Rescuing Digital Data from Submerged HDD

Toshinobu Yasuhira, Kazuhiro Nishimura, and Tomofumi Koida

High-Tech Crime Technology Division, National Police Agency,
2-1-2 Kasumigaseki, Chiyoda-ku, Tokyo, Japan
{yasuhira,k_nisimura,koida}@post.cyberpolice.go.jp

Abstract. As the increasing number of personal computers is involved in various criminal cases, the importance of the capability of extracting crucial digital data from these electromagnetic devices is getting emphasized. There are criminal cases where digital devices happen to be found in mud, water, and fire. Because digital devices have the possibility of storing essential key information that might contribute to the solution of particular criminal cases, it is usually required to retrieve data contained in the electromagnetic storage installed in personal computers by any means however damaged they may appear to be. This study reports one of the best practices of our successful experimental result on the extraction of digital data from damaged hard disk drive. This result is expected to help digital forensic practitioners deal effectively with similar cases in difficult situations.

Keywords: damaged hard disk drive, lubricant film, cleaning procedure, single platter.

1 Introduction

Since the emergence of personal computers in the 20th century, the industry of this particular hardware has made steady progress. In inverse proportion to the decreasing physical sizes of hard disk drives (HDDs), the capacity of the data storage has been drastically increasing. Personal computers now reach into every corner of society and become one of the most common daily necessities. It is next to impossible to imagine our daily lives without the small electronic devices.

On the other hand, the advance of technology raises new challenges for law enforcement organizations. It is a fact that personal computers are involved in most criminal cases and that the data stored in HDDs plays an important role in criminal investigations. It is also true that the constant technical innovations in the field of IT are always giving driving forces to the computer industry for updating or improving their products. What is adverse for the law enforcement agencies, new models of data storage installed in the latest personal computers are being launched on the market one after another, resulting in the difficulty for the police organizations to keep up with the latest technical standards.

Once a personal computer is found to be involved in a criminal investigation, the officers who have sufficient amount of knowledge and experiences should have the responsibility to deal with the digital evidence contained inside correctly. Criminals

P. Gladyshev and M.K. Rogers (Eds.): ICDF2C 2011, LNICST 88, pp. 226–237, 2012.

usually try to erase all data associated with their criminal activities before they are arrested. They are always ready to drop whole of their personal computers into water, mud, and fire for fear that the police organizations should be successful in extracting crucial data from the abandoned electronic devices. The National Police Agency, Japan has several successful experiences in the field of data extraction from such damaged devices. A successful forensic analysis is reported in this report.

2 Background

Fig. 1 shows a basic structure of a HDD. A HDD is composed of several parts as shown in it. A printed circuit board (PCB) serves a purpose of controlling the means of electrical connection between such components as flash ROM and hard disk controller. A platter is a circular disk on which magnetic signals are written. The recording surfaces of platters have crucial information area called SA ("Service Area" or "System Area") sometimes on the outer edge of some types of disks where the basic information regarding the management of a HDD is stored such as serial number, model, a list of bad sectors originally found at the manufacturing process (P-List), a list of sectors having gone bad after the HDD is in use (G-list) and so on. Because the digital data stored on the platter have huge impacts on criminal investigations in most cases, it is very important to handle this particular circular disk very carefully for being able to retrieve the evidential data successfully. As mentioned, SA contains such important information as dominates the operation of HDDs that it crucially depends on the technical skills to make the basic information recorded in SA usable whether the digital data on the platter can successfully be visualized or not.

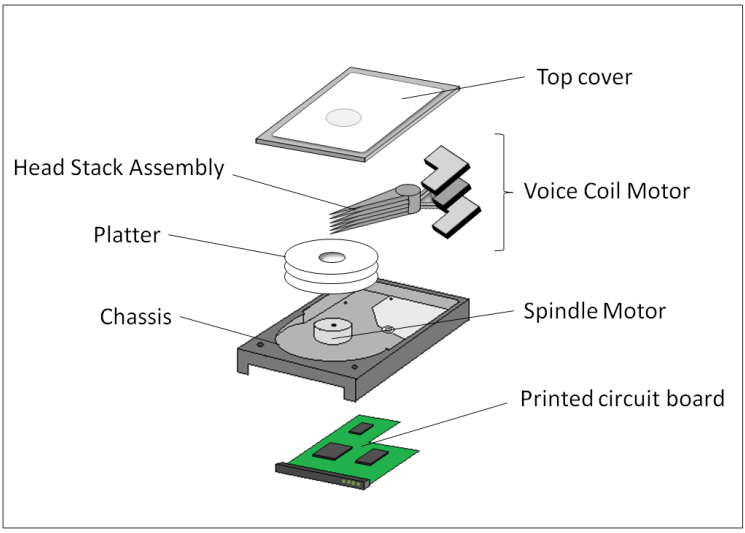

Fig. 1. Basic Structure of a HDD

The damaged HDD to be reported here was brought in by one of the Japanese government agencies. The size of the HDD manufactured by TOSHIBA was 2.5 inch and the capacity of the data storage was 60GB. The interface standard for the connection storage devices was parallel ATA (PATA). The personal computer in which the HDD used to be installed was dropped under sea water, and was left unattended for almost a year even after the salvage from the sea water. The condition of the HDD appeared to be pessimistic. However, the fact was a consolation to us that the HDD containing only one 2.5" platter inside would simplify the data extraction procedures because special attention usually needs to be paid to the adjustment of the platters' relative positions when it comes to a HDD with multiple platters inside. For the purpose of understanding the internal situation correctly, it was determined to examine the inner parts of the HDD by removing the top cover in our clean room. It was found that the sea water had already crystallized everywhere and that the magnetic head for reading digital data from the platter stuck to the ramp load in the HDD (Fig. 2). Moreover, crystallized salt covered the surface of the platter and the PCB. The terrible situation suggested the necessity of cleaning each part up prior to taking a further step for extracting data from the data storage.

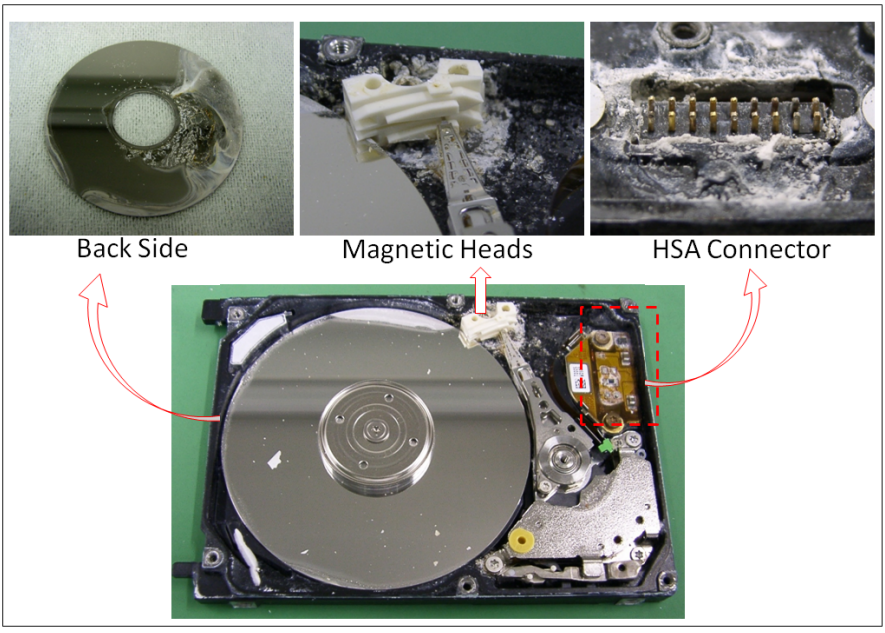

Fig. 2. The inside of the HDD immersed into sea water

There are various kinds of tools available for extracting data from a HDD. However, the consideration of utilizing these tools is usually practical only when the HDD functions properly without showing any problems in the platter's rotation and the magnetic head's movement. As it can be seen in Fig.2, the inside of the HDD

immersed into sea water was badly damaged by the crystallized salt. It was quite hopeless for us to expect that the HDD started functioning normally even when electricity was supplied. Moreover, prior to jumping at the consideration of energy supply, it must be noted that turning on electricity imprudently might give a fatal damage to the internal parts of the data storage. There may be something wrong with the internal electric circuits due to some damages, and there may be chances that dust or any particles deeply entering the inside of the precision instrument do damage to the surface of the platter or other critical internal parts. Therefore, instead of challenging the high likelihood of irrevocably damaging the HDD by attempting to power on, it was determined to give up trying software-based data recovery. Consequently, the top cover of the HDD was removed in our clean room facility for the purpose of examining the inner parts more in detail, and took every effort to extract the digital data stored on the platter effectively.

3 Data Recovery Plan

As mentioned in the previous section, SA contains critical data necessary for controlling the operation of a HDD. It sometimes occurs that chemical spillage or fire burnt over the HDD does damage to the surface of the platter inside. However, in most cases after appropriate handling processes, at least some parts of data can be extracted after all as long as the damage is just superficial and the SA still survives. Even if the SA is damaged for some reasons, there is still a method to read the digital data recorded on the platter. A company whose business includes data recovery service [1] reports a data recovery method that takes advantage of a spin-stand microscopy. A spin-stand is an innovative rigid disk tester designated to simulate actual HDD. Components of a HDD can be flexibly modified on a spin-stand such as magnetic heads, platters, location of the particular sector to be written, the specific pattern to be written and so on. Spin-stands have been popularly utilized in research environments to study different aspects of magnetic recording [2]. The utilization of the spin-stand makes it possible for forensic practitioners to remove magnetic heads and platters from HDDs, and to mount and operate them within a simulated HDD environment.

Admitting that the spin-stand apparatus provides powerful methods to read 0/1 signals out from HDD data storage, it is said that the reconstruction of the collected digital data into perceivable information is necessary after the data extraction process in order to produce evidence tolerant of criminal trials, for instance. It seemed to take quite a long time to firstly understand the data structure, and secondly restore the extracted data to something understandable. Luckily in our case, no physical stress caused by external force was apparently confirmed on the platter, and the SA seemed to be free from any damage. If the dirt and contamination were able to be successfully removed from the inside of the HDD, it was believed that there was a high probability that some parts of data at least stored on the platter could be rescued. Thus, taking the

time constraint at that time also into consideration, our definite policy to pursue was directed to transplanting the critical inner parts onto a newly prepared HDD body. Because there were few systematic technical papers in the public domain for us to consult, a continuous process of trial and error was attempted, aiming at finding out the most appropriate methods to extract digital data from the submerged HDD.

3.1 Flash ROM Replacement

The platter of the submerged HDD (original HDD) was decided to be installed in another newly prepared HDD (new HDD). A PCB cannot be replaced by another one of even exactly the same model because most of today's HDDs have their own specific parameters, part of which are usually stored in the flash ROM of the PCB [3]. In other words, a flash ROM in a HDD contains the critical information for controlling the whole function of the HDD, and the recorded data on a flash ROM is, in most case, peculiar to the platter installed in the particular HDD. In this sense, a HDD cannot be expected to work properly if the pair of the flash ROM and the platter fails to be surely transplanted to a new HDD at the same time. Based on the technical consideration, it is usually the case with a PCB that the whole of the PCB is transplanted and reused on a new HDD when little damage is identified on it. However in our case, due to the difficulty in removing the crystallized salt completely from the deep inside of the HDD as well as the surface of the PCB aiming at making the HDD re-functioning properly again, it was determined that only critical inner parts, the platter and the flash ROM, on the PCB of the original HDD should be once removed and recycled on the PCB of the new HDD.

Fig. 3 shows a conceptual drawing of the transplantation of internal parts from the original HDD to the new HDD. The flash ROM on the PCB of the original HDD was carefully detached, and the flash ROM formerly put on the PCB of the new HDD at the manufacturing factory was replaced by the removed flash ROM from the original HDD. Since the problems associated with lead (Pb) contained in soldering materials were revealed globally, the use of lead-free solder has become mainstream. The melting point of popularly-used lead-free solder is around 220 °C or so. In usual situations, a soldering iron at a little higher temperature around 280 °C is used for the removal of the flash ROM by heating up each pin coming out of the memory chip. But in our case, it was found out that the targeted flash ROM was very rigidly fixed on the PCB, and the pinpoint heating method using a soldering iron seemed to take a relatively long time. Surplus heat conducted from too long a contact of the soldering iron might do harm to other parts on the PCB. Thus, instead of heating each pin of the ROM chip focally by using a soldering iron, the method to expose the entire chip to hot air generated by a heat gun was chosen. Because the actual temperature of hot air cannot be controlled so easily, continuous observation of the solder's condition was required by softly swaying the chip with a pair or tweezers step by step. As a result, the flash ROM was successfully removed from the PCB without particular problems.

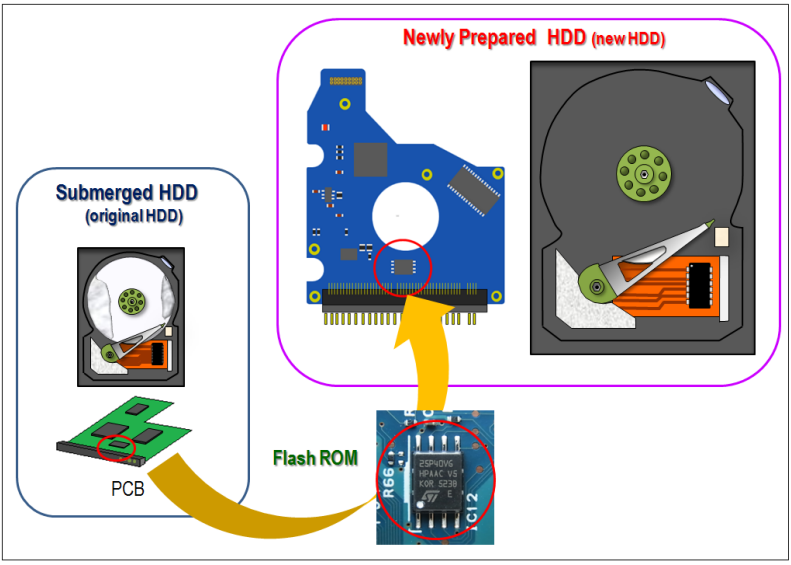

Fig. 3. Replacing procedure of the flash ROM on the PCB from the submerged HDD to another newly prepared HDD

3.2 Cleaning Procedure

The process of transplanting the critical inner parts starts with the careful removal of the platter from the original HDD. As already identified in Fig. 2, the detached platter was found to be covered with crystallized salt and appropriate cleaning-up procedure was required. Small lumps of salt crystals were carefully removed by using cotton buds immersed in ethanol in our clean room facility. After the rough removal of salt crystals, the platter was cleaned in an ultrasonic cleaner (USD-1R) manufactured by ASONE [4]. The platter was dropped into pure water at the temperature of 55 °C, and cleaned in the cleaner whose functioning frequency was fixed at 40 kHz for 5 minutes. As one of the most promising drying methods largely utilized by hard disk manufacturers, several information on hot de-ionized water drying methods are open to the public and available even on the Internet [5, 6]. Hot de-ionized water drying is a typical method in which a flat plate-like object with a smooth surface is put into heated pure or de-ionized water and then pulled out of the water at a constant speed in order to dry the object without permitting droplets to stick to its surface as shown in Fig. 4. Several rehearsals were engaged by using other platters as practices before attempting the actual object. The rehearsals showed that lifting at the speed of about as slow as 1 mm/sec gave us satisfying results without letting any droplets adhere to the platter surface in our case. A rinse in the pure water was tried immediately after the platter was cleaned in ethanol. Then, the lifted platter was completely dried at room temperature in the clean room. Even a small trace of a droplet on the platter may obstruct the smooth movement of the magnetic head, which could result in another trouble of scratching the surface of the platter, and end up with doing damage to the recorded data.

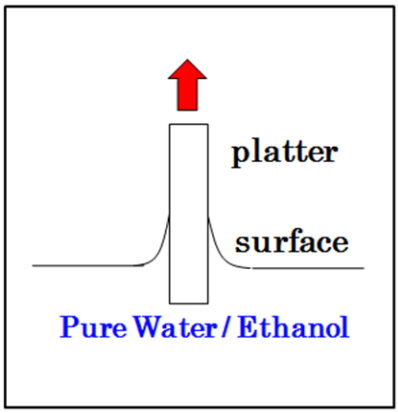

Fig. 4. Conceptual drawing of Hot De-ionized Water Drying

According to the information regarding typical industrial procedures of manufacturing HDDs available, lubricant is applied to the platter of HDD [7]. The role of lubricant mitigates the friction on the surface of the platter, which effectively prevents the damage caused by destructive contacts between the magnetic head and the surface from occurring. During the cleaning process of the platter, it was discovered that it seemed that some parts of the lubricant film originally layered on the platter had been degraded. As described in the conceptual picture (Fig. 5), a platter is composed of several layers. Under regular conditions, the lubricant film layer coats the whole of the protection film (diamond-like carbon: DLC) layer. It is reasonably believed that defective parts could fail to create spherical shape drops of water/ethanol due to the low surface tension in the apparently damaged areas on the platter while normal flawless lubricant film layer repels water droplets properly. The same situation was observed in our experiment. Instead of furthering more detailed research on what was happening on the surface microscopically, our experiment was promoted based on the assumption that the reconstruction of the lubricant film was the key to extract the data from the circular disk.

Perfluoropolyether (PFPE) is reported to be one of the most suitable lubricant materials [7]. The lubricant film of PFPE is generally coated on platter surfaces by immersing the circular disk in a solution of PFPE diluted by a solvent and then withdrawing them from the liquid. On the surface of a platter, the solvent quickly evaporates because of its high vapour pressure, leaving behind just thin PFPE layer [8]. Hydrofluoroether (HFE) is reported to be an appropriate material as a solvent to make a dilute solution of lubricant [7, 9]. Due to its lower adhesiveness to a magnetic head, one type of PFPE, Fomblin Z-DOL 2000 produced by Solvey Solex [10] was chosen as a suitable lubricant material in our case. HFE (NOVEC HFE-7100) provided by 3M [11] was selected as the solvent to dilute the PFPE. The mixing rate was in the weight ratio of one PFPE to a thousand HFE. The mixed solution was agitated for 5 minutes at room temperature by using a magnetic stirrer (SRS111AA) manufactured by ADVANTEC [12]. The lubricant film was coated by taking

advantage of the same procedure as the water drying method applied to the cleaning/rinsing procedure of the surface of the platter. Whenever unevenness such as a striped pattern and so on of the lubricant film was visually observed, the procedure was tried to repeat until the wavy surface of the lubricant layer on the platter appeared to become as unremarkable as possible.

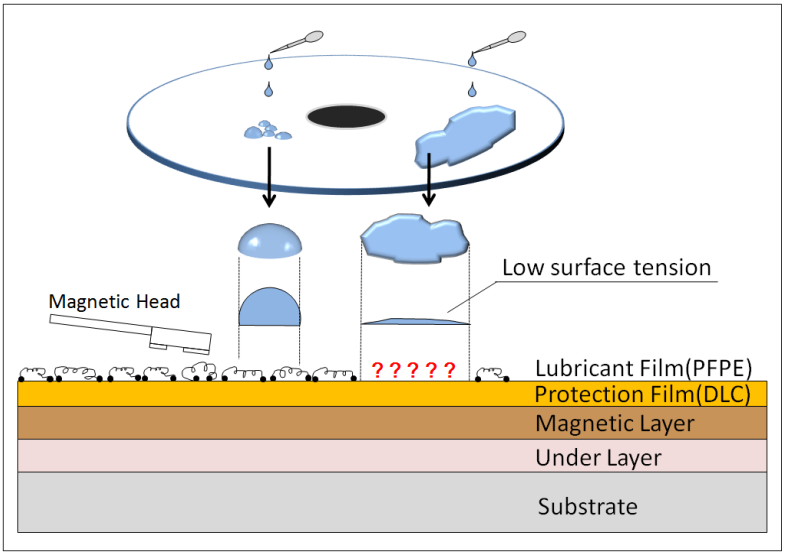

Fig. 5. Conceptual drawing of the platter's layers and its surface

It is empirically understandable that the thickness of the lubricant film should be ideally thin so that the platter rotation won't suffer from more friction between the magnetic head and the lubricant film than necessary. Moreover, there is also the disadvantageous possibility that too thick a layer could create a surplus distance between the magnetic head and the platter, which might prevent the head from picking up the magnetic signals recorded on the platter. An article reports that ideal thickness of the lubricant film is about 1 nm for a platter with the recording density of 100Gbit/inch^2 [13]. After the appropriate treatment to the relevant platter, the processed circular disk was installed into a target HDD whose flash ROM had been already replaced as well so that the digital data stored inside was ready to be extracted.

3.3 Power-on Sequence

The operational sequence of the HDD at power-on includes the execution of several internal tests such as the MPU bus test and register read/write test at the first stage [14, 15]. After the self-diagnosis is successfully completed, the spindle motor installed in the HDD starts functioning. When it is confirmed that the spindle motor has gained expected speed, the magnetic head is loaded on the platter. Then, the HDD

puts the head onto the SA area and reads the system information. Based on the obtained information from the procedure, a requirement to execute self-calibration is set up. The mechanical sound generated during the power-on sequence sometimes also gives a useful hint as to whether the HDD functions normally or not. When every procedure is fully prepared, the HDD gets ready for communicating with the host.

Even if the visual appearance of a HDD looks fine, it is important to make sure that logical interface functions appropriately. A HDD has numerous registers that allow the host to send commands and access different bits of information. Status Register is one of them that contains the current status of the HDD including the Busy bit (BSY), Device Ready bit (DRDY) and Device Seek Complete (DSC) bit. BSY shows when the HDD is waiting for a command to complete. While DRDY indicates that the HDD is ready to accept a command, DSC shows that the magnetic head is positioned over the platter. In our case, PC-3000 developed by ACE Laboratory [16] was utilized to check the Status Register of the re-assembled HDD, and Adapter PC-2" was selected as a connecting interface between the 2.5" HDD and PC-3000 hardware. Errors in the Status Register identified by PC-3000 were good indicators showing us whether the data extraction was going well or not. There were cases in which the data extraction process appeared to be suspended without making any noises usually coming from the internal movement of the HDD. In these cases, the platters once installed in the body of the new HDD was detached again, and the cleaning procedure described in the previous section was repeated until the re-assembled HDD became fully ready for the data extraction.

4 Data Extraction Procedure

Various kinds of tools for HDDs duplication are available now. Hard disk duplicators allow copying a hard drive to other HDDs. In most cases, the data recorded by the users is completely imaged from the seized HDD to another HDD so that the digital data inside could be analyzed while the seized HDD is kept untouched. However, in our case, the full imaging of the master HDD was abandoned because the platter formerly installed in the original HDD was found to still contain too many error sectors to advance further analyses even after the appropriate handling process had been taken. It is recognized that there are several cases that error sectors give bad influences on a platter in a HDD. A magnetic head installed there tends to move repeatedly on a particular area, trying to catch the magnetic signals written there in vain since the error sectors prevent the head from capturing them correctly. Staying on a particular area could make a head stick to the platter, which might result in a functional disorder of the HDD in the end.

In order to avoid the abovementioned problems and make sure of the maximum recovery of necessary data, file-based extraction procedure was chosen. A specialized software product, DATA Extractor UDMA, functioning in tandem with the PC-3000 hardware-software system enables a user to extract the information regarding Master Boot Record (MBR) and Master File Table (MFT) [17]. While the MBR contains a partition table that describes where particular partitions are located, the MFT stores

the details of all files such as metadata about every file, directory and so on. The MBR and MFT are very useful in finding out the names of data files and the locations where the files are recorded on the data storage. In our case, four critical data files needed restoring. Once the locations of all data were specified, the file-based extraction method worked very well. All of the four data files were successfully imaged to another HDD for duplicating data. In fact, the data files rescued from the damaged HDD were associated with GPS trajectory datasets, and contributed to the closure of the particular investigation.

5 Discussion

5.1 Cleaning Method of Platters

The functioning frequency of the cleaner utilized in this experiment was fixed at 40 kHz due to its limited performance. Namely, we had no choice but to use it at the frequency. In addition, the temperature of the pure water in which the platter was cleaned was also the maximum temperature that the cleaner could achieve. Thus, the frequency and the temperature applied in this experiment weren't variable parameter but fixed values in our case. Accordingly, different parameters weren't necessarily attempted in the course of cleaning the platter. These parameters applied in this experiment seem to have been successful, but there is still room for the improvement to make the analysis results more robust.

Moreover, there is an opinion that a platter's exposure to a solution for a long duration in an ultrasonic cleaner may do damage to the magnetic signals recorded on the platter [18]. The variable parameters such as the length of time, temperature and frequency associated with the ultrasonic cleaning procedure need to be optimized so that a full recovery of digital data stored in the platter can turn out to be successful.

5.2 HDDs with Multiple Platters

The damaged HDD dealt with in this experiment had only one 2.5" platter inside. However, it goes without saying that there are various types of HDDs in the global marketplace. Some have a 3.5" platter and others contain multiple numbers of the platters. In our case of a single 2.5" platter, little attention was needed in the process of putting the platter in the original onto the new HDD. On the contrary, it has already been experienced that the situation changes in handling 3.5" platters. This larger platter of 3.5" seems to require more precise and higher technique in re-assembling a HDD, and the platter installation should be paid more careful attention to. Even a very small flaw in assembling the parts would make it impossible to retrieve data from the platter. Besides, when it comes to a HDD with multiple platters, it is essential to anchor the several platters as they are, and ideally never to change their way of being fastened whenever they are required to be detached from the HDD body. In order to effectively cope with such an apparently difficult situation, it is necessary to develop technical skills regarding how to fix the orientations of all platters. Again, several trials have been attempted so far, aiming at effectively taking care of such HDDs with

multiple platters. Since it has already been recognized as a key skill how precisely the relative position of the platter against the magnetic head can be restored, technical advancement in the related field is strongly expected in order to appropriately re-assemble the HDD and make certain of extracting crucial data stored in damaged data storages.

6 Conclusion

A successful experience in rescuing digital data from a submerged HDD was reported in this paper. Though the outward appearance of the originally brought-in HDD was so devastated, the platter installed in the HDD seemed to survive physical damages. In fact, the platter was fortunate enough not to suffer from any physical deformation especially in the SA on the platter. After taking appropriate cleaning procedures, new lubricant film was coated on the platter for the purpose of re-assembling all necessary device parts into a HDD, and restoring the regular condition of a platter in a newly prepared HDD. The platter going through the cleaning and lubricating procedures was transplanted into another HDD body. Consequently, the essential digital data stored in the platter of the seized HDD was successfully extracted by utilizing the functions of PC-3000. The restored data contributed to furthering the relevant investigation effectively.

Since there were various parameters to be confirmed in order to successfully conduct the cleaning procedure, further experiments should be attempted, aiming at finding out the most reasonable and appropriate methods to clean platters in HDDs, and making them re-functional after the precise re-assembling for retrieving data. Recently, the number of HDDs composed of multiple platters inside is increasing due to the public popularity for large data volume capacity. It will be one of the most important assignments how to extract data from such HDDs with multiple platters in the near future.

Acknowledgments. We wish to acknowledge Shigeo Hattori, Kiyoshi Kuniura, Mamoru Takahashi, and Toshimi Murata for their guidance and support of this project.

References

1. dataclinic, http://www.dataclinic.co.uk/data-recovery-spinstand.html
2. Mayergoyz, I.D., Tse, C.: Spin-stand Microscopy of Hard Disk Data. Elsevier Series in Electromagnetism (2007)
3. Tseng, C.Y.: The study and development of automatic data acquisition system for spin-stand imaging and drive independent recovery of hard disk data. Dissertation Submitted to the Faculty of the Graduate School of the University of Maryland (2007)
4. ASONE, http://www.as-1.co.jp
5. Monthly Journal of Tribology (192), 49–51 (2003)

6. Speedfam Clean System Co., Ltd., http://www.speedfam-clean.jp/pdf/05onjunsuikansou.pdf
7. Zhang, H., Mitsuya, Y., Fujikawa, Y., Fuwa, A., Fukuzawa, K.: IEEE Transaction on Magnetics 45(10), 3632–3635 (2009)
8. Gao, C., Lee, Y.C., Chao, J., Russak, M.: IEEE Transaction on Magnetics 31(6), 2982–2984 (1995)
9. Lee, H., Bhusan, B.: Journal of Colloid and Interface Science 353, 574–581 (2011)
10. Solvey Solex, http://www.solvaynorthamerica.com
11. 3M, http://solutions.3m.com/wps/portal/3M/en_US/Novec
12. Advantec, http://www.advantec.co.jp/english/index.html
13. Monthly Journal of Tribology (187), 12–14 (2003)
14. Fujitsu, MHT-AH Series, http://www2.fcpa.fujitsu.com/sp_support/ext/mobile/datasheets/mht5400rpm-datasheet.pdf
15. Fujitsu, MH2080AH, MHT2060AH, MHT2040AH Disk Drives Product Manual, http://www.fujitsu.com/downloads/COMP/fcpa/hdd/discontinued/mht20xxah_prod-manual.pdf
16. ACE Laboratory, http://www.acelaboratory.com/index.php
17. ACE Laboratory, http://www.acelaboratory.com/dataextractor.php
18. Private discussion with a data recovery vendor