U.S. Department of Justice
Drug Enforcement Administration

www.dea.gov

Microgram Bulletin

Published by:
The Drug Enforcement Administration
Office of Forensic Sciences
Washington, DC 20537

The U.S. Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by the Department of Justice. Information, instructions, and disclaimers are published in the January issues.

- SEPTEMBER 2006 -

- INTELLIGENCE ALERT -

MUSHROOMS LACED WITH *GAMMA*-HYDROXYBUTYRIC ACID (GHB) AT A METHAMPHETAMINE LABORATORY IN MIDWEST CITY, OKLAHOMA

The Oklahoma State Bureau of Investigation Central Regional Laboratory (Oklahoma City) recently received a dark brown glass jar containing apparent psilocybe mushrooms (see Photo 1). The exhibit was seized at a clandestine methamphetamine laboratory by the Midwest City Police Department (Midwest City is a suburb of Oklahoma City). The mushrooms (total net mass approximately 3 grams) had the texture and odor typical of psilocybe mushrooms; however, derivatization with bis(trimethylsilyl)trifluoroacetamide (BSTFA) followed by analysis by GC and GC/MS indicated neither psilocin or psilocybin but rather *gamma*-hydroxybutyric acid (GHB; not quantitated, but a rather low loading based on the gas chromatogram). This

Photo 1

is the first ever submission of GHB-laced mushrooms to the laboratory.

[Editor's Notes: The analyst in this case has analyzed several dozen cases of psilocybe mushrooms, and feels that these were in fact psilocybe mushrooms that had been intentionally laced with GHB. It is unclear why the mushrooms were negative for psilocin or psilocybin.]

* * * * *

- INTELLIGENCE ALERT -

ECSTASY MIMIC TABLETS (CONTAINING *META*-CHLOROPHENYL-PIPERAZINE (MCPP)), AND CAPSULES CONTAINING 2,5-DIMETHOXY-4-IODOPHENETHYLAMINE (2C-I), IN IOWA

The Iowa Criminalistics Laboratory (Ankeny, Iowa) recently received 44 multi-colored tablets with no logo, suspected Ecstasy (see Photo 2). The exhibits were seized by the Iowa City Police Department (circumstances unknown; Iowa City is in southeastern Iowa). Analysis of the tablets (not weighed, 9 x 3.5 millimeters) by TLC and GC/MS, however, indicated not MDMA but rather *meta*-chlorophenylpiperazine (mCPP; not quantitated, but a moderate loading based on the TIC). This is the first submission of mCPP to the laboratory.

Photo 2

The laboratory also recently received 6 clear capsules, each containing a small amount of white powder, submitted as an unknown/suspected controlled substance (photo not taken, but the same as those pictured in the January 2006 issue of *Microgram Bulletin* (page 3)). The exhibits were seized by the Marion Police Department (circumstances unknown; Marion is in eastern Iowa). Analysis of the powder (not weighed) by Marquis, TLC, and GC/MS indicated 2,5-dimethoxy-4-iodophenethylamine (2C-I; not quantitated but apparently high purity based on the TIC). The identification was tentative, due to the lack of a reference standard. This is the second submission of presumed 2C-I to the laboratory; the first occurred in 2004.

* * * * *

- INTELLIGENCE ALERT -

ECSTASY MIMIC TABLETS (CONTAINING *META*-CHLOROPHENYL-PIPERAZINE (mCPP)) IN FRISCO, TEXAS

The Texas Department of Public Safety Crime Laboratory in Garland recently received 6 beige tablets and partial tablets with the Mitsubishi logo on one face and half-scored on the opposite face, resembling previously submitted Ecstasy tablets (see Photo 3, next page). The exhibits were seized by the Frisco Police Department (circumstances not provided; Frisco is a northern suburb of Dallas). Analysis of the tablets (total net mass of intact and partial tablets 1.70 grams) by color tests, UV, and GC/MS, however, indicated not MDMA but rather *meta*-chlorophenyl-

Photo 3

piperazine (mCPP; not quantitated but a moderate loading based on the TIC). This was the first submission of mCPP to the laboratory.

* * * * *

- INTELLIGENCE BRIEF -

DEGRADED KHAT (FROM PARIS, FRANCE) AT THE NORTHERN KENTUCKY/CINCINNATI AIRPORT, KENTUCKY

Photo 4

The Kentucky State Police Northern Regional Laboratory (Cold Spring) recently received 75 bundles of apparent khat (see Photo 4). Each bundle contained 4 smaller sub-bundles, and was wrapped in the standard manner, in a large leaf secured with a husk-like twine. The exhibits (total net mass approximately 13 pounds) had been shipped in a cardboard box from Paris, France to the Northern Kentucky/Cincinnati Regional Airport, and were seized by U.S. Customs and Border Protection agents. Unusually, there was no effort to cool the material during shipping, and it had a moist and distinctly wilted appearance, with signs of mold, upon receipt at the laboratory. Analysis of extracts by GC and GC/MS indicated no cathinone, but confirmed cathine (not quantitated). It was estimated that the package had been in transit for at least 14 days prior to its seizure, explaining its degraded appearance and complete loss of cathinone. This is the second submission of khat to the laboratory; the first was submitted approximately 5 years ago. Cathine is a Schedule IV controlled substance under Kentucky law.

* * * * *

- INTELLIGENCE ALERT -

WALL HANGINGS CONTAINING COCAINE FROM GUATEMALA AT MIAMI AIRPORT, FLORIDA

The DEA Mid-Atlantic Laboratory (Largo, Maryland) recently received 7 multicolored fabric wall hangings with wooden dowels at each end (see Photos 5 and 6). The dowels were hollowed out, and contained white powders, suspected cocaine (see Photo 7). The exhibits were seized by Immigration and Customs Enforcement personnel from a parcel service flight from Guatemala to Miami, and were submitted to the laboratory after a controlled delivery in the mid-Atlantic region (details not available). The dowels were 18 inches long by about 1 ½ inches in diameter, and were outfitted with end caps which appeared to be glued on. Analysis of the powder (total net mass 439.3 grams) by GC, MS, and IR confirmed 90 percent cocaine hydrochloride. This was the Mid-Atlantic Laboratory's first encounter with this smuggling technique.

Photo 5

Photo 6

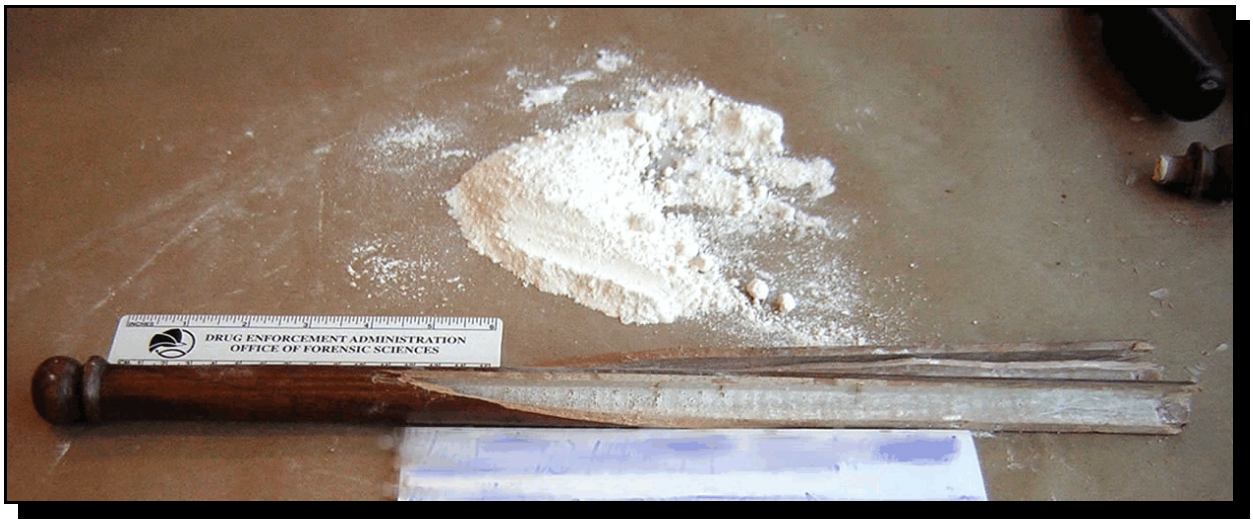

Photo 7

* * * * *

- INTELLIGENCE ALERT -

POLYDRUG SEIZURE (MDMA POWDER, ECSTASY TABLETS, QUAALUDE MIMIC TABLETS (CONTAINING DIAZEPAM), AND MARIJUANA) NEAR OROVILLE, WASHINGTON

Photo 8

The DEA Western Laboratory (San Francisco, California) recently received a polydrug seizure including: A) 5 boxes each containing 12 food saver plastic bags of white powder, suspected methamphetamine (see Photo 8); B) 30,004 red tablets with an infinity logo, suspected MDMA (no photo); C) 10,890 white tablets with a Lemmon 714 logo on one face and half-scored on the opposite face, apparent Quaalude tablets (no photo); and D) 477 grams of plant material, suspected marijuana (no photo). The exhibits were seized near the U.S./Canadian border by agents from the U.S. Border Patrol Office in Oroville, Washington (circumstances not provided). Analysis of the powder (total net mass 59.57 kilograms) by FTIR and GC/MS indicated not methamphetamine but rather 86 percent MDMA hydrochloride. Analysis of the red/infinity logo tablets by GC, GC/MS, and GC/IRD confirmed MDMA hydrochloride (94 milligrams/tablets). Analysis of the white/Lemmon 714 logo tablets by GC, GC/MS, and GC/IRD indicated not methaqualone but rather diazepam (39 milligrams/tablet). Analysis of the plant material by microscopy, Duquenois-Levine, TLC, and GC/MS confirmed marijuana. This was the largest ever submission of powdered MDMA hydrochloride to the Western Laboratory.

* * * * *

- INTELLIGENCE BRIEF -

PCP LABORATORY IN SOUTH HOLLAND, ILLINOIS

The DEA North Central Laboratory (Chicago, Illinois) recently assisted the DEA Chicago Field Division, the South Chicago HIDTA Task Force, and the South Holland, Illinois Fire Department in the seizure of a clandestine phencyclidine (PCP) laboratory located in a house in South Holland (a suburb of Chicago). The laboratory was inactive at the time of its seizure, and appeared to primarily be a storage site for chemicals used in the synthesis of PCP, as well as for PCP base which had not been extracted from reaction mixtures. However, sales of PCP were active and ongoing prior to the raid. Chemicals found at the site included 2 unlabeled one-gallon

cans of cyclohexylamine, 4 gallons of cyclohexanone, approximately 4 gallons of ether, and 50 pounds of white powder (analysis by FTIR and uranyl acetate microcrystalline test identified the latter substance as potassium cyanide). Also recovered at the residence were 73 two-quart mason jars containing bi-layered liquids with volumes varying between 200 - 500 milliliters. Analysis of the top (organic) layers by GC/MSD indicated cyclohexanone, bromobenzene, cyclohexylpiperidine, biphenyl, 1-piperidinocyclohexene, PCC, and PCP. Analysis of chloroform extracts of the lower (aqueous) layers by GC/MSD indicated residual amounts of the same compounds identified in the organic layers. The search also recovered printed Internet procedures for the preparation of Grignard reagents. This is the first PCP lab which the North Central Laboratory has responded to in over 2.5 years. Followup investigations determined that the lab had been in operation for about 2 years, and that the cyclohexylamine was purchased in error by the laboratory operators (who mistakenly believed it could be used to manufacture PCP).

* * * * * * * * * * * * * * * * * * * * * * * * *

SELECTED REFERENCES

[Selected references are a compilation of recent publications of presumed interest to forensic chemists. Unless otherwise stated, all listed citations are published in English. Abbreviated mailing address information duplicates that provided by the abstracting service. Patents and Proceedings are reported only by their *Chemical Abstracts* citation number.]

1. Block R. **Cocaine base to soup.** Journal of the Clandestine Laboratory Investigating Chemists Association 2006;16(3):21. [Editor's Notes: Reports on the re-analysis of partially decomposed samples of cocaine base that had been stored in metal paint cans for 6 years. *JCLICA* is a law enforcement restricted journal. Contact: Wisconsin State Crime Laboratory, 4626 University Ave., Madison, WI 53705-2156.]

2. Carter JF, Sleeman R, Hill JC, Idoine F, Titterton EL. **Isotope ratio mass spectrometry as a tool for forensic investigation (examples from recent studies).** Science & Justice 2005;45(3):141. [Editor's Notes: An overview and minor review. Includes Ecstasy tablets and heroin samples as examples. Contact: Mass Spec Analytical Ltd., Filton, Bristol BS99 7AR, UK.]

3. Hanna GM. **NMR regulatory analysis: Enantiomeric purity determination for R-(-)-desoxyephedrine and antipode methamphetamine.** Pharmazie 2006;61(3):188. [Editor's Notes: The title study was performed using a 400 MHz NMR and a chiral solvating agent (not specified in the abstract). The purpose was to determine the enantiomeric purity of R-(-)-methamphetamine in nasal decongestant sprays. Contact: Northeast Regional Laboratory, Food and Drug Administration, Jamaica, NY 11435-1034.]

4. Jiang D, Wei Y, Zhao G, Cheng C. **Research of IMS technology and its application in narcotic drugs and explosives detection.** Tongweisu 2005;18(1-2):51. [Editor's Notes: Narcotics and explosives were not specified in the abstract. This article is written in Chinese. Contact: Shanghai Institute of Applied Physics, Chinese Academy of Sciences, Shanghai 201800, Peop. Rep. China.]

5. Kitlinski LM, Harman AL, Brousseau MM, Skinner HF. **Reduction of phenylephrine via hydriodic acid - red phosphorus or iodine - red phosphorus: 3-Hydroxy-N-methylphen-**

ethylamine. Journal of the Clandestine Laboratory Investigating Chemists Association 2006;16(3):12. [Editor's Notes: Presents the title study (phenylephrine-containing products are replacing pseudoephedrine-containing products across the United States). *JCLICA* is a law enforcement restricted journal. A slightly different version of this article was co-published in: *Microgram Journal* 2005;3(3-4):142. Contact: U.S. Department of Justice, Drug Enforcement Administration, Southwest Laboratory, 2815 Scott Street, Vista, CA 92081.]

6. Kuwayama K, Tsujikawa K, Miyaguchi H, Kanamori T, Iwata Y, Inoue H, Saitoh S, Kishi T. **Identification of impurities and the statistical classification of methamphetamine using headspace solid phase microextraction and gas chromatography - mass spectrometry.** Forensic Science International 2006;160(1):44. [Editor's Notes: The title techniques can be used for impurity profiling and discrimination. Contact: First Chemistry Section, National Research Institute of Police Science, 6-3-1, Kashiwanoha, Kashiwa-shi, Chiba 277-0882, Japan.]

7. McFadden K, Gillespie J, Carney B, O'Driscoll D. **Development and application of a high-performance liquid chromatography methods using monolithic columns for the analysis of ecstasy tablets.** Journal of Chromatography A 2006;1120(1-2):54. [Editor's Notes: Presents the title study. "A large number of Ecstasy tablets seized in Ireland" were analyzed. Contact: Science Research Department, Letterkenny Institute of Technology, Donegal, Ire.]

8. Nerkis S, Oruc HH. **Determination of amounts of the active substance and added substances in cannabis, heroin, and ecstasy tablets used in Bursa and in the Bursa region.** Bagimlilik Dergisi 2006;7(1):11. [Editor's Notes: 21 Cannabis, 55 heroin, and 65 Ecstasy tablet exhibits were characterized by GC/MS and FTIR. This article is written in Turkish. Contact: Bursa Leg. Med. Soc., Turk.]

9. Person EC, Savopolos JA. **Elemental identification of lithium in clandestine laboratory casework by atomic emission spectroscopy.** Journal of the Clandestine Laboratory Investigating Chemists Association 2006;16(3):23. [Editor's Notes: Presents the title study. *JCLICA* is a law enforcement restricted journal. Contact: Department of Forensic/Analytical Chemistry, California State University, Fresno, 2555 East San Ramon Ave., SB/70, Fresno, CA 93740.]

10. Poortman-Van Der Meer A. **The synthesis of MDMA with $NaBH_4$ as the reducing agent; the "Cold Method."** Journal of the Clandestine Laboratory Investigating Chemists Association 2006;16(3):10. [Editor's Notes: Details withheld in accordance with *Microgram* policy. *JCLICA* is a law enforcement restricted journal. Contact: Netherlands Forensic Institute, Postbus 24044 The Hague, The Netherlands.]

11. Sasaki T, Makino Y. **Effective injection in pulsed splitless mode for impurity profiling of methamphetamine crystal by GC or GC/MS.** Forensic Science International 2006;160(1):1. [Editor's Notes: 48 samples were analyzed. The technique minimized thermal decomposition, and the results can be used for impurity profiling and discrimination. Contact: Entest Japan, 7-13-8 Higashi Shinkoiwa, Katsushika-ku, Tokyo 124-0023, Japan.]

12. Shibuya EK, Souza-Sarkis JE, Negrini-Neto O, Moreira MZ, Victoria RL. **Sourcing Brazilian marijuana by applying IRMS analysis to seized samples.** Forensic Science International 2006;160(1):35. [Editor's Notes: The results allowed differentiation of marijuana grown in dry versus wet areas of Brazil. Contact: Laboratorio de Caracterizacao Quimica e Isotopica, Centro de Quimica e Meio Ambiente, Instituto de Pesquisas Energeticas e Nucleares, IPEN/CNEN-SP, Av. Lineu Prestes 2242, Cidade Universitaria, Sao Paulo, SP CEP 05508-900, Brazil.]

13. Tanner-Smith EE. **Pharmacological content of tablets sold as "Ecstasy": Results from an online testing service.** Drug and Alcohol Dependence 2006;83:247. [Editor's Notes: Presents the title study and results. Tablets were submitted anonymously, from 1999 to 2005. Contact: Department of Sociology, VU Station B Box 351811, 2301 Vanderbilt Place, Vanderbilt University, Nashville, TN 37235-1811.]

* *

SCIENTIFIC MEETINGS

1. Title: 32nd Annual NEAFS Meeting (Third and Final Bimonthly Posting)
Sponsoring Organization: Northeastern Association of Forensic Sciences
Inclusive Dates: November 1 - 4, 2006
Location: Tarrytown DoubleTree Hotel (Westchester County, New York)
Contact Information: E. Schwartz (914 / 231-1810 or ess6 -at- westchestergov.com)
Website: None Provided

* *

NEW EMAIL ADDRESSES NEEDED

The email addresses for the following organizations returned rejection notices to the *Microgram* Editor for at least the past three issues of *Microgram Bulletin*, and therefore the respective organizations have been dropped from the subscription list. Note that the errors include "mailbox full", "over quota", "user not found", or "user unknown" messages, and also a variety of anti-spam/filtering rejection messages (the latter likely resulting from failure to "whitelist" the microgram_editor@mailsnare.net address). The *Microgram* Editor requests your assistance in contacting these organizations, determining if they wish to remain on the *Microgram* subscription e-net, and if so asking them to forward a valid email address to the microgram_editor@mailsnare.net address. In addition, if the Office has closed or is known to be no longer interested, please forward that information to the *Microgram* Editor.

U.S. Subscribers (by State):

Colorado - Grand Junction Police Department Laboratory;

Florida - St. Cloud Police Department;

Indiana - LaPorte City Police Department;

Kansas - Kansas Bureau of Investigation/Pittsburg Laboratory;

New Jersey - Franklin Township Police;

Texas - Fort Worth Police Department/Crime Laboratory.

Non-U.S. Subscribers (by Country):

Switzerland - Stadpolizei Zurich;

United Kingdom - Strathclyde Police Headquarters (Glasgow, Scotland);

Uraguay - Prefectura Nacional Naval (Montevideo).

Computer Corner #210

The Hard Disk "Security Mode Feature Set"

by Clay Schilling
Group Supervisor
DEA Digital Evidence Laboratory

The rapid rate of change in computer technology is a continuous challenge for digital evidence examiners. In most cases, these changes are technical improvements in software or hardware. More recently, however, the fallout from a non-technological issue is creating a significant operational challenge for digital evidence examiners, that being **information security**. The loss and/or criminal mis-use of personal information has rapidly become a paramount issue for both individuals and organizations. In an effort to combat the problem, many digital technology users have implemented some form (or forms) of information security. This represents a major shift in public attitudes and behavior - five years ago, protecting personal information was (on average) a low priority for users - but now it is a major concern.

One of the better-known forms of information security is data encryption, which is generally defined as "the process of obscuring information to make it unreadable without special knowledge." To read encrypted data, you must provide a key or password that allows it to be decrypted. Data encryption has been around for many years, as evidenced by the numerous software and hardware products that are currently available to perform it. As noted above, however, until recently encryption was not commonly utilized by most users.

While both software and hardware encryption protocols present unique problems for computer forensic examiners, this article will only focus on the issues presented by a specialized "pseudo-encryption" technique - the "security mode feature set" found on most modern hard disks that have an Advanced Technology Attachment (ATA) interface. The "security mode feature set" is a hard disk firmware-implemented password lock that was first defined in the ATA-3 Interface standard published in 1997 as American National Standards Institute (ANSI) standard X3.298-1997. Since that date, nearly all manufactured ATA hard disks (such as Integrated Device Electronics (IDE, also known as Parallel ATA or P-ATA), and Serial ATA) have had this capability built in, but until recently it has been only rarely used. "The security mode feature allows a host [that is, the computer] to implement a security password system to prevent unauthorized access to the internal disk drive" (http://www.t13.org). Support of this feature is indicated in Word 128 of the Identify Device response command, which enables the host to receive parameter information from the internal disk drive during the boot sequence.

Many subject matter experts do not believe that this security feature is a true encryption protocol, because it does not actually encrypt the information on the disk; rather, it makes the disk inaccessible until the proper password is provided. However, it does meet the basic definition, since the information cannot be read without the password.

The "security mode feature set" uses two independent 32-byte passwords, one "user" and one "master," and specifies one of two security modes - "high" and "maximum." Each password must be at least 4 characters in length. The "user" password enables the security feature, blocking access to all user data on the hard disk. The "master" password can be used to unlock the hard disk if the "user" password is lost or if an administrator requires access. Providing an incorrect "user" or "master" password does nothing to the hard disk or the information it contains; rather, the hard disk cannot be accessed until the correct password is entered. A password ("user" or "master") can only be provided a maximum of five times before the system must be reset or power-cycled. The passwords can be set using either the system's Basic Integrated Operating System (BIOS) or with third party tools.

The security mode dictates whether the "master" password is used only to "unlock" the hard disk and access the data ("high"), or instead is used to "unlock" the hard disk and wipe the data ("maximum"). That is, use of the "master" password when the security mode is set to "maximum" will prompt the computer to erase all the information by writing zeros onto all sectors of the hard disk before allowing access to it - a fatal error for a digital evidence examiner. Because this action destroys the data (including any potential evidence), the examiner must first determine the security mode before even thinking about applying the "master" password, and obviously the examiner can never use the master password if the security mode is set to "maximum." The security mode cannot be either determined or set in the BIOS, and therefore only third party disk utility software can be used. The level is set to "high" by default.

The passwords and large sections of the hard disk's firmware are stored on the non-user accessible service area of the disk, and not on the controller card or mother board. Therefore, when a hard disk password is set, it travels with the device, so the disk is protected even if it is placed in another computer. This means that the password cannot be bypassed by replacing the controller card, or by removing the complementary-symmetry/metal-oxide semiconductor (CMOS) battery, or by adjusting jumper settings to "reset" it.

When engaged, the "security mode feature set" presents digital evidence examiners with some interesting challenges - the first being determining whether the hard disk is password protected, and the second being determining what security mode is set, "high" or "maximum." Knowing which password was used to lock the disk is not critical, as either will grant access to the data. However, as noted above, knowing what security mode is set is of paramount importance, as utilizing the "master" password when the security mode is set to "maximum" will result in complete loss of the data.

Obviously, if the disk is password protected in this manner, it is not possible to obtain a usable image (copy) for forensic analysis without providing the password, or bypassing it.

Determining the Security Status of a Disk

If the hard disk is removed from a computer and attached to a forensic examination system via a write-blocking device it may or may not prompt for a password. Forensic software may be able to obtain an image, but it will not be exploitable. The problem will be apparent when the examiner notes that the disk is identified as "unused disk space" despite the fact it appears to contain a large amount of random characters that span a significant portion of the disk. This is different than a hard disk that presents itself as "unallocated disk space," which usually indicates some sort of proprietary hardware issue (frequently encountered with laptop systems). Either scenario can be identified by either previewing the disk prior to imaging or by utilizing diagnostic software or other similar specialized third party tools that are designed to identify a disk's security status. If the preview identifies the disk as "unused disk space" or "unallocated disk space", diagnostic software must be used to determine whether or not it is locked. If the disk is locked, the "security mode feature set" has been activated. If the disk is not locked, a hardware proprietary issue is more likely; this can be overcome by obtaining an image using a forensic or controlled boot disk. [Note: Caution must be exercised when using diagnostic software or other third party tools, as they may not be forensically sound and might alter the disk's contents.]

As noted above, the password is stored on the hard drive itself, which means it cannot be bypassed by replacing the controller card, by flashing the memory chip, by transferring the hard disk to another computer, or by running a "brute force" password cracking attack against it (the latter approach is impractical because of the security feature's maximum five attempts per power-cycle limit). However, there are still a few approaches that can be used to obtain the password, the first of which is getting it directly from the computer system owner/user. This of course is only effective if the owner/user is cooperative and was responsible for setting the password. As always, caution should be used when utilizing any information obtained from a perceived cooperating witness, as they may actually be providing false information intended to corrupt or mislead; for example, providing the master password

and stating that the security mode is set to high when it is actually set to maximum. Any information obtained from a witness should be verified before it is used. The second method involves conducting a search for the password around the computer itself. Many individuals write their passwords down on a piece of paper and keep it close to their computer. Whether it is, e.g., taped to the monitor, hidden under the keyboard, or stored in a file, it is definitely worthwhile to conduct an extensive search of the area surrounding the computer. This information could also be malicious, and therefore it (like witness statements) also has to be verified prior to use. The third method involves enlisting the assistance of the hard disk's manufacturer (such as Seagate, Western Digital, or Hitachi) or the computer system's manufacturer (such as Dell, Gateway, and Hewlett Packard). According to the ATA-3 specification, "the Master Password shall be set to a vendor specific value during manufacturing and the lock function disabled." This original password can also be reset by a computer system manufacturer, which means it may be possible to obtain the "master" password by coordinating with the hard disk's or computer system's manufacturer. Most reputable manufacturers have no problem assisting law enforcement with these types of requests, but they will require specific information such as serial, model, and product numbers for the targeted computer system and/or hard disk, and they may require a subpoena before they release any passwords. Once again, however, it is critical to remember that the "master" password cannot be used if the security mode has been set to "maximum".

The last method requires specialized forensic hardware that is designed to intercept the boot sequence, access the hard disk, and obtain the stored password. This method is used by a few digital forensics units and data recovery companies; unfortunately, it is currently very expensive. Digital forensics units without this technology should conduct extensive research into its cost effectiveness before pursuing this solution. Should purchasing this solution prove not to be feasible, an alternative is to coordinate with either larger digital forensics units or data recovery companies for assistance.

Once the password has been provided, the examiner is granted access to the hard disk, and it functions as any other hard disk would - until it is shut down. Shutdown reactivates the security feature, requiring the password to be re-entered upon restarting. The feature can be deactivated using either the BIOS or third party tools, but this is not a proper option for a digital forensic examiner, as the disk is evidence and should be write-blocked. Additionally, the image that is obtained will not be affected by the security feature as long as it is processed using forensic software.

As stated above, the security feature does not encrypt the disk's content - it merely prevents access. If the disk's contents are encrypted, once you access the disk you will either be prompted for another password as the computer's operating system initiates, or you will only be granted access to a generic desktop and have to initiate a decryption algorithm (which will require yet another password), in order to view the disk's contents. The details of disk encryption issues will be discussed in future articles.

As you can see the "security mode feature set" does make a computer forensic examiner's job a little more complicated, but it is nothing that a well-trained examiner cannot overcome. Additional information about this feature can be found at: http://t13.org/project/d2008r7b-ATA-3.pdf

Questions or comments? E-mail: Clayton.D.Schilling -at- usdoj.gov

* * * * *