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.

- MAY 2006 -

- INTELLIGENCE ALERT -

"GREENADES" (MARIJUANA GUMBALLS) IN HOWARD COUNTY, MARYLAND

The Maryland State Police-Forensic Sciences Division Laboratory in Pikesville recently received two yellow gumballs, each with a smiley face printed on one side and a bored hole filled with greenish-brown vegetable matter on the opposite side (see Photos 1, right, and Photo 2, next page). Both gumballs were wrapped in tin foil labeled as "Greenades" with a marijuana leaf and detailed instructions for use (see Photo 3, next page). The exhibits were seized by a school-assigned Police Officer from two high school students performing a purchase while they were passing between classes at a Howard County (Maryland) High School. Analysis of the plant material by microscopy, GC, GC/MS, Mayer's, and modified Duquenois-Levine confirmed marijuana (THC content not quantitated). Each gumball contained approximately one gram of marijuana, and the total net mass of the two gumballs was 17.5 grams. This was the first submission of "Greenades" to the Maryland State Police-Forensic Sciences Division.

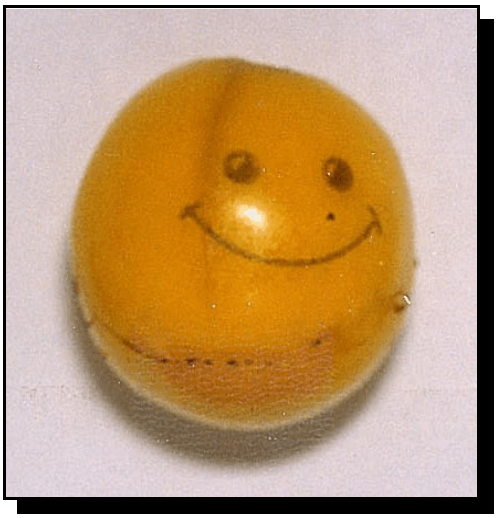


Photo 1

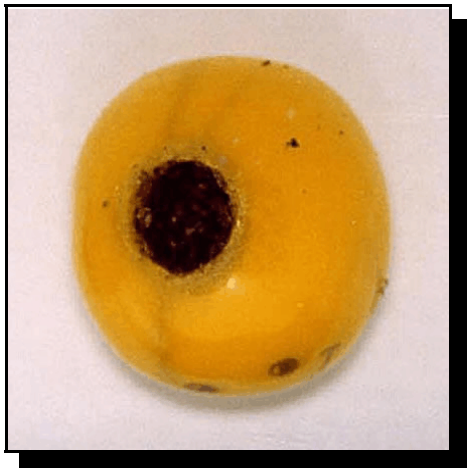


Photo 2

[Notes: The perimeter of the label includes instructions: "Take 30mins -1 hr before you would like receive your high" (and) "Chew for as long as possible, then swallow." Gumball diameter = About 1 inch.]

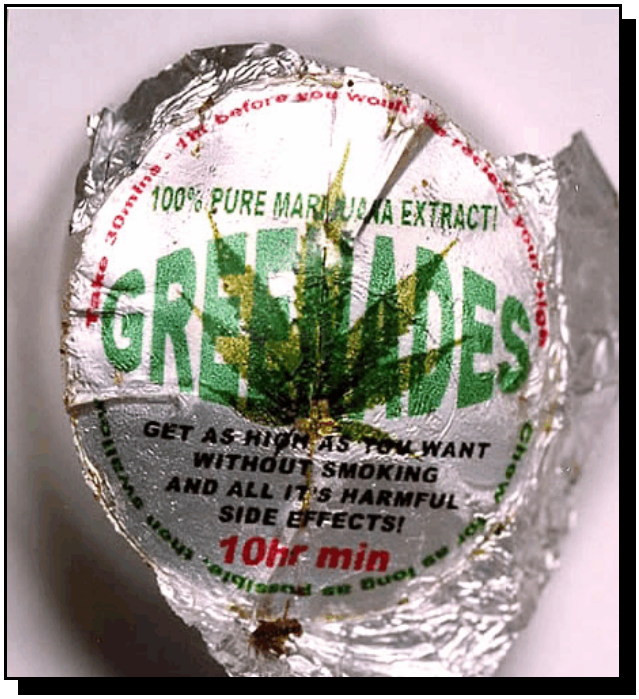


Photo 3

* * * * *

- INTELLIGENCE ALERT -

ECSTASY COMBINATION TABLETS (CONTAINING MDMA, KETAMINE, METHAMPHETAMINE, AND COCAINE) IN EAST BRUNSWICK, NEW JERSEY

The New Jersey State Police East Regional Laboratory (Sea Girt) recently received ten white tablets with a "Motorola" logo, suspected MDMA (see Photo 4). The tablets were acquired in East Brunswick by a detective from the Middlesex County Prosecutor's Office (circumstances unavailable). Analyses of the tablets (total net mass 2.79 grams) by color testing, GC/MS and GC/MS following derivatization indicated not only MDMA but rather a complex mixture of MDMA, ketamine, methamphetamine, cocaine, and possibly diphenhydramine (in approximately a 68 : 24 : 3.5 : 3.5 : 1 ratio). Interestingly, the Marquis color test suggested a complex mixture by changing from flash orange to yellow to dark purple/black. This was the first submission of tablets containing this combination to the laboratory.

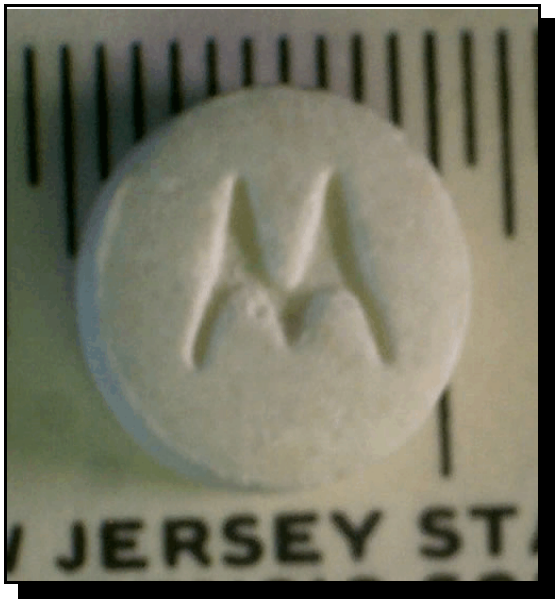


Photo 4

- INTELLIGENCE ALERT -

LSD BLOTTER ACID MIMICS (CONTAINING 4-IODO-2,5-DIMETHOXY-AMPHETAMINE (DOI)) IN ORLANDO AND WINTER SPRINGS, FLORIDA

The Florida Department of Law Enforcement's Orlando Regional Crime Laboratory recently received two separate submissions of apparent LSD "blotter acid," consisting of full sheets, pieces, and individual squares of a green index card-like paper with hash marks (photos not available). The exhibits were seized in Orlando and Winter Springs by their respective Police Departments (circumstances not available). Analysis of methanolic extracts by GC/MS, however, indicated not LSD but rather 4-iodo-2,5-dimethoxyamphetamine (DOI, not confirmed or quantitated due to lack of a reference standard). These were the first submissions of DOI in our laboratory.

[Editor's Notes: DOI is the amphetamine analogue of 2C-I (4-iodo-2,5-dimethoxyphenethyl-amine). According to the analyst, although not formally quantitated, the loading of DOI on the paper was "moderate". The analyst also indicated that the laboratory has not seen LSD blotter acid mimics in some time.]

* * * * *

- INTELLIGENCE ALERT -

BLACK TAR HEROIN SMUGGLED INSIDE A TEDDY BEAR IN EAST BATON ROUGE, LOUISIANA

The Louisiana State Police Crime Laboratory at Baton Rouge recently received ten small packages containing a dark tar-like substance, suspected black tar heroin (see Photo 5). The exhibits were seized in East Baton Rouge by the East Baton Rouge Parish Sheriff's Office, pursuant to a vehicle stop by the U.S. Border Patrol. All ten packages were hidden inside a teddy bear, which in turn was inside luggage in the vehicle. Each packet of the tar-like material was first wrapped in clear plastic, which was then wrapped in black tape. Analysis of the material (total net mass 222.50 grams) by GC/MS confirmed heroin (not quantitated, but only a moderate percentage based on the GC chromatogram). Black tar heroin is not routinely submitted to the laboratory, and this is also the laboratory's first encounter with the use of a teddy bear for smuggling a controlled substance.

[Editor's Note: The tenth package was opened for field testing, and subsequently leaked into the evidence envelope (as seen in Photo 5).]

Photo 5

- INTELLIGENCE ALERT -

ECSTASY MIMIC TABLETS (CONTAINING META-CHLOROPHENYL-PIPERAZINE (mCPP)) IN THE BALEARIC ISLANDS

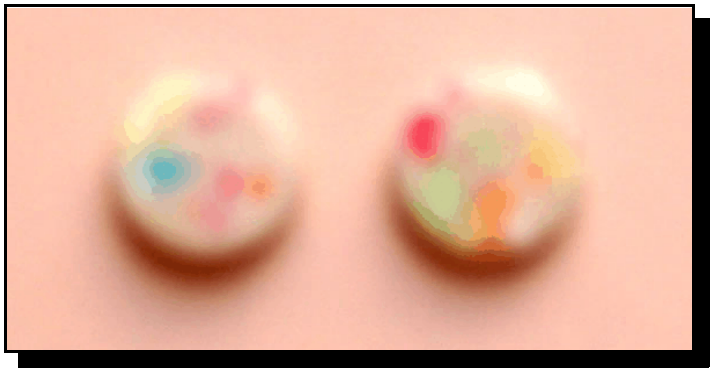


Photo 6

During 2005 the Laboratory of Drugs in The Balearic Islands (Spain) analyzed 17 separate submissions of apparent Ecstasy tablets (two different types) that did not contain MDMA but rather 1-(3-chlorophenyl)-piperazine (aka: *meta*-chlorophenylpiperazine, mCPP). All of them were seized by the Guardia Civil on Ibiza Island. One set (83 tablets total) was mottled blue, red, orange, and green, no logo, varying from 111 to 357 milligrams per tablet (total net mass 25.05 grams) (see Photo 6; note that this is the best available photo). The other set (298 tablets) was white, no logo, averaging 300 milligrams per tablet (total mass 89.35 grams) (photo not provided). The only common feature among the various sets of tablets was their notably poor manufacturing quality. Analyses were performed using GC-FID, GC/MS, and NMR (quantitations not performed due to lack of reference material). These were the first submissions of Ecstasy mimic tablets containing mCPP to the laboratory.

* * * * *

- INTELLIGENCE ALERT -

METHAMPHETAMINE CUT WITH UREA BEING ENCOUNTERED IN THE WESTERN UNITED STATES AND ALASKA

The DEA Western Laboratory (San Francisco, California) recently received an off-white crystalline substance wrapped in a clear plastic baggie, suspected methamphetamine (no photo). The exhibit was acquired in West Valley City, Utah, by agents from the DEA Salt Lake City Office (circumstances unavailable). Analysis of the substance (total net mass not provided) by FTIR, GC/MS, and NMR confirmed 13 percent methamphetamine hydrochloride, dimethyl sulfone, and urea. This is at least the seventh submission of methamphetamine samples cut with urea to the DEA Western Laboratory. Similar samples have been submitted over the past few months from Murray City, American Fork, and Layton, Utah, Anchorage, Alaska, Mount Vernon, Washington, and most recently from San Francisco, California. It is quickly becoming a more common trend.

[Analyst's Comments: The presence of urea in methamphetamine is of interest because the compound is not easily detected on GC/FID or GC/MS (it is sometimes observed as a low hill near the baseline, with only a few low mass fragments). In the above case, urea was identified in the methylene chloride insolubles by FTIR and NMR. Of further interest, urea does not interfere with either the Marquis or sodium nitroprusside color tests.]

- INTELLIGENCE ALERT -

COCAINE CONCEALED WITHIN THE WALLS OF A COOLER ARRIVING AT DULLES INTERNATIONAL AIRPORT

The DEA Mid-Atlantic Laboratory (Largo, Maryland) recently received a red cooler containing four plastic bags of white powder, suspected cocaine (see Photos 7 and 8). The cooler was seized by Immigration and Customs Enforcement (ICE) personnel at Dulles International Airport, Virginia, from a duffel bag found in the cargo area of a flight from San Salvador, El Salvador, that had transited through Atlanta, Georgia. The cooler (approximately 10 x 8 x 6 inches) was empty and otherwise normal in appearance. The bags of powder were wrapped in layers of foil, tape, and mustard, and were concealed between the outer and inner walls of the cooler. Analysis of the powder (total net mass 411.7 grams) by GC/FID, GC/MS, and FTIR-ATR confirmed 85 percent cocaine hydrochloride. This is the second such recent submission to the Mid-Atlantic Laboratory.

Photo 7

Photo 8

* * * * *

- INTELLIGENCE ALERT -

MOROXYDINE HYDROCHLORIDE FOUND IN A HEROIN EXHIBIT FROM LAOS

The DEA Special Testing and Research Laboratory (Dulles, Virginia) recently received an off-white granular substance submitted to the laboratory for analysis from the DEA Country Office in Vientiane, Laos, suspected morphine. The substance was seized by Laotian authorities in an undisclosed area of Laos. Analysis of the substance (total net mass 6.8 grams) by GC/MS, CE, and proton-NMR, however, indicated not morphine but rather 23 percent heroin (calculated as the hydrochloride), along with 26 percent caffeine, 7 percent acetaminophen, 7 percent

O6-monoacetylmorphine (also calculated as the hydrochloride), and an unknown compound. The unknown was detected by CE and NMR, but not by GC/FID or GC/MS (either directly or following MSTFA derivatization). Further analysis of the chloroform insolubles (containing the unknown) by FTIR, LC/MS/MS, and advanced 1- and 2-dimensional NMR techniques indicated 20 percent moroxydine HCl (see Figure 1), an antiviral medicine. This substance does not appear to be used in the United States, but it is commercially available in many other areas of the world. It is unclear why it would be utilized as a heroin adulterant. This is the first submission of a sample containing this unusual adulterant to the Special Testing and Research Laboratory.

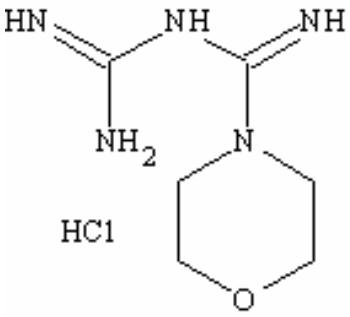


Figure 1 – Structure of Moroxydine Hydrochloride.

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

- SPECIAL INTELLIGENCE BRIEF -

"CHEESE"

Officer Jeremy Liebbe
Forensics and Evidence
Dallas ISD Police Department
1402 Seegar
Dallas, TX 75215

[Taken in Part from the Narcotics Information Bulletin of the Same Title; Unclassified; Reprinted with Permission.]

Between August 15, 2005, and March 1, 2006, the Dallas Independent School District Police Department handled 54 felony offenses and 24 found property cases involving a new drug mixture known on the street as "Cheese," a so-called "starter form" of heroin. "Cheese" is typically found folded inside a small paper bindle, and in the Dallas area is popular among Hispanic juveniles, both male and female, with known users as young as 13 years old. It is typically encountered as a light tan colored powder with granules varying from fine powder to 1.5 millimeters in size (see Photo 9). It is administered by insufflating (snorting) the powder into the nose through a tube, much in the same fashion as

Photo 9

is practiced with cocaine. Users have described the effects as causing euphoria, disorientation, lethargy, sleepiness, and hunger. As with any form of heroin, "Cheese" appears to be highly addictive, and withdrawal symptoms may onset as fast as within 12 hours of cessation of use.

Analysis of "Cheese" samples shows that it contains acetaminophen, diphenhydramine hydrochloride, and up to 8 percent heroin. Due to chemical interference caused by the acetaminophen and diphenhydramine hydrochloride, forensic analysis of "Cheese" can be challenging. It is believed that "Cheese" is manufactured by mixing a small quantity of heroin with a large quantity of crushed Tylenol-PM® caplets (that is, a commonly available formulation of acetaminophen and diphenhydramine hydrochloride).

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

- SPECIAL INTELLIGENCE AND SAFETY ALERT -

WIDESPREAD FENTANYL-RELATED OVERDOSES AND DEATHS IN THE NORTHEASTERN AND UPPER MID-EASTERN UNITED STATES !

Over the past year, law enforcement encounters with illicitly manufactured fentanyl have dramatically increased. Two clandestine fentanyl laboratories, a kilogram package of high purity fentanyl hydrochloride, a variety of fentanyl containing tablets (both Ecstasy-type mimics and Oxycontin® counterfeits), various mixtures of heroin/fentanyl powders, and at least one cocaine/fentanyl powder, have been seized from locations throughout the United States. Of particular concern, the distribution of heroin/fentanyl powders in and nearby the Chicago and Philadelphia metropolitan areas starting in February 2006 has (as of mid-May) resulted in several hundred overdoses and about fifty deaths, with additional overdoses and deaths being reported daily.

Fentanyl is a Schedule II Controlled Substance, classified as a narcotic analgesic (opiate). It is medically used both for acute and chronic pain control. It is also abused, usually as a substitute for heroin. Various pharmacological studies estimate fentanyl to be 30 to 50 times more potent than heroin (thus explaining the large numbers of overdoses and deaths associated with its abuse). The most common adverse effect is respiratory suppression - that is, the victim simply stops breathing.

All law enforcement personnel, including forensic and crime laboratory personnel, along with medical emergency response personnel, hospital emergency room personnel, toxicologists, pathologists, and similar, should be well aware of this still ongoing situation. Anyone who believes they have been exposed to fentanyl-containing materials, or who is experiencing fentanyl-overdose-like symptoms such as disorientation and respiratory distress, should seek immediate medical attention. In addition, any samples of known or suspected fentanyl-containing materials should be handled with appropriate care, and prominently labeled so that personnel along the chain of custody are aware of their unusually hazardous character.

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

Request for Information on the Illicit Manufacture of Fentanyl

- Potential Control of Fentanyl Precursors Being Considered -

The Drug Enforcement Administration (DEA) is concerned with the recent increase in the illicit manufacture and distribution of fentanyl, and in the large numbers of overdoses and deaths associated with its abuse. In response to this situation, the DEA's Drug and Chemical Evaluation Section (ODE) is considering controlling fentanyl's precursor chemicals. Therefore, ODE is interested in obtaining information on all seizures of illicitly manufactured fentanyl that have occurred within the past four years, as well as all future seizures through the end of CY-2007, in order to document the extent of this problem. This request is specifically looking for information concerning the synthetic route used by the clandestine laboratory to manufacture fentanyl. Furthermore, in order to document the impact on public health, ODE is requesting data on the number of overdoses, and overdose deaths attributed to illicitly manufactured fentanyl only (that is, not from legitimately manufactured fentanyl patches or from pharmaceutical grade fentanyl citrate, both of which are occasionally diverted and abused).

Primary Fentanyl Synthesis Routes: In 1965, Janssen Pharmaceutica patented the original synthesis for fentanyl, which used N-benzyl-4-piperidone as the starting material. The Janssen synthesis is challenging, and is beyond the rudimentary skills of most illicit chemists; however, it has been used in a number of settings by illicit chemists with advanced technical training. In the early 1980s, an alternate fentanyl synthesis route was published in the scientific literature, that used N-phenethyl-4-piperidone (NPP) as the initial starting material. The NPP synthesis route has been independently tested and verified (Noggle FT, Andurkar SV, Clark CR, DeRuiter J. GC-MS analysis of fentanyl synthesized from 1-phenethyl-4-piperidone. Microgram 1993;26(12):285).* This latter route has also been utilized in a number of clandestine laboratories.

Identification of Fentanyl Synthesis Route: The synthesis route used to manufacture illicit fentanyl can be determined by the identification of "marker" contaminants in the seized material. The presence of benzylfentanyl (a.k.a. N-(1-benzyl-4-piperidyl)-N-phenylpropanamide) suggests that the original Janssen synthesis route was used. Using GC/MS, benzylfentanyl can be presumptively identified by matching the four primary mass fragments (at *m/z* = 82, 91, 146, and 173) in its mass spectrum (see spectrum, Page 61). If present, the peak for benzylfentanyl will have a relative retention time (RRT) of about 0.963 to that of fentanyl (note that this will vary dependent on the type of capillary column and GC temperature program that are used).

In contrast, the presence of the immediate precursor 4-anilino-N-phenethyl-piperidine (ANPP) suggests that the NPP synthesis route was used. Using GC/MS, ANPP can be presumptively identified by matching the three primary mass fragments (at *m/z* = 146, 189, and 280) in its mass spectrum (see spectrum, Page 62). If present, the peak for ANPP will have a relative retention time (RRT) of about 0.891 to that of fentanyl (again, this will vary dependent on the type of capillary column and GC temperature program that are used).

Request for Information: Unfortunately, the information in the pertinent law enforcement databases on fentanyl seizures only rarely includes the determination of the synthetic route. Therefore, ODE is directly soliciting information from all federal, state, and local agencies and

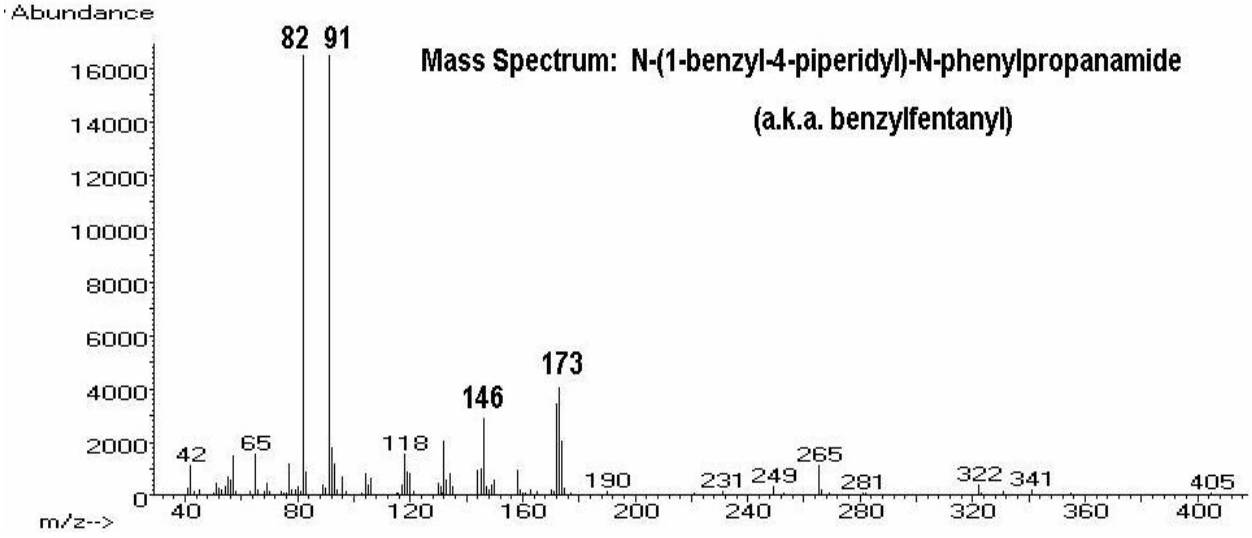
offices (law enforcement, forensic and crime laboratories, toxicology laboratories, coroner's offices, medical examiners, etc.) to document the presence or absence of the contaminants ANPP or benzylfentanyl in fentanyl seizures that have occurred within the past four years, as well as all future seizures through the end of CY 2007. ODE is specifically requesting the documentation of all occurrences of illicitly manufactured fentanyl (again, not from pharmaceutical sources), the synthesis route used (e.g., as determined from the presence of "marker" compounds), and the number of known overdoses and overdose deaths cause by illicitly manufactured fentanyl, if known.

Please note that ODE is not requesting re-analyses of closed case exhibits; rather, it is requested that the data in the pertinent case file(s) be reviewed with an eye towards identifying the referenced "marker" compounds. And that the analyses of all future submissions of fentanyl-containing exhibits be conducted with an eye towards specifically looking for the referenced "marker" compounds.

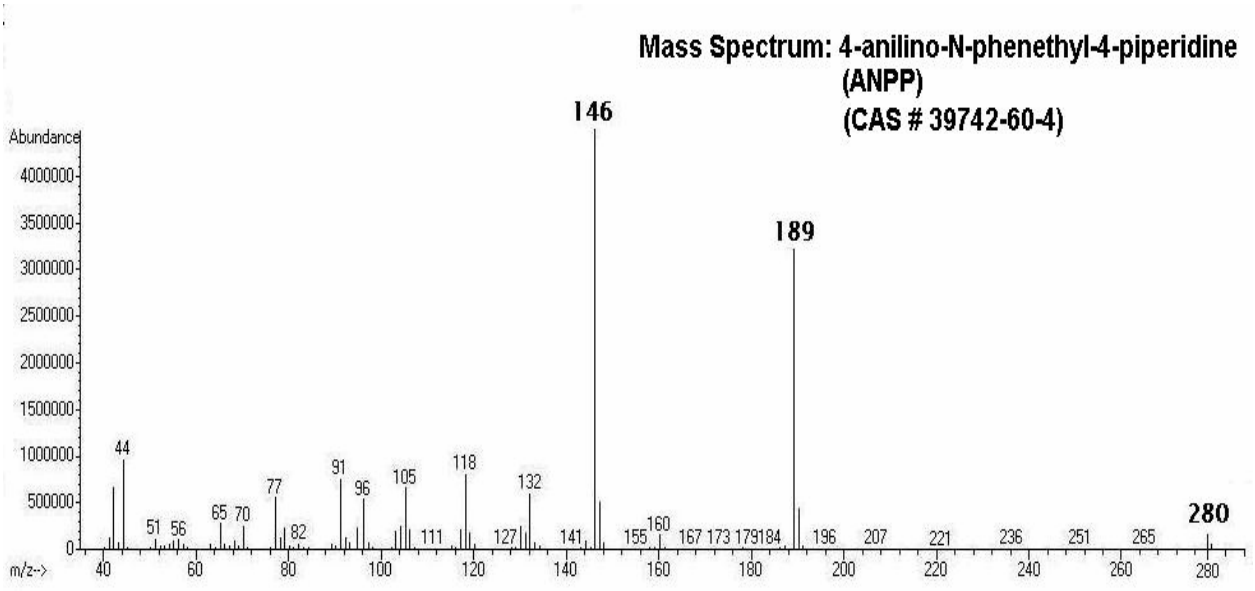
All information should be provided to: Mr. Wilson, Drug Science Specialist: Office: (202) 307-7183; Office Fax: (202) 353-1263; or Office Address: Attn: Mr. Wilson, Drug Enforcement Administration, Drug and Chemical Evaluation Section (ODE), Washington, DC 20537.

[* All issues of *Microgram* prior to January 2003 are Law Enforcement Restricted.]

- - - - - - - - - -



- - - - - - - - - -



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

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. Listed mailing address information exactly duplicates that provided by the abstracting service. Patents and Proceedings are reported only by their *Chemical Abstracts* citation number.]

1. Dahlen J, von Eckardstein S. **Development of a capillary zone electrophoresis method including a factorial design and simplex optimisation for analysis of amphetamine, amphetamine analogues, cocaine, and heroin.** Forensic Science International 2006;157(2-3):93. [Editor's Notes: Amphetamine and 13 analogues (not specified in the abstract) were analyzed, and the method was successfully applied to street samples. Contact: Swedish National Laboratory of Forensic Sciences - SKL, Linkoeping SE-581 94, Swed.]

2. Haroz R, Greenberg MI. **Emerging drugs of abuse.** Medical Clinics of North America 2005;89(6):1259. [Editor's Notes: A review of non-traditional drugs, including analogues, plants, and diverted pharmaceuticals. Contact: Department of Emergency Medicine, Medical College of Pennsylvania Hospital, Drexel University College of Medicine, Philadelphia, PA (zip code not provided).]

3. Shen J, Sun J, Li N, Liang L, Xu X, Liu H, Zhang C. **Investigation on THz fingerprint spectrum of illicit drugs.** (Proceedings) Chemical Abstracts 2006;144:186167e.

4. Tagliaro F, Bortolotti F. **Recent advances in the applications of CE to forensic sciences (2001-2004).** Electrophoresis 2006;27(1):231. [Editor's Notes: A minor overview and review. The first section includes illicit drugs. Contact: Department of Public Medicine and Health, Section of Forensic Medicine, University of Verona, Verona, Italy.]

5. Zhang S. **Kit for combined detection of drugs, its preparation method and blocking agents used for the same.** (Patent) Chemical Abstracts 2006;144:144626y.

Additional References of Possible Interest:

1. Below E, Rosenstock S, Lignitz E. **Hemp products in the German food market place. THC content and forensic meaning.** Blutalkohol 2005;42(6):442. [Editor's Notes: Debunks the common legal defense ploy (in Germany) that use of hemp-based consumer products caused a positive drug test for cannabis or hashish. This article is written in German. Contact: Insitut fuer Rechtsmedizin, Ernst-Moritz-Arndt Universitaet, Greifswald D-17487, Germany.]

2. Duyndam A. **XTC: The game and marbles.** Chemisch2Weekblad 2005;101(11):20. [Editor's Notes: A brief overview of illicit MDMA laboratories in the Netherlands (abstract indicates forensic chemistry). This article is written in Dutch. Contact: Neth. (no other contact information was provided).]

3. Lachenmeier DW, Emmert J, Kuballa T, Sartor G. **Thujone - Cause of absinthism?** Forensic Science International 2006;158(1):1. [Editor's Notes: Includes analytical studies of current and vintage absinthes, and also of absinthe prepared (by the authors) using historical recipes; the authors conclude that reported historical levels of thujone in absinthe cannot be confirmed, and also that the low levels of thujone found in absinthe is not responsible for "absinthism". Contact: Chemisches und Veterinaeruntersuchungsamt (CVUA) Karlsruhe, Weissenburger Str. 3, Karlsruhe D-76187, Germany.]

4. Sakayanagi M, Yamada Y, Sakabe C, Watanabe K, Harigaya Y. **Identification of inorganic anions by gas chromatography/mass spectrometry.** Forensic Science International 2006;157(2-3):134. [Editor's Notes: Uses derivatization with pentafluorobenzyl-p-toluene sulfonate and a crown ether as a phase transfer catalyst; 10 anions could be analyzed down to the 30 ng level. Contact: Kanagawa Prefectural Police Headquarters, Scientific Criminal Investigation Laboratory, 155-1 Yamashita-Cho, Naka-Ku, Yokohama 231-0023, Japan.]

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

SCIENTIFIC MEETINGS

1. Title: 32nd Annual NEAFS Meeting (First 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

---

2. Title: 16th Annual CLIC Technical Training Seminar (First Posting)
Sponsoring Organization: Clandestine Laboratory Investigating Chemists Association
Inclusive Dates: September 6 - 9, 2006
Location: Hong Omni Mont-Royal Hotel (Montreal, Quebec, Canada)
Contact Information: See O.C. Anderson (620 / 792-4353 or carl.anderson -at- kbi.state.ks.us)
Website: None Provided

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

Computer Corner #206

In-House Training - Part II

by Clayton D. Schilling
Group Supervisor
DEA Digital Evidence Laboratory

Part I of this series (Computer Corner #205) addressed the establishment of a comprehensive and effective in-house training program that is designed and administered at three distinct levels, those being: Basic, Advanced, and Skill Maintenance. This article will concentrate primarily on the details of Basic Training.

Basic Training

Entry level training should be designed to educate both novice and experienced practitioners in the fundamentals of conducting effective digital forensic examinations in accordance with your agency's specifications. The digital forensics field is extremely broad, and examination requirements can vary tremendously between agencies. It is therefore very important to establish a program that will train all new employees, regardless of their skill levels upon arrival. For a new practitioner, or for those that have only beginner-level knowledge and skills, the program should comprehensively cover the skills needed to establish a solid foundation. For already experienced practitioners, entry-level training programs are often rather boring - but it is still necessary for them to participate, so they understand the agency's specific requirements.

Providing an outline for each training topic or module is paramount to the basic program's success. This outline should include an overview or introduction, a list of objectives, the number of lecture, lab, and practical exercise hours, a list of handouts and/or references that will be used, and a summary of each of the discussion topics that will be addressed.

The overview or introduction paragraph is a summary of what the training will consist of, and should help the student understand what is being taught. The objectives list identifies measurable goals within the topic that lets the student know what specific knowledge, skills, and abilities they should understand or have mastered at each level. The individual objectives should be formally measurable by successful completion of either a specific task or a test. The number of lecture, lab, and practical exercise hours typically required to complete each area in the topic should be specified (lecture hours cover the amount of time spent teaching the information, lab hours cover the time spent performing the hands-on portions of the training, and the practical exercise hours cover the time spent on testing). This information can be summarized using a simple, two-rowed, four columned table containing column headings and total hours typically needed for each topic or subtopic (e.g., see below). The last column should contain a total of all the hours required for the topic.

Lecture	Lab	Practical Exercise	Total
2	2	2	6

The handouts and/or references list is self-explanatory. The discussion topics summary identifies the step-by-step method(s) by which the training will be conducted. Typically, this paragraph is a bulleted listing of subtopics that follow a logical progression in leading the

student from A to Z in the primary topic. It should be detailed enough that any instructor could use it to conduct the class, and also enable the student to answer or clarify any future questions.

A verbal overview is an excellent means to introduce a training program to the student(s). The purpose of the program can be explained (that is, that the training is designed to provide the student(s) with the skills needed to conduct digital forensics examinations in accordance with established organizational policies and procedures, which are consistent with industry standards). Additionally, an explanation of how the training will be conducted can be provided (for example, in a lecture format, supplemented with hands-on activities and practical exercises). The testing methods and standards should also be detailed, and should specify both the passing requirements (e.g., a minimum numeric score for written tests and a "pass/fail" score for practical exercises) and the failing consequences (e.g., re-training and re-testing) for all administered tests and practical exercises, to include the final written test and hands-on practical. “Final” consequences should also be specified; that is, if a passing grade is still not achieved after re-training, the student will be removed from the program, reassigned to another area, or released from employment.

In addition to the core skills, what other topics should your training program cover? As was discussed in Part I, it can (and should) include a wide variety of topics, such as organizational history and structure, ethics, standard operating procedures, legal issues, documentation, evidence handling, forensic processes, and so on.

The organizational history and structure training helps the students understand the importance of their role in your agency's mission. The policies and procedures training identify the guiding protocols by which your agency operates, and the methodologies each examiner should use in performing their job. The quality assurance training should address topics such as examiner proficiency testing, re-analysis and peer review, analytical inconsistencies, and so on. The ethics training should cover your agency's ethics policies as well as related legal issues such as *Giglio v. United States*, 405 U.S. 150 (1972).

Other important topics include legal issues, evidence handling, and examination documentation. Various legal precedents that are specifically pertinent to digital evidence, such as the Fourth Amendment (search and seizure issues), the Federal Rules of Evidence (“best evidence” issues), the Electronic Communications Privacy Act (ECPA), and Frye/Daubert issues (*Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923) and *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993)), to name a few, should be covered in great detail. It is critically important for examiners to understand how the law affects their work. Moot Court training, which will expose the examiner to the court system and expert witness testimony, should also be included. Examination documentation (that is, case file organization and management, comprehensive note taking, and report writing) is another organization-specific topic that should be covered.

As mentioned earlier, the topic of digital forensics is extremely broad and the examination requirements can vary tremendously between agencies. The following is a sample listing of the types of forensic-specific training that could be incorporated into a basic training program:

* Digital forensics using open source and industry standard forensic software
* Linux/Unix and Macintosh computer forensics (overview)
* Cell phone and PDA forensics

* Wiping hard drives and other media
* Forensic platform preparation and control checks
* Imaging and archiving of magnetic and optical media
* Operating Systems - Microsoft Windows, Linux, Unix, etc. (overview)
* Recovering - Swap files/Temporary files/Cache files/Deleted files
* Carving unallocated disk space and file slack
* Password cracking

Advanced/In-Service Training

Advanced Training is designed to provide examiners with opportunities to improve their digital forensic skills. In most cases, this training is taught by external providers, and usually focuses on just one or two specific topics, e.g., date/time stamp analysis, Internet history processing, or Steganography. However, it can also be taught by qualified in-house personnel if the agency is looking to share specific, higher-level knowledge that a certain examiner possesses, e.g., SQL database or Exchange Server processing.

Skill Maintenance Training

Skill Maintenance Training should be designed to provide examiners with opportunities to improve and/or maintain their digital forensic skills. This training is usually completed in-house and provides an excellent opportunity for an agency to share knowledge and skills between examiners.

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

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

* * * * *