



## 3 Days Course on Forensic & Anti-Forensic Data Recovery: Tools & Techniques



### Two Sigma Technologies

Suite B, 19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,  
68100 Batu Caves, Selangor  
Tel : 03-61880601/Fax :03-61880602  
sales@2-sigma.com  
www.2-sigma.com



## Forensic & Anti-Forensic Data Recovery: Tools & Techniques

Forensic Data Recovery is the collection, preservation, analysis, and presentation of computer-related evidence. Computer evidence can be useful in criminal cases, civil litigation, and human resource and employment proceedings. Far more information is retained in a computer than most people realize. It's also more difficult to completely remove information than is generally thought. For these reasons, as well as others, computer forensic examinations can typically recover lost or deleted information (or at a minimum find evidence of the information) even when it has been intentionally deleted. Computer hard drive forensic examinations go far beyond normal data recovery techniques, probing areas and files on the media not normally accessed by untrained personnel. These examinations can locate whatever data a business, agency, or individual needs. Meanwhile for Anti-Forensic is a set of tools and techniques used as countermeasures for forensic analysis. Such techniques include data hiding, artefact wiping, disk cleaning utilities, file wiping utilities, disk degaussing/destruction techniques.

This training course is designed to introduce the latest data recovery techniques and solutions. The training course would also offer counter countermeasures for forensic analysis.

### Course Settings

Date	Refer to Training Calendar
Venue	Refer to Training Calendar
Fees	Contact Us at sales@2-sigma.com
Timings	0900-1700 (3 Days)
Inclusive	Certificates and notes
Audience	The course has been designed for IT personnel, administrators, computer support staffs and an end-user who are aware the importance of data in their storage. No previous repair or data recovery experience necessary.

### 3-Days Training Course would offer an excellent solution for:

1. Crash Windows Operating system corrupt.
2. Accidental Disk Formatted
3. Virus Attack
4. Partition loss or Corruption FAT/NTFS
5. Lost or Missing files and folders
6. Email recovery. pst / .wab / .dbx / .mbx
7. Password recovery (Workstation Win98/Vista/Win7/ Word/Excel/PDF dan Server 2003/2008)
8. Recover corrupted file from CD/DVD/Pendrive
9. Repair corrupt Files after recover ( word/ excel/ pdf)
10. Data Hiding, Encryption and Steganography
11. Artefact wiping
12. Disk Cleaning Utilities
13. Disk degaussing/destruction

#### Two Sigma Technologies

Suite B, 19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,  
68100 Batu Caves, Selangor  
Tel : 03-61880601/Fax :03-61880602  
sales@2-sigma.com  
www.2-sigma.com



## Training Methodology

Practical exercises combined with highly engaging activities will be used to reinforce learning objective. To highlight few of practical hands-on includes:

- Recover deleted files
- Recover data from CD / DVD
- Recover data from SD Card / MicroSD
- Recover data after MFT destroyed
- Recover data after Hard Disk has been formatted.
- Recover deleted Emails Outlook pst / .wab / .dbx / .mbx
- Recover Windows XP / Win 7 Admin Password
- Recover Windows Server Admin Password
- Recover Password (Words /Excel )
- Delete/erase/wipe any file from any media
- Delete/erase/wipe all data from any media and bring it back
- Anti-Forensic tools and techniques

## Data Recovery -Schedule

Day 1	
09.00am – 10.00am	<b>What is a file system?</b> <ul style="list-style-type: none"> <li>• Attributes of a file system</li> <li>• Microsoft Operating System</li> </ul>
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	<b>Hard Disk as a Storage Device</b> <ul style="list-style-type: none"> <li>• Platter/Heads/Circuit board /BIOS C-H-S Addressing</li> </ul> <b>File System on-Disk format</b> <ul style="list-style-type: none"> <li>• Master Boot Record/OS Boot Record</li> </ul> <b>Indexing Methods</b> <ul style="list-style-type: none"> <li>• FAT 16 – Attributes 16-bit addressing /Placement / File Entry Tables</li> <li>• FAT 32 – Attributes 32-bit addressing /Placement / File Entry Tables</li> <li>• TSF – Attributes (MFT) Database type/Placement/File Entry Tables</li> </ul> <b>Data Area</b> <ul style="list-style-type: none"> <li>• FAT 16 – Root Directory (Static)</li> <li>• FAT 32 – Root Directory (Virtual)</li> <li>• NTFS – MFT (Virtual) /INDX (Virtual) / Data Area (Virtual)</li> </ul>
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	<b>Practical Exercises I</b>

### Two Sigma Technologies

Suite B, 19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,  
68100 Batu Caves, Selangor  
Tel : 03-61880601/Fax :03-61880602  
sales@2-sigma.com  
www.2-sigma.com

Day 2	
09.00am – 10.00am	<b>File System Weaknesses</b> <ul style="list-style-type: none"> <li>Corrupt MBR</li> <li>Corrupt OS Boot Record</li> <li>Corrupt FAT /NTFS</li> <li>Corrupt MFT</li> <li>Virus pre-empting operating system load</li> </ul>
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	<b>Data Recovery</b> <ul style="list-style-type: none"> <li>Operating system will not boot</li> <li>MBR corrupted or missing</li> <li>OS boot record corrupted or missing</li> <li>OS Start up files missing or corrupted</li> <li>Virus pre-empting operating system load</li> </ul> <b>Practical Exercises II</b>
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	<b>Practical Exercises III</b>
Day 3	
09.00am – 10.00am	<b>Anti-Forensic Data Recovery Solution</b> <ul style="list-style-type: none"> <li>Data Hiding, Encryption and Steganography</li> <li>Artefact wiping</li> </ul>
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	<b>Anti-Forensic Data Recovery Solution (Continue)</b> <ul style="list-style-type: none"> <li>Disk Cleaning Utilities</li> <li>Disk degaussing/destruction</li> </ul> <b>Practical Exercises IV</b>
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	<b>Practical Exercises V</b>

### More Information

#### **Two Sigma Technologies**

19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,  
68100 Batu Caves, Selangor  
Tel: 03-61880601/Fax: 03-61880602

To register, please email to [sales@2-sigma.com](mailto:sales@2-sigma.com) or fax the registration form to 03-61880602, we will contact you for further action.

#### **Two Sigma Technologies**

Suite B, 19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,  
68100 Batu Caves, Selangor  
Tel : 03-61880601/Fax :03-61880602  
[sales@2-sigma.com](mailto:sales@2-sigma.com)  
[www.2-sigma.com](http://www.2-sigma.com)