/
- http://www.magnetforensics.com/dropbox-decryptor-a-free-digital-forensics-tool/

Dropbox

- Dropbox consists of cloud-based services for user identity and management, data storage, access, and management, and programmatic interfaces (APIs);
  - clients for data access and storage on desktop and mobile operating systems; and
  - web applications for data and service management.
- The Dropbox client enables users to drop any file into a designated folder.
  - The file is then automatically uploaded to Dropbox's cloud-based service and made available to any other of the user's computers and devices that also have the Dropbox client installed.
  - Users may also upload files manually through the Dropbox web application.
- Dropbox client supports synchronization and sharing along with personal storage.
  - It supports revision history, so files deleted from the Dropbox folder may be recovered from any of the synced computers.
  - Specifically Dropbox supports multi-user version control.
- Dropbox uses Amazon's S3 storage system to store the files.


Dropbox Logo


Synced


Syncing

Dropbox – deleting & restoring files

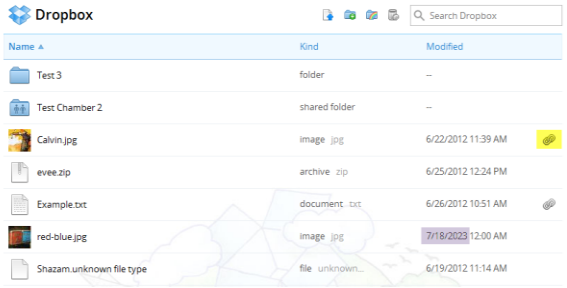
- This ubiquitous service makes it inevitable that it will be used to back-up or transfer files that are relevant to a forensic investigation.
  - The Dropbox servers store many useful logs in regards to account history and a user's file history.
- This case study indicates methods for discovery and collection of activities and files related to an investigation.
- Topics:
  1. What artifacts are created during the installation process?
  2. What artifacts are left behind after Dropbox is uninstalled?
  3. What information can be gathered from the Dropbox database files?
  4. What artifacts are created when a file is uploaded or downloaded?
  5. What evidence is there when a file is shared using Linking or a Shared Folder?
  6. What logs does Dropbox create and how accurate are they?
  7. Are there any other sources of information relating to Dropbox?

Dropbox – deleting & restoring files (continued)

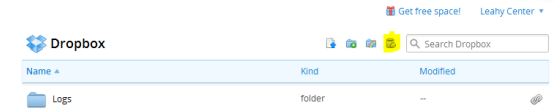
- Toolbox:
  - Dropbox – Dropbox.com
  - Winhex – winhex.com/winhex
  - Hexedit – hexedit.com
  - Guidance Software's Encase 6.19 – guidancesoftware.com
  - VMware – vmware.com
  - ProcessMonitor download.cnet.com/Process-Monitor/3000-2094_4-10603966
  - Regshot sourceforge.net/projects/regshot
  - Wireshark – wireshark.org
  - Python – python.org
  - Windows 7/8
  - Chrome – google.com/chrome
  - Internet Explorer

Dropbox – deleting & restoring files (continued)

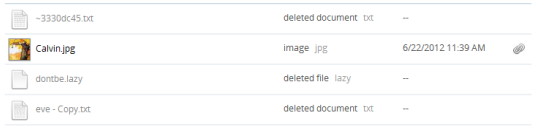
- Evidence collections
  - Web Portal
    - Account handle and login info not available on client (neither available from server!?).



Dropbox – deleting & restoring files (continued)

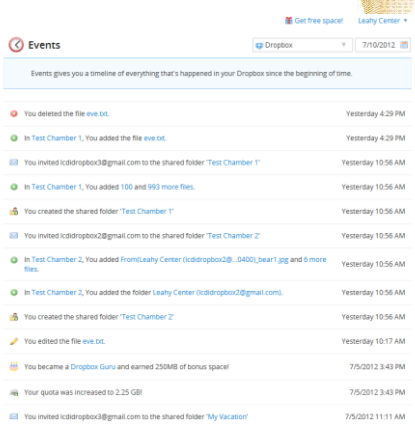


- The greyed out files are deleted files that are seen using the "view deleted files" feature.

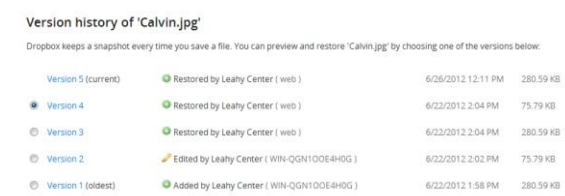


Dropbox – deleting & restoring files (continued)

- Events Log:



Dropbox – deleting & restoring files (continued)



Dropbox – deleting & restoring files (continued)

- Linked files & Folders

Logs	folder	--	
mammal	folder	--	

- One can see this without a Dropbox client!

Logs

eve (2).txt	29 bytes	14 days ago
eve (3).txt	29 bytes	14 days ago

J Vella – Digital Forensics
Deleted Files

Dropbox – deleting & restoring files (continued)

- One can read, through Dropbox API, a database (with two tables) all activities and artefacts held per account!

J Vella – Digital Forensics
Deleted Files