

Case Study – Forged Letters issued on behalf of HP Government

By –

Rajender Singh Rana, M. Sc. (Physics), CIC*, PGDCA, ADCA***, MCA******
Assistant Government Examiner
Laboratory of Government Examiner of Questioned Documents,
Directorate of Forensic Science, Ministry of Home Affairs, Govt. of India,
Railway Board Building, Shimla- Himachal Pradesh (India)

A case was received in this Laboratory regarding retrieval of some Official Letters supposed to have been issued on behalf of Himachal Pradesh Government Departments. The accused was purported to have processed these letters on the suspect Hard Disk (IDE). The suspect Hard Disk (HDD in short) was seized by the Investigating Officer from a Cyber Café in Himachal Pradesh, India and was supplied along with the copies of the Letters alleged to have originated from the suspect HDD.

The suspect HDD was imaged to a new sterile HDD and the image was added to the Access Data FTK version 1.61 as per procedure. Data carving of all the files was opted for and the same was also added to the case.

Extensive Text and Index searching of the Image of the suspect HDD revealed no results; indicating thereby that the suspect Letters were not typed on the Computer bearing the suspect HDD. However working on the assumption that removable media was used to transport the forged letters to the suspect PC for taking print outs at the Cyber Café, another detailed effort was made to search for any evidence, especially in the Printer Spool files, if available from the suspect HDD. Understanding that print files spool images could be found within the carved Graphics files, the graphic files were examined (totaling about 19000).

After working on the case for about 10-12 hours a breakthrough was made in the form of Images stored in EMF format, which contained the images of the suspect letters. It needs to be mentioned here that EMF stands for Enhanced Metafile Graphic Files and are those files which a user sends to a printer to be printed, a graphic file (EMF) is created for each page of the document. EMF files are deleted after the print job is over; however FTK can carve these files out of unallocated space.

There were about a dozen of such letters and it was possible to link the suspect HDD with the printed copies of the Letters supplied by the Investigating Officer.

* **Certificate in Computing**

** **Post Graduate Diploma in Computer Applications**

*** **Advanced Diploma in Computer Applications**

**** **Master in Computer Applications**