



# Data Theft: Insider Threat

**Whistle Forensic LLP**

[www.whistleforensic.com](http://www.whistleforensic.com)  
[enquiry@whistleforensic.com](mailto:enquiry@whistleforensic.com)

## Data Theft by Insider: A Case Study

### Background

Tackling insider threat is one of the most challenging tasks for an organization. Many of the employees tend to



unauthorizedly take company's confidential data with them, especially after acceptance of

their resignation and before their last working day (i.e., while serving the notice period).

In this incident, similar wrongful conduct by an employee was suspected by a Multi-National Corporation. Management of the company suspected that an employee had taken company's confidential information without authorization. The employee had separated from the company, almost around a year back.

In order to confirm the suspicion, the management of company wanted to ascertain if the employee had actually taken company's data with him or not; if yes, the details of the data unauthorizedly taken by employee to gauge the extent of damage.

### Investigative Details

Various investigative approaches were suggested to the company and after careful evaluation of each approach, the company decided to get forensic analysis of the laptop issued to the employee (while he was working for the company).

As the employee had separated around a year back and his laptop was issued to another employee, there was a possibility that logs/data could have been overwritten on the hard disk drive of the laptop. Notwithstanding this, company entrusted its faith on forensic examination of the laptop.

Certain basic details about the suspected employee were taken from MNC like name, mobile number, email address, date of resignation and last working day.

After completion of documentations, the hard disk drive of the laptop was forensically imaged

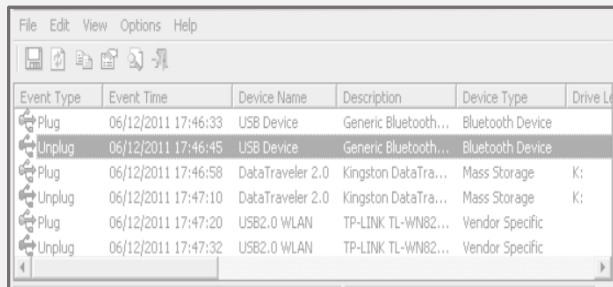


(*imaging is bit by bit copy of hard disk*). The imaged data was then processed and analysed using ADF Digital Evidence Investigator® Pro, (leading forensic software

for processing of computer forensic images) and other such forensic tools.

On analysis of forensically processed image file, evidences could be gathered for following:

- **USB Logs:** These logs confirmed that



Event Type	Event Time	Device Name	Description	Device Type	Drive Letter
Plug	06/12/2011 17:46:33	USB Device	Generic Bluetooth...	Bluetooth Device	
Unplug	06/12/2011 17:46:45	USB Device	Generic Bluetooth...	Bluetooth Device	
Plug	06/12/2011 17:46:58	DataTraveler 2.0	Kingston DataTra...	Mass Storage	K:
Unplug	06/12/2011 17:47:10	DataTraveler 2.0	Kingston DataTra...	Mass Storage	K:
Plug	06/12/2011 17:47:20	USB2.0 WLAN	TP-LINK TL-WN82...	Vendor Specific	
Unplug	06/12/2011 17:47:32	USB2.0 WLAN	TP-LINK TL-WN82...	Vendor Specific	

*Representative Photo (not original)*

multiple USB drives were connected to the laptop. These USBs were connected:

- A week before submission of his resignation.
  - A day before his last working day.
  - The employee had even connected his mobile phone in USB mode.
  - The unique drive letter (like E:/, F:/ and G:/) for each USB was mapped.
- **Google drive:** Logs suggested that a number of files were uploaded/accessed

from Google drive. Further, files with same name as accessed from Google drive were found on the hard disk drive of the laptop. This access was done a week before the submission of resignation.

- **File/Folder Access Logs:** On analysis of windows registry files, it was found that certain files/folder were opened on USB while it was connected to the laptop. The name of files/folder, so opened on USB were found on the hard disk drive of the laptop and these were “Confidential” files of the company.

- **Emails:** Certain files marked as “Confidential” were sent from official email address of the employee to his personal email address. These emails after sending were deleted.

A detailed forensic investigation report having aspects of each such file/folder was shared with the company for logical closure of case.

*Digital Forensics is one of the best approach to establish or negate involvement of an individual in suspected Data Theft incident*

Whistle Forensic team conducting Digital Forensic Investigations hold premier credentials from GIAC and SANS