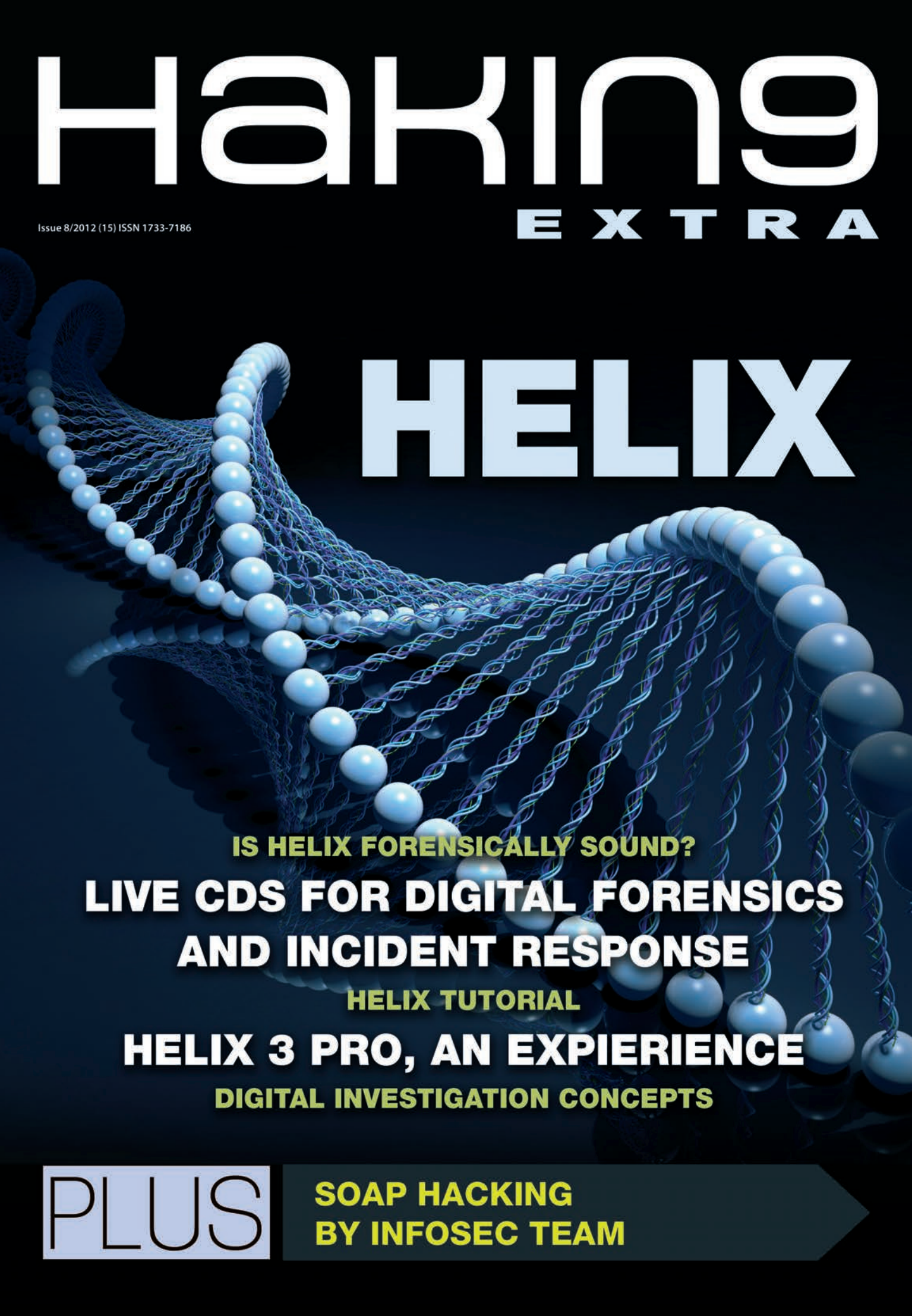
hakin9 EXTRA

Issue 8/2012 (15) ISSN 1733-7186



HELIX

IS HELIX FORENSICALLY SOUND?

LIVE CDS FOR DIGITAL FORENSICS AND INCIDENT RESPONSE

HELIX TUTORIAL

HELIX 3 PRO, AN EXPIERIENCE

DIGITAL INVESTIGATION CONCEPTS

PLUS

SOAP HACKING
BY INFOSEC TEAM

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth* **HDD diagnostics**, **firmware recovery**, **HDD duplication**, and **file recovery**. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch

Atola TECHNOLOGY

Visit atola.com for details

Learn ethical hacking › Become a Pentester™

- Get trained today through our exclusive 7-months hands-on course.
- Gain access to our complex LAB environment exploiting vulnerabilities across many platforms.
- Receive a trainer dedicated to you during the 7 months.
- 10 different hands-on engagements, 2 different certifications levels.

MONTH 1	› Vulnerability Assessment - level 1 › Vulnerability Assessment - level 2 › Vulnerability Assessment - level 3
MONTH 2	› Network Penetration Testing - level 1 › Network Penetration Testing - level 2
MONTH 3	› Network Penetration Testing - level 3
MONTH 4	› Web Application Penetration Testing - level 1 › Web Application Penetration Testing - level 2
MONTH 5	› Web Application Penetration Testing - level 3
MONTH 6	› Certification Exam 1 - Certified Cyber 51 Pentesting Professional - (CC51PP)
MONTH 7	› Certification Exam 2 - Certified Cyber 51 Pentesting Expert - (CC51PE)

~~Regular Price 1260 USD~~

Discounted Price

999 USD

Sign Up Now

www.cyber51.com

Cyber 51

Managing:
Michał Wiśniewski
m.wisniewski@software.com.pl

Senior Consultant/Publisher:
Paweł Marciniak

Editor in Chief:
Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Art Director:
Marcin Ziółkowski

DTP:
Marcin Ziółkowski
www.gdstudio.pl

Production Director:
Andrzej Kuca
andrzej.kuca@hakin9.org

Marketing Director:
Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Proofreadres:
Michael Munt, Rebecca Wynn,
Elliott Bujan, Bob Folden,
Steve Hodge, Jonathan Edwards,
Steven Atcheson, Robert Wood

Top Betatesters:
Nick Baronian, Rebecca Wynn,
Rodrigo Rubira Branco, Chris Brereton,
Gerardo Iglesias Galvan, Jeff rey Smith,
Robert Wood, Nana Onumah,
Rissone Ruggero, Inaki Rodriguez

Publisher: Hakin9 Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
www.hakin9.org/en

Dear hakin9 Extra followers,

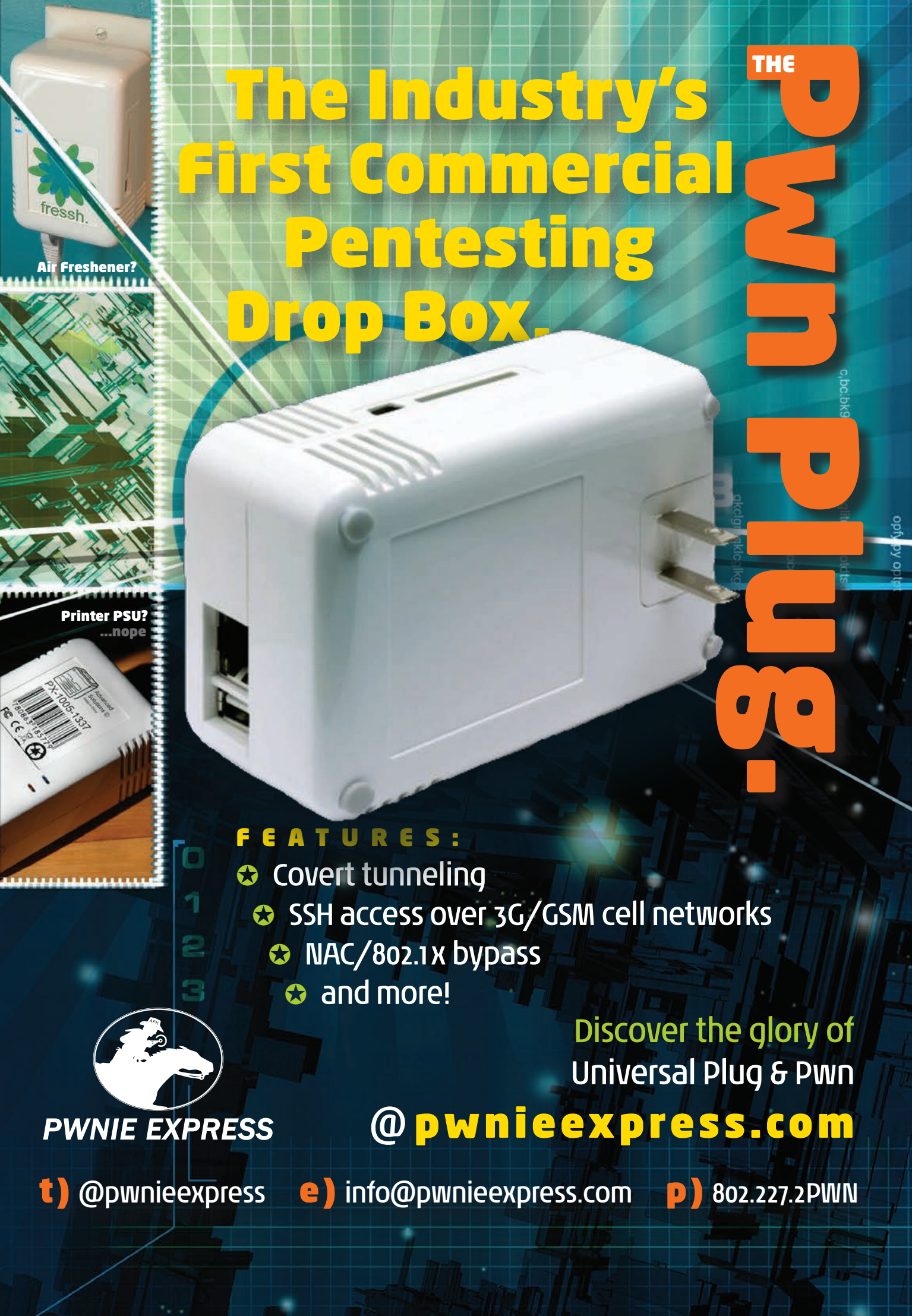
this month, in reply to your requests we decided to devote the current issue to Helix. What makes products from e-fense family so distinctive and desirable? Simply, they're easy in use and have plethora of functions: it not only can manage your network settings, but it is also an outstanding forensic tool. However, some of our authors not necessarily agree with that fact. Some authors will praise it, some others will roast it. Actually, multitude of opinions is something refreshing and thought-provoking. We'd love to present one point from different perspectives. This month: Amy Cox and Eyal Lemberger will check if Helix is really forensically sound. Keith Swanson is going to present Real-World Imaging Tips using Helix. Jon Evans will show his expertise on live cds for digital forensics and incident response. Elias Psyllos is going to share his Helix 3 experience. Mounir Kamal is going to discuss digital investigation concepts. Guys from INFOSEC provided me with an article by Ken Johnson on hacking SOAP (and not only SOAP).

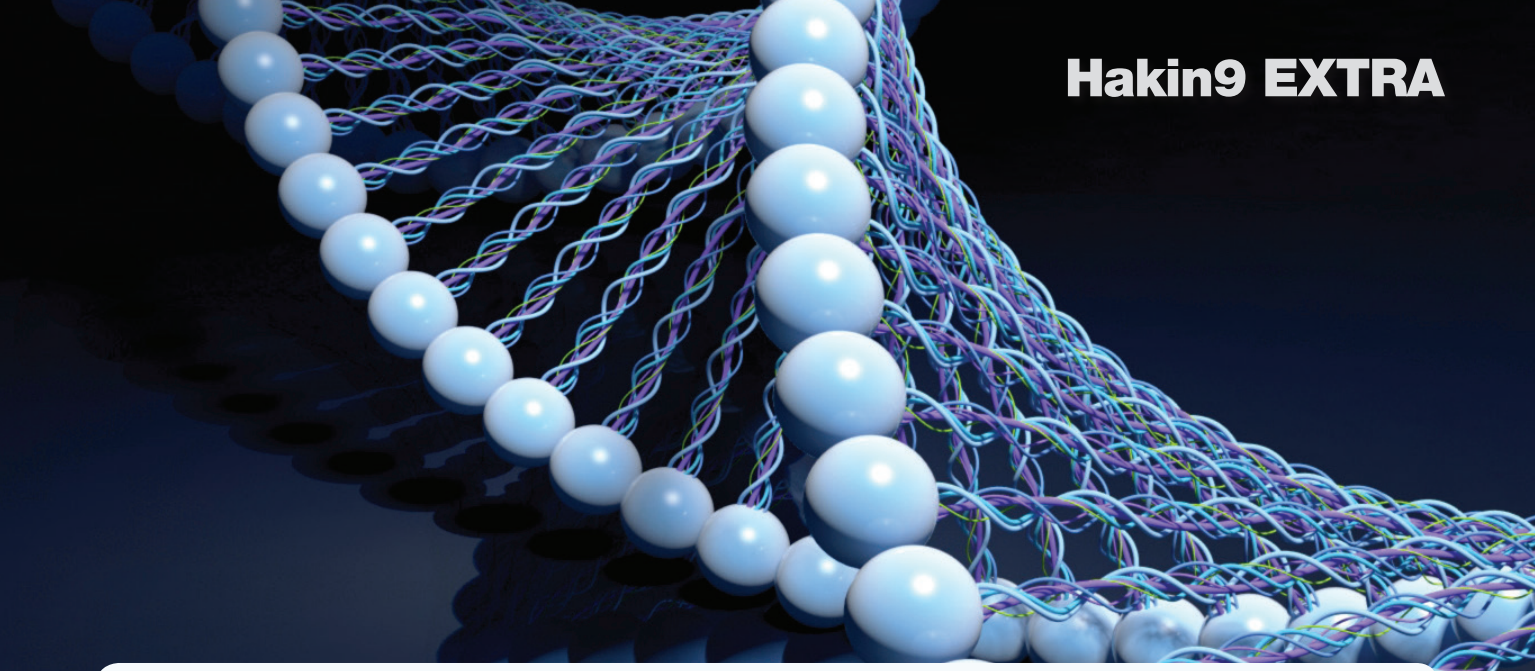
I hope that you will enjoy reading hakin9 Extra.

P.S. For those who would like to obtain CEH certificate and finish Cyber 51's course – we still offer promo options for hakin9 readers – just register via our affiliated link and enjoy -260$ bonus.

http://www.cyber51.com/affiliates/idevaffiliate.php?id=109&url=17

Michał Wiśniewski, hakin9 Extra
m.wisniewski@software.com.pl


THE
Pwn Plug.
The Industry's First Commercial Pentesting Drop Box.
Air Freshener?
fressh.
Printer PSU?
...nope
FEATURES:
Covert tunneling
SSH access over 3G/GSM cell networks
NAC/802.1x bypass
and more!
Discover the glory of
Universal Plug & Pwn
@ pwnieexpress.com
PWNIE EXPRESS
t) @pwnieexpress
e) info@pwnieexpress.com
p) 802.227.2PWN



8. Helix2009R1 is Forensically Sound...Surely?

By Amy Cox and Eyal Lemberger

The golden rule is that the initial media should not be altered. But ACPO do give some wriggle room with the secondary rule being that if the original media is altered in any way it must be done by someone who knows what they are doing and therefore understands the exact changes that happen. In other words and expert who can explain what has happened and why.

12. Real World Imaging Tips using Helix

By Keith Swanson

A RAW image in .dd format is the fastest and you may need to use that to speed things up. This format will also take up the most space on your target hard drive. So now we have to balance space issues with speed. We are all familiar with EnCase and the .E01 format. This will use less space but will also take more time.

18. Live Cds for Digital Forensics and Incident Response

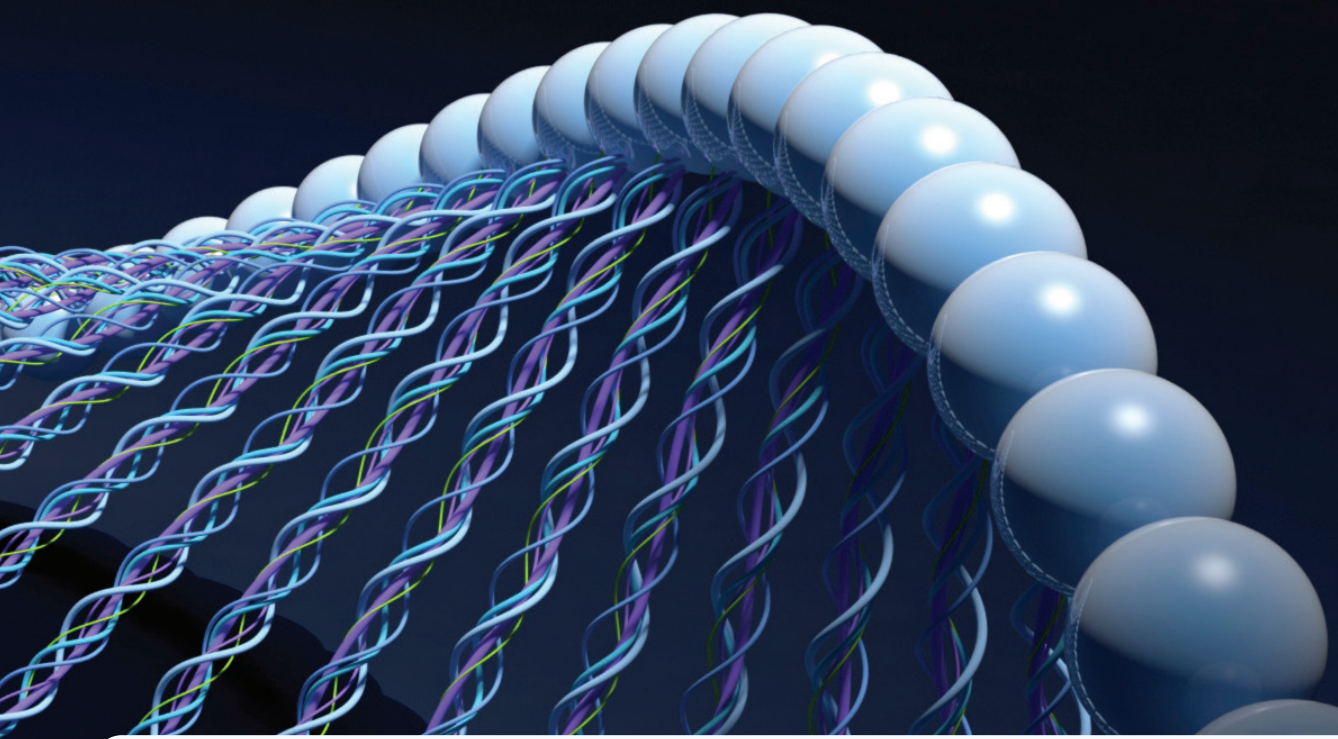
By Jon Evans

As with any tool know its limitations as well as appreciating its strengths. It is also important to test your tools, become thoroughly familiar with how they operate to ensure that during deployment they perform as anticipated. It is also important to identify any potential pitfalls. This is crucial when performing Live Forensics where you are obtaining evidential data from live running systems. Whilst performing post mortem forensics Helix is a good tool, however like other well known Linux forensic CDs flaws have been identified. For example earlier versions of Linux boot cd's which mounted file system even as read only would alter the journal count on ext3 filesystems, by decrementing it by one. Even though this effectively results in a 1 bit change, it is still a rather undesirable result potentially.

22. Helix 3: An Experience

By Elias Psyllos

One of the great features of Helix 3 Pro is the GUI face. Once Helix has fully booted you will see a clean and organized screen, as though you started the program from your desktop. For those that have not used this before, this is where it gets EASY. Go to the top left of the screen, select Applications, go down and select «Acquisitions and Analysis». Select Helix 3 Pro, and the Helix 3 Pro Acquisition tool will appear.On the left side of the Acquisition tool, you will see a section labeled «SYSTEMS» and it will list all the hardware attached currently to the computer (e.g. hard drives, CD/DVD ROMS, thumb drives, external drives, etc.) as well as the partitions associated with each. Select your source drive (the drive you want to create the forensic image of) from the left side of the screen and then click the «AQUIRE» button. On the right hand side of the screen will appear the «Acquire Device» dialog/selection box.



26. Digital Investigation Concepts

By Mounir Kamal

Electronic evidence is an information and data of investigative value that is stored on, processed or transmitted by an electronic device. Any data may be exist in three major status for example a computer running operating system data may be stored in hard disk or may be in memory for the purpose of processing or sending it to over network or internet and you can collect evidences in every status and if we back to the diagram in figure 1 based on many factor you can decide from which status you can collect you evidence.

32. SOAP hacking by INFOSEC team

By Ken Johnson from INFOSEC

Simple Object Access Protocol, or SOAP, leverages an XML structure for messages and typically communicates over HTTP protocol. Web service protocols are a lightweight communication mechanism useful for API driven connectivity and are often seen in use with mobile applications. To follow along with certain portions of the tutorial, you will need to install JRuby, Buby, Savon, and Nokogiri gems, and to download (or purchase) a copy of PortSwigger's Burp Suite. The idea here is that to extend some of Burp's capabilities to make attacking SOAP easier.

36. Atola Insight – More Than Just a Data Recovery Tool

By ATOLA Team

Atola Technology offers two hardware options for the DiskSense unit: USB and Ethernet. Both units have such features like serial port, real time current monitor, power control, write protection switch, buzzer, and LED indicators. Atola Insight Ethernet works with two ports to allow for direct disk-to-disk duplication, transfers data at speeds up to 110 MB/sec, and connects to an Ethernet port from any PC or laptop. Atola Insight USB ensures data transfer at speed up to 38 MB/sec and connects to the USB port with ease, also proper as mobile utilization. It's up to you to make a decision which one of Atola DiskSense units you will enjoy using.

HELIX2009R1 IS FORENSICALLY SOUND... SURELY?

AMY COX AND EYAL LEMBERGER

Helix3 is a bootable Live CD for use by forensic investigators for analysing systems running Windows or Linux. This article will discuss the issues that the forensic community have brought to light regarding the tool and test the forensic validity of the most recent open source version of the boot CD. It will end by discussing if any of the issues actually affect its usefulness as a tool.

Our intention is for you to learn the basics of how a Live CD, such as Helix3, works and how certain aspects of the tool may result in its forensic validity being open to question. Therefore although the article may relate to Helix3 it contains information that may help with other Live CDs. We will then offer ways to deal with the problems and try to spark debate as to whether the problems affect the validity of the evidence located.

A Little Background

Shortly after e-Fense and AccessData formed their partnership Helix left the open-source world. The last free version of the tool was released in June 2009 and it is still available today (*https://www.e-fense.com/store/index.php?_a=viewProd&productId=11*). Helix3 is not actually the third version of the tool its version number is 2.0 and it has been announced that the partnership has no intention of updating the free version. When the user downloads this free version the webpage informs you that although you get the tool you don't get access to their forums. Only if you purchase a licence for the 'Pro' version can you access the forums.

Neither of us has made the jump to the commercial 'Pro' version so this article will deal with Helix2009R1 only.

Helix started life being built on Knoppix but is now built on Ubuntu. It is a set of forensic tools for both Linux and Windows. The actual tool functionalities will not be covered here as they are most likely covered elsewhere in this dedicated issue of *Hakin9:Extra*.

Prior to the release of this version e-Fense suffered a major blow when the forensic community found that the previous versions of Helix were not forensically sound. This was because the tool had the ability to recover damaged ext3 partitions, automount partitions and alter journal files.

We feel we should point out that in fact several tools suffered such a blow, not just Helix3. Earlier versions of DEFT, CAIN and Backtrack all suffered criticism as well. In fact any Live CD based on the Debian distribution of Linux (at that time) would by default attempt to fix a corrupted ext3 file system. How each of the tools dealt with the problem ranged from denying the issue exists to coming back with a stronger tool.

In 2008 *Helix 2008R1* was released which may have been e-Fense's response to the issue. They stated at the time that:

Helix has been modified very carefully to NOT touch the host computer in any way and it is forensically sound. Helix will not auto mount swap space, or auto mount any attached devices. Helix also has a special live side for Incident Response and Forensics.

Woderful, they came back with a stronger Live CD that fulfils the forensic requirements... or did they?

Why Helix3 failed in the first place?

The Live CD was considered flawed for these four main reasons:

- A Live CD's original purpose was not to be a forensic tool.
- On a partition formatted with the ext3 filesystem the journal may be affected if the filesystem suffers from a corruption.
- The casper scripts were not configured to take into account forensic expectations.
- The flags used to automount specific filesystems were misconfigured.

The original Knoppix live CD is based on Debian GNU/Linux and it was originally designed for two reasons:

- To enable users to have a demo of GNU/Linux with full hardware detection capabilities, without actually having to install it on their systems.
- To enable an easy recovery of failed systems.

SeagateDataRecovery.com

Bad things can happen to your laptop. They don't have to happen to your data.

Seagate Data Recovery Services work on any disk drive.

Seagate takes the dread out of data mishaps. From accidental file deletions to physical hard disk damage–from any brand–we make it easy to get your files back. With our No Data–No Recovery Charge Guarantee, our skilled professional data recovery technicians use cutting-edge technology to retrieve your data. And for your peace of mind, we also recover data from server applications and virtual technologies. Learn more at www.seagatedatarecovery.com.

Seagate®

MONITOR STRONY

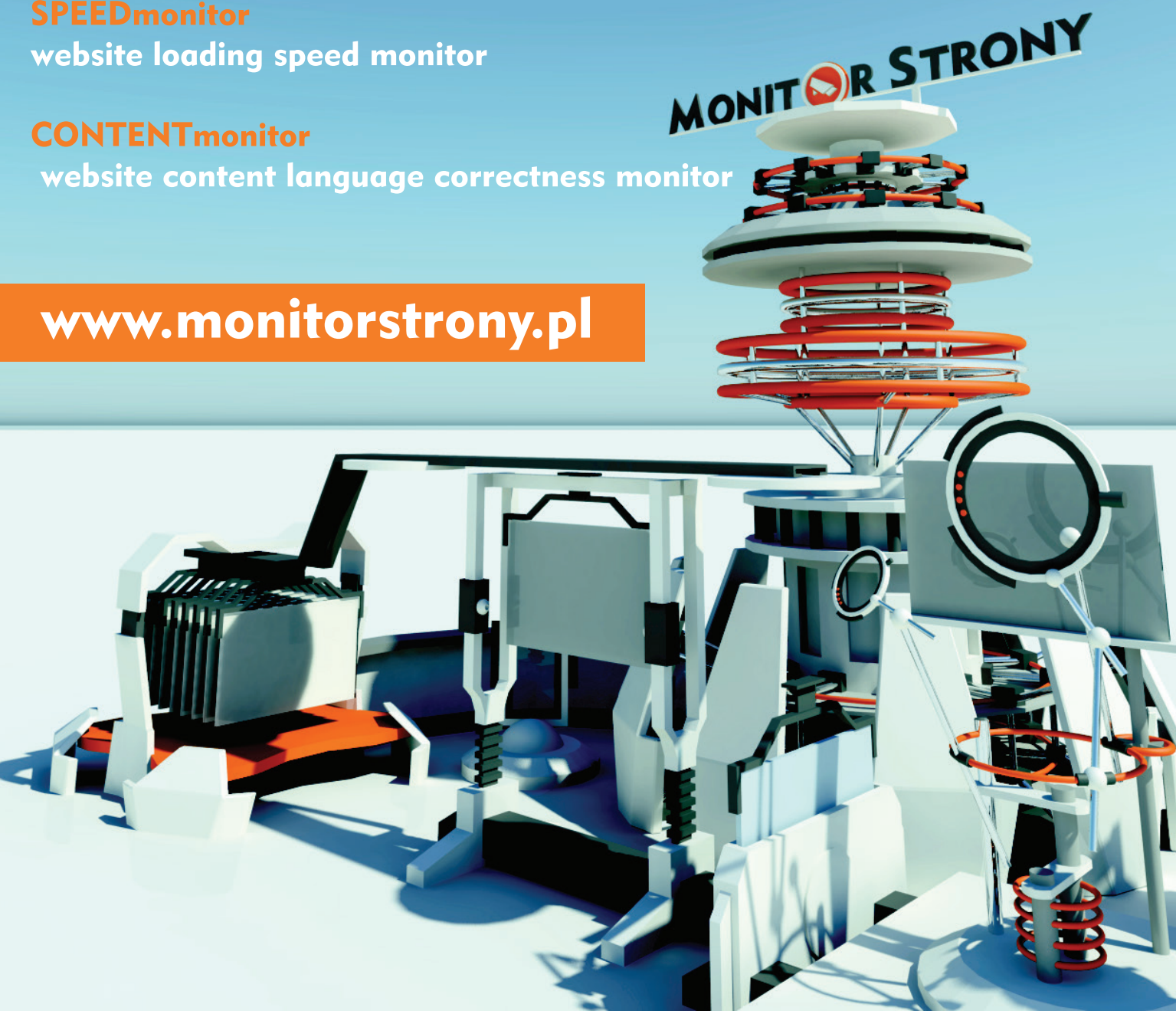
Innovative e-services for websites monitoring

SEOmonitor
SEO website monitor

SPEEDmonitor
website loading speed monitor

CONTENTmonitor
website content language correctness monitor

www.monitorstrony.pl



FUNDS FOR INNOVATIONS

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND

PROJECT CO-FINANCED BY THE EUROPEAN REGIONAL DEVELOPMENT FUND UNDER THE OPERATIONAL PROGRAMME INNOVATIVE ECONOMY

REAL WORLD IMAGING TIPS USING

KEITH SWANSON

We are charged with the response to almost anything in todays Law Enforcement age. We may get called to a terrorist attack, homicide, robbery, or just a theft of beer. Who knows? Can you be prepared for everything? Can you build a kit that will cover all of your needs?

This is a task for all Detectives or Electronic Incident Responders. The difference lies in what we are charged with dealing with. Blood spatter, fingerprints, and shell casings are much different that cell phones and iPads. Todays technology moves fast and what we find at a scene today could be a little baffling at first.

Our requirements for the proper handling of evidence and the analysis of that evidence are constantly changing with the advent of a new device or technology. Mohrs law is a constant and can be applied not only to chip processing power but to the growth of technology in general, in my humble opinion.

Fingerprinting has been around for centuries and despite some defense attorney dreams, it is an established science. In the fingerprinting world things don't change a whole lot. Anything new is thoroughly vetted by the established scientists and is put in use.

Not so easy on our electronic side, todays technology changes on the fly. What is state of the art now, is oh so old news 5 minutes later. By the time a new process is vetted and approved by the superior minds in Computer Forensics, that device is old news and we don't see it again. Please see HD DVD, Beta, Mini disk, zip disks etc. Not that we don't see these things, just that we don't see these things as much once they are surpassed by something bigger, better, and faster.

Specialized tools and software designed for one device, or one operating system cannot be viable. Today we are asked to build our kits with no budget, no support, and without really knowing what we are facing. We have to maximize what each of our tools can do. Multi use tools are the key. Carrying around one CD that can be used in many different ways beats a case of them for each system we find.

Let's talk budget. While Helix is no longer free, it isn't exactly a trillion dollars either. When a product can be used in many different ways, that's called getting your bang for the buck. The bean counters in accounting like that, and it also frees up money for other toys, like a new core i7 wonder computer. But I digress.

This article is not going to be a complete go by the steps course in imaging 101, no way. Take the time to get the training you need, or go work with someone who will mentor you through the process. While writing this my unit had several discussions about how detailed I should make this, the consensus is that imaging with Helix is something that should get hands on time.

That being said we will take a look at how to make the process easier and faster, and some of the advantages to Helix when imaging and some of the issues.

Sure there are times you have no choice, Cell Phones being a prime example.

When responding to an event, we have to look at the hardware presented to us for analysis.

Can we access that drives? How much damage will be done to get at the drives? Can we effectively attach our write blocking systems?

Who is the crowd has taken apart an apple Product Lately? iMac? MacBook Pro?

If you're like me, those little screws will make you nuts. Let's face life… There is always at least one screw left after you are done reassembling the damn thing and you have no idea where it goes. Now what?

RAID systems? Great, now I get to rebuild a RAID and I have several people breathing down my neck looking for evidence to arrest the suspect.

It's easy for some to say "Tell them to back off, it's a scientific process" blah blah blah… Hey. I have been the arresting Detective; I have been on the scene of the homicide that depends on the info on that hard drive. I have found that kid that was missing after meeting someone on Facebook. Time is of the essence, and they are going to press you, as they should, to get it done and get it right.

This is where a multi tool like Helix comes in.

We are going to look at some of the imaging tools in Helix from a real world scenario.

I'm not a college professor, or graduate student writing a research paper, I'm a Detective, just like all of us in Law

inj3ct0r

if you'll hacked us
we'll pay you 10K $
http://1337day.com/

Exploit database separated by exploit type
(local, remote, DoS, Poc, etc.)

CODENAME:
SAMURAI SKILLS COURSE

<< Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time , any where)
- Our Course is Totally Different from Other Courses (new Techniques)

LIVE CDS FOR DIGITAL FORENSICS AND INCIDENT RESPONSE

JON EVANS

This article looks at Live CDs as a tool for forensics and incident response. By Live CDs we are talking about the ability to deploy live forensic tools to a running system as well as the capability to boot a suspect system using the same CD. The focus here is on the concept of utilising a trusted toolkit to assist with the acquisition of data for digital forensics and incident response. The article will demonstrate some of the traditional uses for capturing both volatile data and forensic acquisition of disks. This is not meant as a comprehensive guide but as an introduction.

Introduction

This article focuses on the infamous Helix Incident Response CD. The Helix IR CD has two facets, the first being used as a Live CD meaning you can deploy trusted forensic tools on a live running system the primary purpose of which is to capture volatile data. This article will only provide a brief introduction to the subject area of live forensics, for more I would recommend reading Harlan Carvey's Windows Forensic Analysis DVD Toolkit, or Eoghan Casey's Malware Forensics: Investigating and Analyzing Malicious Code. The second is as a bootable CD whereby you can boot a suspect system into a trusted Linux environment to perform acquisition, or even triage. Although Helix IR is dated it is useful in this context as a basis for the reader to gain a basic understanding of how Live CDs can be deployed and in what circumstances. As a result the reader should gain some understanding how a CD is put together, how it is deployed and in what circumstances it can be harnessed. Bootable Forensic CDs are an ideal introduction to the power of Linux for data acquisition, and often useful when dealing with complex system setups. As an example bootable Linux CDs can be useful for acquisition of Server RAIDs, or systems which present challenges when attempting to disassemble in order to remove a hard drive for acquisition e.g. laptops, multi media centres and servers etc.

These are just some of the strengths of utilising Linux for forensics;

- Free! Open Source. This also means it can be compiled to run on a number of varying architectures, e.g. ARM, PowerPC, MIPS, OpenRISC, See Wikipedia for a more comprehensive list. This provides the possibilities of developing a forensic toolset for some diverse systems including embedded systems;
- Linux has a wealth of file system support (37 following a basic count in the Linux 3.4.4 kernel). In addition to various partition types and drivers for dealing with Memory Technology Devices;
- A wealth of freely available tools for digital forensics, network forensics and malware analysis;
- Diverse selection of scripting languages, text manipulating and parsing tools, ideal for log file analysis.

Background to Helix Live CD for forensics and IR

Helix IR was developed by Drew Fahey. Drew was an agent with the U.S. Air Force Office of Special Investigations he later founded E-Fense where he continued developing Helix. Drew is now Vice President of Products at Blackbag Technologies. The initial public beta release of Helix was 23rd November 2003, version 1.3.2 and was based on Knoppix. The last publicly available release was Helix 2009R1on 5th February 2009. Shortly after which it became a paid for product with some additional enhancements commonly known as Helix3 Pro. Helix2009R1 can still be obtained via registration at https://www.e-fense.com/store/index.php. Drew was also responsible for developing Live Response a USB key with a trusted toolkit for capturing physical memory and volatile data, this and Helix3 Pro are now part of the AccessData portfolio of products. You can still obtain earlier versions without registration, the last version being Helix 2008 R1. The MD5 hash value for which is 93a285bfa8ab93d664d508e5b12446d3.

Get the best real-world Android training anywhere!

Attend AnDevCon IV

The Android Developer Conference

December 4-7, 2012

San Francisco Bay Area

Choose from more than 65 classes and workshops!

- Learn from the top Android experts, including speakers straight from Google!
- Attend sessions that cover app development, deployment, management, design and more
- Network and connect with hundreds of experienced developers and engineers like yourself

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

Register Early and SAVE BIG!

www.AnDevCon.com

Follow us: twitter.com/AnDevCon

"AnDevCon is a fantastic conference! There is no better place to experience the latest and greatest technologies and techniques in the field of Android development. If you attend one conference this year, this one should be it!"

—Jay Dellinger, Senior Software Engineer, Manheim

A BZ Media Event

HELIX 3 PRO: AN EXPERIENCE

ELIAS PSYLLOS

The Request: I received a call for a collection of computers on-site and needed to respond quickly. I grabbed my forensic go-kit that I had built, containing a wide variety of products; such as write blockers, wiped hard drives, cables, and imaging software, etc.

The Scene: I arrived on-site to find 6 computers and have limited time to complete my imaging/verification process. I immediately layout a plan of how to attack the scenario. All chain of custody forms are filled out, labels created, pictures taken and I have secured a location to set my equipment up to begin imaging. I remove the first 3 machines hard drives and use three Tableau TD1's to begin imaging them. The remaining three machines; I use my two forensic laptops and two write blockers hooked up to the hard drives that I have removed, using Helix 3 Pro as my imaging software. (Note: If the machine is already running, depending on the operating software, Helix 3 Pro will boot up by itself (auto run) or you can initiate the .exe file) Rather than waiting for a TD1 or laptop to free up, I decide to use a bootable Helix 3 Pro disc in the last machine of the remaining three.

The machine is currently off, I use a paper clip to pop the CD/DVD-ROM drive on the machine and place the Helix 3 pro disc in the machine. The key to the next step is not allowing the system to actually boot up, any changes to the system could affect the evidence and chain of custody. I want to start the system and immediately select the Boot Sequence, the option for this will show at the bottom or top of the screen when you first power on the system. Beware you only have a few seconds to select the Boot sequence option before the machine starts the operating system. As a precautionary measure keep your hand on the power cable to the machine, if you can't select the Boot sequence option in time, pull the power cord. This will prevent the machine from booting the operating system. Once you are in the Boot sequence, select the CD/DVD-ROM drive and Helix will open up. Select the "BOOT HELIX 3 PRO" option, you do not want to select the "INSTALL" option on a machine that is considered evidence. The system should now boot up Helix 3 Pro, and you will see Helix's scripts begin to run. If the screen goes black during Helix's boot up, do not panic, Helix is in the final stages of booting.

One of the great features of Helix 3 Pro is the GUI face. Once Helix has fully booted you will see a clean and organized screen, as though you started the program from your desktop. For those that have not used this before, this is where it gets EASY. Go to the top left of the screen, select Applications, go down and select "Acquisitions and Analysis". Select Helix 3 Pro, and the Helix 3 Pro Acquisition tool will appear.

On the left side of the Acquisition tool, you will see a section labeled "SYSTEMS" and it will list all the hardware attached currently to the computer (e.g. hard drives, CD/DVD ROMS, thumb drives, external drives, etc.) as well as the partitions associated with each. Select your source drive (the drive you want to create the forensic image of) from the left side of the screen and then click the "AQUIRE" button. On the right hand side of the screen will appear the "Acquire Device" dialog/selection box.

The "Acquire Device" selection will be where you will select the criteria (output type, segmentation, hash protocol, etc.) and fill in the details (examiner name, case number, description, notes, etc.) for your image. Make sure if you have not already, to connect your destination drive (the drive you want to save your image to). At the top middle of Helix 3 Pros main screen, you will see your device appear. Select your device, and an option window will appear. Select the "MOUNT" option.

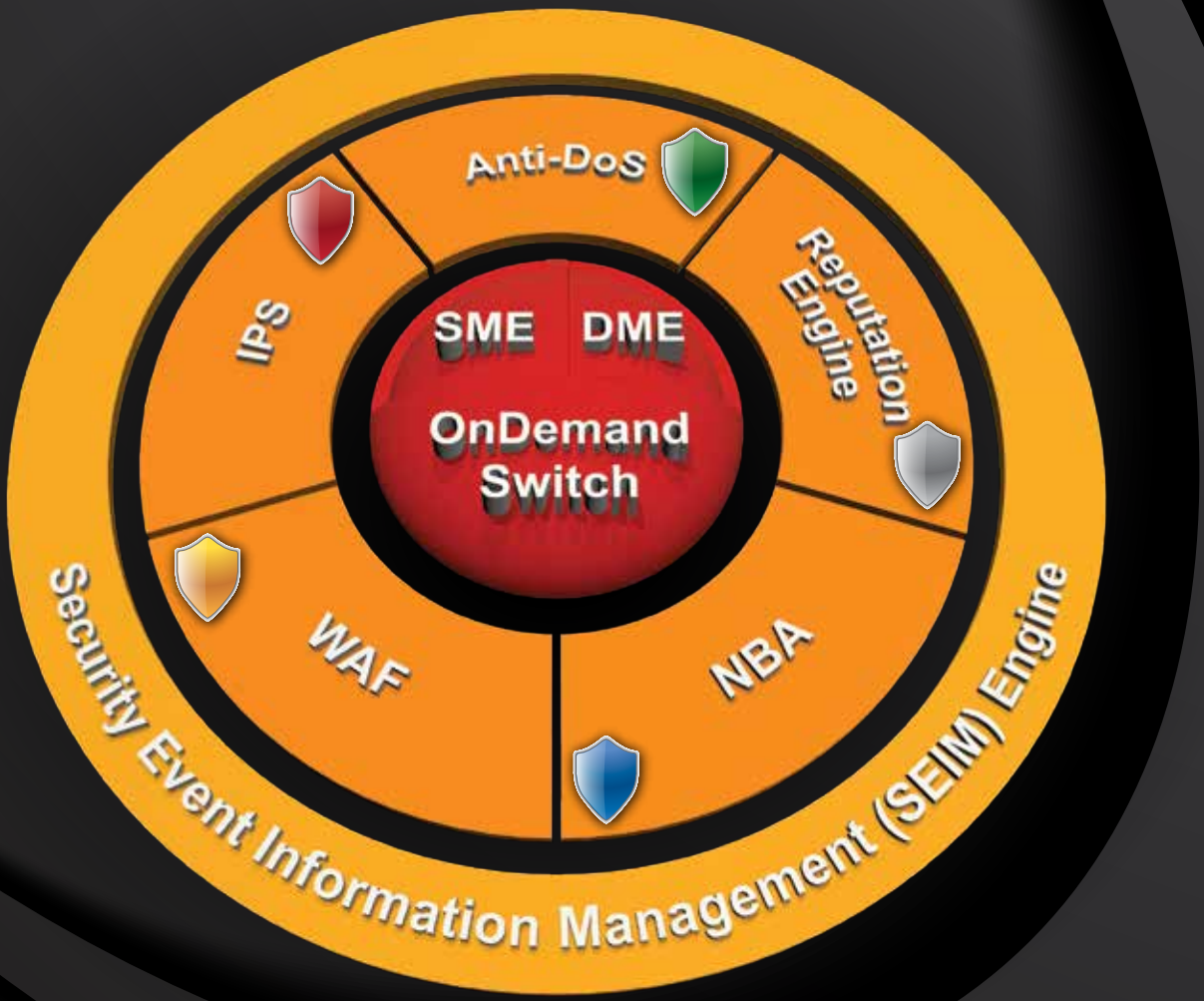
Back in the acquisition screen select the drive you want to save your image to (which should be the drive you just mounted). Select the "Start" button and the imaging process will begin. When the image is done, make note that there is an MD5 hash value.

Disconnecting and Shutting Down Helix: Unmount the destination drive (that we had previously mounted) by going back up to the top middle and select the destination drive and then select "Unmount" in the window that appears. On the top right corner of the screen, next to Helix User, select the power button. Select the "Shut Down" option, and once helix runs through the shut down sequence you will be prompted to select "Enter". Eject the disc first, then select Enter and the system will then shutdown.

Now I have imaged and verified all 6 machines at almost the same time without delay waiting for a laptop or a TD1 to free up. For every Helix license you have, you can image a machine, so no matter how large or small the collection, you can purchase the necessary licenses. I have also minimized my time needed on-site by conducting the imaging and verifications of the machines almost simultaneously.

ELIAS PSYLLOS
Computer Forensic Analyst, Sr.

radware



Protecting Networks from a New Age of Hacktivism

Radware Attack Mitigation System:

- Real-time, Multi-vector Attack Detection
- Hardware Accelerated DDoS Mitigation
- Integrated Event Correlation & Reporting
- 24x7 Emergency Response Team Support

For more information, visit: www.radware.com

DIGITAL INVESTIGATION CONCEPTS

MOUNIR KAMAL

In this article, a process model for Digital Forensics Investigation is developed and suggested as an alternative way to start digital investigations. The proposed model introduces the notion of a digital crime scene with its own digital evidence to be applied to law enforcement.

This article is structured as follows: Firstly, Providing background about Cyber-Crime definitions and categories. Secondly, presenting a new model for the relation between digital forensics attributes and showing its significance to start solid investigation. Finally, provides scenarios in order to demonstrate the effectiveness of the model when applied on the investigations in reality. i.e. memory investigation, live investigation, hacking investigation, virtualization, cloud computing investigation process and network investigation.

Cyber-crime Background

The intense increase in cyber-crime is due to the innovative ideas that criminals have with regard to new types of cyber-crime and new ways to commit these crimes.

Criminals exploit human and technologies vulnerability to commit crimes in a way that makes it very hard to trace them back. The ever-changing nature of technology from virtualization to encryption …etc. contributes to the problems encountered by experts when collecting and preparing digital evidence for courtroom presentation.

Cyber Crime Definition

There are many definitions for cyber-crimes but the most common one is: *Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern computing devices and telecommunication networks.*

Cyber Crime Categories

- **The computer as a target:** The attacker seeks to deny the legitimate users or owners of the system access to their data or computers. A Denial-of-Service (a.k.a., DOS or DDOS) attack or a virus that renders the computer inoperable would be examples of this category.
- **The computer as a tool of the crime:** The computer is used to gain some other criminal objective. For example, a thief may use a computer to steal personal information.
- **The computer as incidental to a crime:** The computer is not the primary instrument of the crime; it simply facilitates it. Money laundering and the trading of child pornography would be examples of this category.
- **Crimes associated with the prevalence of computers:** This includes crimes against the computer industry, such as intellectual property theft and software piracy.

What is Digital Forensics?

Digital forensics is defined as "The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, and use of validated tools, repeatability, reporting, and proper expert witness presentation"

When considering this definition of digital forensics, investigators must apply the following two tests for evidences in both digital and physical forensics to survive in a court of law:

- **Authenticity:** Where the evidence originated?
- **Reliability:** How the evidence was handled?

Rules of Digital Forensics

An expert forensic investigator will do two things: make sure to preserve as much of this data in its original form, and to try to re-construct the events that occurred during a criminal act to know what happened.

Because digital evidence is very volatile and can easily be contaminated or compromised when handled incorrectly, fo-

SOAP HACKING BY INFOSEC TEAM

KEN JOHNSON

I often receive-testing related questions from AppSec folks new to web services about the techniques used to discover and attack them. Often, web services are seen as difficult to enumerate, interpret, and exploit. Additionally, web services are thought of as an arena with only a small arsenal of tools available.

We'd like to bridge that gap a bit by introducing some techniques and offering code, which can be found here. Let's jump right into it.

In this article we will specifically cover SOAP. Other popular standards exist, such as JSON and REST, but for the purpose of this tutorial we limit our exploration to SOAP.

Simple Object Access Protocol, or SOAP, leverages an XML structure for messages and typically communicates over HTTP protocol. Web service protocols are a lightweight communication mechanism useful for API driven connectivity and are often seen in use with mobile applications.

To follow along with certain portions of the tutorial, you will need to install JRuby, Buby, Savon, and Nokogiri gems, and to download (or purchase) a copy of PortSwigger's Burp Suite. The idea here is that to extend some of Burp's capabilities to make attacking SOAP easier.

As mentioned previously, SOAP communicates messages in an XML structure. This XML structure can be defined using a (web services description language (WSDL) document. Enumerating this information provides a wealth of data used in formulating attacks and forming requests.

SOAP actions and parameters are very useful bits of information, and they can be extracted from the WSDL. An action might be something like getEmailAddress, which is passed using a parameter and value such as "profileid=1000". Forming that request and sending it may allow you to discover other user's e-mail addresses simply by changing the profiled value.

Now we could perform the enumeration of a WSDL manually by reviewing the response and making sense of the (sometimes) large amounts of data within the XML tags, but why not create re-usable code to do this quickly and seamlessly?

Install JRuby: `$ sudo apt-get install jruby`

Install the Savon and Buby gems:

```
$ sudo jruby -S gem install buby $ sudo jruby -S gem install savon
```

Now it's time to write some code. The Savon gem is a Ruby/JRuby library that allows us to build a SOAP client and interact with web service. Create a file named attack_soap.rb and enter the following code:

Line-by-Line Review:

Lines 1-2:
This is a directive to our script that basically says, "Use these libraries."

Line 5:
Next we need to enter code that allows us to hook into Burp Suite and provide a medium through which the tool and our code can meet. We defined a class *CustomMenuItem.* (Line 33 will provide more details about when this feature comes into play.)

Lines 8-9:
We create a method called *enum_wsdl*. This method is called on line 27 and passed a URL (*rhost* object). On line 9 you see that we instantiate the Savon client and pass it the value associated with *rhost*.

Lines 11- 12:
Both of these are optional values. Line 10 specifies the use of basic authorization which a username and password of "guest". Line 11 sends traffic to our Burp proxy instance.

Lines 13- 18:
Line 13 ensures that *client.wsdl* and *client.wsdl.soap_actions* exist prior to being called. Line 14 gives us a pretty purple –{*}- icon and states, "List of available action(s):". Lines 15-17 iterate through the array of *soap_actions*, "puts" each action to the console, and on line 17 we end the loop statement.

Lines 19-21:
Rescue clause in case things go belly-up and if so, we will gracefully handle the error on line 19. On line 20 we will print a red –{-}- marker along with the error (*$!*) to the screen. Line 21 ends the *enum_wsdl* method.

Lines 23 -24:
Line 23 is where we define a method called *menu_item_clicked*. This is extremely important because Burp wants to invoke this method, naming convention specific. In class, we passed it on line 33 when the menu item is clicked (makes sense).

All this means is the class *CustomMenuItem* must have a method named *menu_item_clicked*. Take care in noticing we pass it **params*. This means multiple objects can be passed to this method.

On line 24 we break up the couple of objects that are passed into two separate objects called *menu_item_caption* and *message_info*.

Lines 26 – 31:
The object *message_info* is an array of messages. Each messages has certain values it is associated with. When we iterate through this array, line 26, we can access these values.

ATOLA INSIGHT. MORE THAN JUST A DATA RECOVERY TOOL.

Whether it is a drive that has bad sectors, locked or damaged, with missing files or degraded heads, Atola Insight can easily work with it.

Atola Technology introduces **Atola Insight** – the only data recovery device that allows providing the whole cycle solutions for data recovery process.

Get started in three steps. Atola Insight is the only data recovery tool with the easiest way of connectivity. All you have to do is to attach the unit to the PC with a single cable, connect to a drive, and switch on the tool. Moreover, the unit itself favors to save your working space by placing the hard drive right on top of the device. Atola's thought-out solution gets rid of the unnecessary mess that other tools tend to make. Easy to start. Simple to work.

Hardware options to choose. Atola Technology offers two hardware options for the DiskSense unit: USB and Ethernet. Both units have such features like serial port, real time current monitor, power control, write protection switch, buzzer, and LED indicators. Atola Insight Ethernet works with two ports to allow for direct disk-to-disk duplication, transfers data at speeds up to **110 MB/sec,** and connects to an Ethernet port from any PC or laptop. Atola Insight USB ensures data transfer at speed up to 38 MB/sec and connects to the USB port with ease, also proper as mobile utilization. It's up to you to make a decision which one of Atola DiskSense units you will enjoy using.

Designed to meet any needs. Atola Insight was the first tool with the following automatic advanced features for data recovery market: in-depth diagnostic of all hard drive components, firmware recovery, password removal, case management systems, and many other things. One of the main highlights in the tool that is not being fulfilled to the full extent in its power in existing data recovery products – is diagnosis. Atola Insight presents the only one of its kind: self-acting diagnostics that is based on in-depth testing of circuit boards, heads, media surfaces, firmware, and file systems consequentially. With one click, you can run a big process of diagnostics. Just a couple of minutes and you get a full diagnostic report that comes with recommendations summary of all the components of a hard drive. It's worth trying to appreciate its true value.

It's your own recovery lab. Atola Insight is the most amazing tool for data recovery specifically designed to solve major problems and even more. Innovative technology allows providing complete data recovery process automatically. Case management system helps to save each of your action in one place. You can report to the device history at any time you want. Well- thought-out solutions enable canceling use of any other data recovery tools.

Atola Technology applies the latest market-oriented technologies, strives to improve the efficiency and functionality of products to the highest level, and makes all efforts to define the future for the data recovery market.

Figure 1. *Atola Insight*

Develop for the Next Big Platform!

Attend the Windows Phone Developer Conference and get the best developer training!

WP DevCon

The Windows Phone Developer Conference

October 22-24, 2012
Hyatt Regency
Burlingame, CA
www.WPDevCon.net

Learn from the top experts at the Windows Phone Developer Conference, including 12 Microsoft MVPs!


Darrin Bishop


Michael Cummings


Nick Landry


Jose Luis Latorre


Chris Love


Colin Melia


Walt Ritscher


Lino Tadros


Kelly White


Shawn Wildermuth


Chris Williams


Chris Woodruff

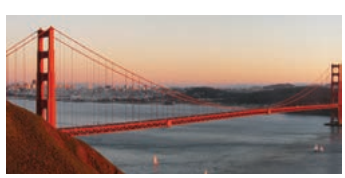
50+ Classes and Workshops

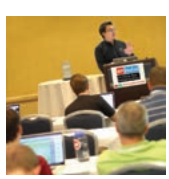
focus on a variety of important topics:

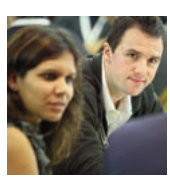
- Design implementation
- Location intelligence services
- Rich data visualization and implementation
- Cloud-based mobile solutions
- Development leveraging HTML5
- User experience
- Application design
- HTTP protocol
- Building reusable components
- Microsoft push notification service
- Creating custom animation
- and many more!

Visit WPDevCon.net for a full list of speakers, bios, classes, workshops, and special events!

Learn, network, and seize the opportunities that Windows Phone represents.







Register Early for the biggest discounts! at www.WPDevCon.net

Produced by BZ Media SD Times @WPDevCon

THEY SELDOM SMILE AT THE NSA. CAN YOU MAKE THEM GRIN?

Learn how to synthesize and apply these vital skills and leadership ability to succeed in the fast moving field of Network Security.

Bachelor of Science
Network Engineering
Network Security
Technology Forensics

Master of Science
Information Assurance

Program accreditations, affiliations and certifications:

ACCREDITED
The Higher Learning Commission
MEMBER
The Higher Learning Commission · North Central Association
For more information: www.ncahlc.org

⚠ CLUSTERGEEK WITH CAUTION

LEARN, EXPERIENCE AND INNOVATE WITH THE FOLLOWING DEGREE STUDENTS: Advancing Computer Science, Artificial Life Programming, Digital Media, Digital Video, Enterprise Software Development, Game Art and Animation, Game Design, Game Programming, Human-Computer Interaction, Open Source Technologies, Robotics and Embedded Systems, Serious Game and Simulation, Strategic Technology Development, Technology Product Design, Technology Studies, Virtual Modeling and Design, Web and Social Media Technologies

Prepare to Defend!
www.uat.edu
877.828.4335

PLEASE SEE WWW.UAT.EDU/FASTFACTS FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS