# 

Digital forensics



### What is Digital Forensic?

Digital forensics is the art and science of *finding, analyzing, preserving* and *the precise documentation* of digital evidence, wherever it may be found, and then interpreting those findings in a way that makes it meaningful to any client or trier of fact. It is the use of scientifically derived and proven methods toward the *preservation, collection, validation, identification, analysis, interpretation, documentation* and *presentation* of evidence derived (Digital Evidence) from digital sources/media.

#### **Digital Evidence in Criminal Investigation**

Digital evidence is being employed effectively in all types of litigation. From hostile work environment issues, *criminal defense* cases, *intellectual property matters*, *financial fraud* to *family law practices*, etc. Mostly all matters of litigation benefit from the services of a digital forensics examiner.

#### Information that can be digital evidences in any litigations..

<u>Computer Information – Forensic Analysis on Hardisk, External</u> <u>Drive, Thumb Drives</u>

- Confidential files:
  - Hidden, deleted, temporary and password-protected files can be recovered
  - Documents and spreadsheets
  - Contact information and calendars
- Email/Chats
  - Confidential files transfer
  - Confidential communication
- Internet browsing history and habits
  - Online banking transactions
  - Online purchase/payment
  - Online gambling, etc..
- Pictures, graphics, videos and music
- Event logs, hacker activity and break-in attempts
  - Capture of suspect activity (fraudster activity)
  - Timeline based for files, internet transactions, etc..
  - Timeline capture of files transfer, email, chat..etc.
- Software installed (illicit, pirated and legitimate)
  - All types of programs details capture

#### <u>Mobile Phone Information – Forensic Analysis on All types of</u> CDMA phones

- Phone number and service provider information
- Uutbound and inbound call information
- Text messages, instant messages, MMS
- Emails.Gmail,Hotmail,Yahoo, Skypes,etc..
- Address books and calendars
- GPS data and location information
- Internet browsing history and habits
- Photos, videos, music and voice recorder data
- Predictive dialing directories and dictionaries
- Hidden, deleted, temporary and password-protected files can be recovered
- File System Support
- SIM Cloning
- Reporting PDF,HTML,TXT,XLS supported, etc....

## OG IT FORENSIC SERVICES (002038326-H)

- Private Digital Forensic Investigator
- Computer Forensic
- Mobile Phone Forensic
- Digital Media Acquisition and Analysis
- Hardisk/External hard disk,Thumbdrive,CD,etc..
- eDiscovery Services
- Digital Evidence Preparation
- LIVE Security Incident Response
- Forensic Accountant Engagement

OG IT Forensic Investigator is certified with Computer Hacking and Forensic Investigator and SANS Certified Security Incident Handling

MISSION: Bringing FINANCIAL FRAUD, IDENTITY THEFT & CYBER CRIME to JUSTICE with Digital Evidence

## **Forensic Process..**

Acquisition of digital media has to be done immediately. Followed by Forensic imaging, or copying, that involves the following critical phases:

- Securing and preserving the data source;
- Imaging the items/media (physical/logical),
- Documenting the approach and methods used to copy data;
- Validating the accuracy of the evidence.

The essence of digital forensics begins with the procedures utilized to create a forensic image. A proper forensic imaging process insures the integrity of the evidence by preserving it.



For more information regarding Digital Forensic Services please emai/contact:

- P +6019 2113491 / + 6016 2000397
- E support@ogitforensics.com
- E privateinvestigator@ogitforensics.com



Examples of Digital Evidence used in court of law
Banking – Statement download, Internet cache deleted in hard disk was retrieved https://ebpp.maybank2u.com.my/ebpp/PDFDownload?PDFType=rtjdl8RZVBI%3D&merchant=yyyyyy%3D&accno=% 2Byyyyyyyyk1%2yyyyy%3D%3D&stmtdate=yyyyyfGY00m0%2yyyB%2Byyy%3D%3D&MIBdate=J%2yyyyyyyyF%2B F2OVuQ%3D%3D.MBBcurrent 2010-11-30[1].pdfHTTP/1.1 200 OK Content-length: 243484 Content-type: application/pdf Content-disposition: attachment; filename="MBB2010-11-30.pdf"
Internet Banking online Transactions – Deleted from cache, but remain in hard disk   https://www.maybank2u.com.my/mbb/m2u/jsp/common/mbbReceipt.jsp?transactionType=Open+3rd+Party+Transfer&stat   us=Successful&fromAccountDisplay=   +PCA&amount=RM5000&referenceView=xxxxxxxx&ther=%3Ctr   %3E%3Ctd%3ETo+Open+3rd+Party+Account+%3A%3C%2Ftd%3E%3Ctr%3E%3Ctr%3E%3Ctr%3B%3Cstrong%3Exxxxxxx%3C   %2Fstrong%3E%3C%2Ftd%3E%3Ctr%3E%3Ctr%3E%3Ctr%3E%3Ctr%3E%3Cdt%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ctd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ctd%3E%3C%2Ftd%3E%3Ctd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ctd%3E%3C%2Ftd%3E%3Ccf%3E%3C%2Ftd%3E%3Ccf%3E%3C%2Ftd%3E%3Ctd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ccf%3E%3Ccf%3E%3Ccf%3E%3C%2Ftd%3E%3Ctd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ctd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ccf%3E%3C%2Ftd%3E%3Ccf%3E%3Ccf%2Fstrong%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ccf%3E%3Ccf%3E%3Ccf%3E%3Ccf%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ccf%3E%3C%2Ftd%3E%3Ccf%3E%3Ccf%3E%3Ccf%2Ftd%3E%3Ccf%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3C%2Ftd%3E%3Ccf%2Ftd%3E%2Ccf%2Ftd%3E%3Ccf%2Ftd%3E%2Cffd%3E%2Ccf%2Ftd%3E%3Ccf%2Ftd%3E%2Cffd%3E%2Cffd%3E%2Ccf%2Ftd%3E%2Ccf%2Ftd%3E%2Ccf%2Ftd%3E%2Ccf%2Ftd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Cffd%3E%2Ftd%3E%2Cffd%3E%2Ftd%3E%2Ftd%3E%2Ftd%3E%2Ftd%3E%2Ftd%3E%2Ftd%3E%2Ftd%3E%2Ftd%3E%2Ftd%2Ftd%3E%2Ftd%2Ftd%2Ftd%2Ftd%2Ftd%2Ftd%2Ftd%2Ftd
External Media – USB File logs – File was open from external media contains expenses F:/ABC expenses.xls <-/mnt/test//System Volume Information/_restore{46DE8921-1D39-44D2-A9E9- 64119261F211}/RP563/A0271258.lnk- which is stored on a local vol type - Removable- SN 0x4622dfc9 - Working dir: F:/ [SI ID exists-working dirpoints to a file or dir] - mod since last backup
Confidential Email Sent/Receive - Retrieve from deleted space (un allocated) of hard disk   From: name1,name2 [mailto:name1.   Sent: Tuesda
Chat messages   3433297408 ":"msg","msg":{"text":"then i will contact men see if he really ada   jalan","time":1282307008591,"clientTime":1282307007710,"msgID":"720597684"},"from":100000269152979,"to":10000051990147   8,"from_name":"mentioned::"mentioned::"mentis::"mentioned::"mentioned::"mentis::"mentis::"m
Highly Confidential Files modification and deletion info – Retrieved from deleted space of hardisk Filename A A A Hull Path B C C Created D Modified Control (14) 140 - 20 20:848,14092 UT C 2011-140 - 20 20:848,14092 UT C 2
Digital Forensic Reading Reference - RM65mil cyber fund fraud case the first in Malaysia <u>http://www.asiaone.com/News/AsiaOne%2BNews/Crime/Story/A1Story20080301-52197.html</u> - Collecting Digital Evidence <u>http://www.computerweekly.com/Articles/2011/09/21/247962/Law-enforcement-needs-to-get-smart-about-collecting-digital-evidence-says-forensic.htm</u>

Digital Evidence can only be obtained from Forensic Investigation & Analysis.!!