CHAMPLAIN COLLEGE
1878

The Patrick Leahy Center for Digital Investigation

LCDI

Fall 2012

Volume 2, Issue 1

The Senator Patrick Leahy Center for Digital Investigation (LCDI) is a world-class laboratory designed to international standards, focused on establishing and assisting with public and private sector initiatives surrounding cybercrime, digital forensics, and information assurance. As a leader in Digital Forensics in higher education, Champlain College offers students an opportunity to learn more while participating in "real lab work" at both the undergraduate and graduate levels.

10 ***Passwords*** Not to Use

1. **123456, 123, 123123, 0123, 2468, 987654, etc.**
2. **123abc, abc123, 246abc, etc**
3. **First name**
4. **Favorite band**
5. **Favorite song**
6. **First letter of given name then surname**
7. **QWERTY, asdf, and other keyboard rolls**
8. **Favorite cartoon or movie character**
9. **Favorite sport, sports star, or sports team**
10. **Country of origin**

Good Tool to Use

Log2timeline

Timeline analysis is an important part of the digital forensic process.

Log2timeline is a great tool for timeline analysis, written in Perl for Linux by Kristinn Guðjónsson.

Log2timeline parses log files and artifacts so that they are presented in an easy to read timeline, called a super timeline, which supports examiners in their forensic analysis. It extracts timestamps from the files and outputs them into a body file. It is a command line based tool and can be found in the SIFT Workstation by SANS

Year-to-Date Metrics

- Completed 25 data recovery jobs for Champlain College faculty, staff, and students.
- Examined over 15 terabytes of data.
- Conducted over 2890 hours of Research & Development
- Completed 9 Forensic Investigation cases for clients outside of Champlain College.
- Staffed by 8 Student Interns, 17 Student Employees, 8 Student Volunteers, and 2 Alumni.

Upcoming Events:

- **Champlain College's Fall Open House**
  October 27, 2012 8:00am – 2:30pm EST
  Champlain College Campus
- **VT Tech Jam**
  October 28th and 29th 10:00am – 5:00pm EST
  Borders Building - 29 Church St, Burlington, VT
- **DFIR Online**
  November 15, 2012 8:00pm EST
  Andrew Case – Android Forensics
- **Paraben's Forensics Innovation Conference (PFIC)**
  November 4th@ 2:00pmUCT, 6th @9:00amUCT
  Michael Wilkinson – Identifying the Artifacts and behavior of an Unknown Application
  November 6th@10:00amUCT
  Michael Wilkinson – Automating Forensics Pre-Processing Steps using TAPEWORM

Are you Attending?

Data Recovery

Have you ever deleted a file by mistake? Has your hard drive ever stopped working? Did the computer repair shop tell you they couldn't help get your data back? If you answered YES to any of the above, then you need to bring your digital device to the professionals. Let our world-class team discuss your options with clear and measurable results. The LCDI does a number of data recovery jobs for the Champlain College IS Department's Help Desk. Our expertise in data recovery assists the Help Desk expedite jobs submitted by faculty, staff, and students. The LCDI offers this service to all departments, faculty, staff, and students at Champlain College. If you have lost data, come see us and let our team work on your problem.

LCDI
175 Lakeside Avenue, 300A
Burlington, VT 05401
802-865-5744 office

Editor: Joseph Williams | Designer: Bonnie Bohan

TAPEWORM

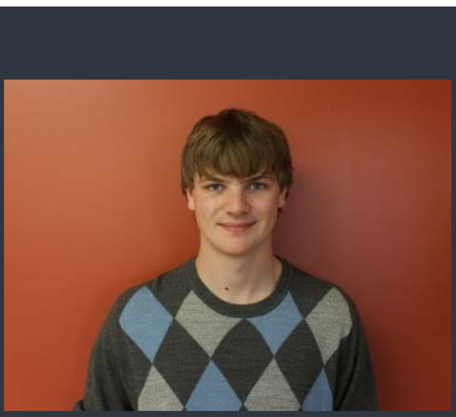
The LCDI partnered with The Analytic Sciences Corporation, TASC, over the summer of 2012 to collaborate and produce an open source forensic tool to be used in the digital forensic market. The LCDI had four Champlain College students, two digital forensic interns and two programming interns, who worked through the summer and beginning of fall to produce TAPEWORM.

TAPEWORM, short for TASC Pre-processing Exploitation & Workflow Management system, is an open source forensic software suite. The idea behind TAPEWORM was to create a software program that combines multiple open source forensic tools in a system that is user friendly, free, and easy to set up and run. The interns at the LCDI devoted the entire summer and first month of the school year to making this idea a reality. The product itself is a 64 bit Xubuntu-based Virtual Machine. The two programmers created a custom GUI, written in the Python programming language, which ties together the different open source tools and allows the user to run them all at once. The product was officially released in October at the Open Source Digital Forensics Conference, which took place in Chantilly, Virginia.

The forensics community has been continuously releasing open source tools that are used to collect evidence. However, these tools are generally run at the console and require considerable amounts of work to get setup. Additionally, several of these tools work in combination, with no one tool containing all the parts necessary to complete the evidence gathering task. TAPEWORM combines these tools and automates their operation in a graphical user environment that is user friendly. This not only allows the tool to be used by someone with less experience, but it also reduces the chance of error. In addition, the automation frees up the time of the investigator, as he or she can set it to run on its own. These tools exist in a Linux Virtual Machine, and everything is ready to run. There is no install or setup: just a logon and go.

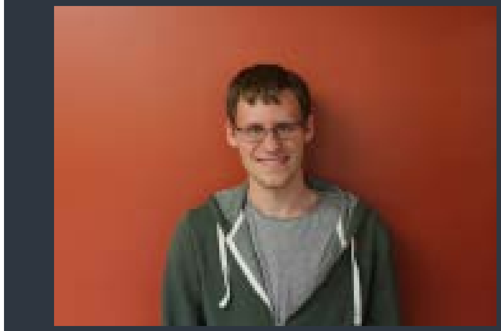
Open Source Digital Forensics Conference 2012 Chantilly, VA: TAPEWORM

At this year's conference, TAPEWORM was officially released. During the release, we had 28 participants in the room with their laptops out and VMware running. They were able to play with TAPEWORM and learn about all of its features. TAPEWORM is an exceptional tool to use because it automates the process of running seven different tools, including 6 possible antivirus suites, in one easy to use interface. By selecting an input of your E01, DD, L01 case file, or a folder of extracted evidence, you can run all of these tools across them with an automated interface. TAPEWORM will run all of the commands with the specific switches, heavily reducing the chance of human error. It also takes all of the output it generates, and then formats it in an easy to read and organized output that can be used to identify data of interest on a drive with unknown data. The efficiency of TAPEWORM lies in the number of different tools it utilizes, each specializing in different aspects of analysis. Some of these include generating timelines, exit reports, and data carving. Overall, the members of the conference were enthused at the functionality of the TAPEWORM suite.



Chapin Bryce

"The TAPEWORM project has been a great experience working with project development. I was brought on to the project because of my experience in digital forensics and Linux. Being my first development project, I really enjoyed learning about all the different aspects involved in creating a suite such as TAPEWORM. My main focus in this project was on ensuring all the dependencies for the tools in TAPEWORM were installed and performing correctly along with the testing and validation of the suite. After working on this project for a little more than 4 months, I am considering shifting my focus in digital forensics from a focus in networking security to scripting and programming. This project has been great opportunity to expand my horizon in the field of forensics and technology."



Connor Hicks

"Working on project TAPEWORM at the LCDI has been   a privilege and a serious learning experience for me. It is the first time that I have programmed for a real project, not just an in school assignment. I've learned more about working as a software engineer on this project than I ever could in the classroom. The LCDI provided a great environment for me as a student going into his first internship. I felt more comfortable when my co-workers are fellow students, and working in a business linked to the college. At the same time TAPEWORM is a major project, and I feel like I've gotten a good grasp of what the environment is like for software engineers in the work place. I am proud to see what TAPEWORM has become over the course of the last 4 months."

Michael Abbott

"The LCDI is a unique blend of an academic environment applying itself to relevant projects in the digital forensics community. My work on TAPEWORM and as an Intern at the LCDI has provided me with real world programming experience. This has directly led to job opportunities upon graduation."

Neil Torpey (not pictured)

"The TAPEWORM project has provided me with the opportunity to work with brilliant people both at Champlain College and in the Computer Forensics field. The open source digital forensics field is a very cool niche that has solidified my passion for the work I am doing, and I hope I will continue to contribute to the open source community into the future. I am looking forward to meeting the people I collaborated with this summer at the Open Source Digital Forensics Conference in October, and hopefully will get some of my textbooks autographed!"

Editor: Joseph Williams **|** *Designer: Bonnie Bohan*

Q&A

With LCDI's Digital Forensics Intern, **Ethan Fleisher**

Ethan Fleisher is a senior from Carlisle, Pennsylvania majoring in Computer and Digital Forensics at Champlain College. Ethan works as a Digital Forensics Intern at the LCDI, where he is involved in Forensics Investigations, R&D Projects, and System Administrator among other jobs.

Q: About Ethan:
I'm a computer and digital forensics student aspiring for a job in the field. I work at the Senator Patrick Leahy Center for Digital Investigation, I'm a CDF Tutor, and I also work part-time at Best Buy selling computers and tablets. In the very little off-time I have, I kick back and relax with my girlfriend, watch TV, sports and movies, and go out with my friends.

Q: Projects you have worked on at LCDI and/or stuff you do at LCDI
I've worked on a lot of projects at the LCDI, with my personal projects ranging from Windows 8 Forensics R&D, casework for the State of Vermont, project management, to network and system administration. I've assisted many of the interns and students with their project, which really reinforces the "student team model."

Q: What's your favorite part about working at the Leahy Center?
The atmosphere of the LCDI is probably the best part. Everyone that works there wants to be there. How often can someone go into a job and be surrounded by people that love what they do, and appreciate all the work that each individual puts into the job? It's amazing.

Q: Here's the big debate: Mac or Windows?
I'm not an Apple fan-boy, but they do make good products. That being said, I'd rather use a Windows machine as well as Android for my phone.

Q: What's your favorite thing about your major?
CDF is such a unique field. I love talking to people about what we do, explaining how important the field is to not only criminal justice, but cyber security as well. CDF really hits on all the important aspects, and it's amazing how many subdivisions there can be. One examiner can be an expert in mobile phones, another malware, and another person the windows operating system. It's all about what you make it to be.

Q: Is the forensic technology as advanced as television shows such as "CSI" portray?
If I could input a video of a class the LCDI taught on July 9th, 2012 here, I would. The CSI portrayal of our job is amazingly absurd in some regards, for example – two people on one keyboard to stop an attacker. We do work some magic; it just takes a bit longer than 45 minutes plus commercials.

Q: What will you miss most about CC?
The most missed thing will just be the college experience itself. I've met a lot of people and made a lot of connections that I plan on keeping, but it's going to be a lot different in seven months when I have that piece of paper.

Current Projects at LCDI

Benchmark

Lead: Freddy Morey
Team Members: Olivia Hatalsky

There are millions of benchmarks and comparisons of different computers and parts in the field of high performance computers, but none of these benchmarks focus on digital. We are working on changing that. The LCDI's main question approaching this project was: is it worth the extra money to purchase a highly customized and powerful forensic specific computer or is it more cost efficient to purchase a mid- to high-end computer at a retail store? We are formulating a process that will test a computer for forensic performance while being able to actively compare it to other systems. We are focusing on software that we use at the LCDI for this test, such as EnCase, FTK, WinHex and others. The end target for this project is to be able to send the procedure out as a proposal to computer manufacturing companies, hoping they run the testing and report back to us, or they send out computers and we do the testing in house.

OS Forensics

Lead: Colby Lahaie
Team Members: Kyle Porto & David Leberfinger

OSForensics is an easy to use open source acquisition and analysis tool. As of now, EnCase and FTK are the "iPhones" in the computer and digital forensics field. They have been proven to be forensically sound and accurate, but these tools can come with a greater cost that many law enforcement agencies cannot afford. The LCDI is looking into OSForensics because we believe it can be a cost effective alternative to high priced forensic tools. It will give local law enforcement a tool they can use in the place of higher priced software, and allow them to have more resources in their arsenal. This project will analyze the affectability and accuracy of this software compared to the leading acquisition/analysis tools.

Volatility

Lead: Catherine Stamm
Team Members: David Leberfinger, Daniel Doonan & Connor Hicks

Volatility is a Python-based framework that utilizes multiple tools in order to analyze RAM images. This tool aids investigators in finding out more about volatile memory on a system by extracting running processes, computer information, memory maps, open network connections, and more. These areas of memory are very important to a case, as they present an abundance of significant data that can be used as evidence. Therefore, an understanding of the functions and capabilities of Volatility is, to us, a necessity for computer investigators. The LCDI will review these functions and produce an easy to follow how to guide for law enforcement agencies.

Open Source – *Joshua Lowery*

Free and open source software is an idea that is slowly catching on in the booming technological culture that we have created. But what does it mean to be open source, and why should it be used over something that is paid for and guaranteed to work?

Open source is free by two definitions: free like free food and free like free speech. Compared to food, it is available for anyone to use and use as much as they want on as many machines as needed. When looked at like speech, it allows people to view their code and does not allow anyone to use it for their own personal gain. It is based off of the idea that knowledge is for everyone and no one has the right to prevent people from learning.

In the forensics realm, open source software is viewed both positively and negatively depending on individual feelings. Some feel that open source software is not as good because it does not have a support line available 24/7; you would need to go online to forums if you have a problem or figure it out yourself. At the same time, it is seen by some to be reliable and customizable to any situation. Many of the programs run through the command line, so the user has to know what is going on and has a better understanding of what the program does rather than just pressing buttons.

The final decision is up to the individual using the software. There are pros and cons to using any type of software, and everyone has their own opinion on what they want out of their programs. Take the test and use open source alongside proprietary software to see if there is a difference. Find out what software best suites the requirements of the job and is the most cost effective regarding: licensing, support, training, and time spent using the tools.

Editor: Joseph Williams | *Designer: Bonnie Bohan*

Private Browsing

Lead: Trevin Mowery

Team Members: Kyle Tellers, David Thomas & Christina Esprit

Most people use the internet every day, but not everyone uses it for good. Some individuals use it for nefarious activities and because of this; they want/need a way to effectively hide what they did on the internet or a way to stop all information from being written to the hard drive, in order to leave no evidence. **Google Chrome**, **Mozilla Firefox**, and **Internet Explorer** all have something built in called “Private Browsing” that can do just that. At least, that is what people believe it can do. The LCDI will conduct research to see if these “Private Browsers” can actually hide all traces of internet history and to see what is left behind or what can be recovered, if anything at all.

Other Projects

Lead: Various

Team Members: Various

For a full list of all the LCDI’s projects, to view past projects or to stay up to date on our current projects, please visit our website.

5 Tips for Incoming CDF First Year Students

1. **Join the Digital Forensics Association – it’s a good way to make connections within your major.**
2. **Do your own research – you will not learn everything in class.**
3. **Use Career Service – they can help you build resumes and look for internships/jobs.**
4. **Use Open Lab Hour – this is a good way to get experience with forensics software.**
5. **Follow forensics newsletters – it will pay off to know what’s going on in your field of study.**

Student Team Model

The Senator Patrick Leahy Center for Digital Investigation is leading the way in forensic education and training in the Vermont area.

Champlain College students who work at The LCDI get hands on experience working and researching cases from start to completion. Our students work in a “Student Team Model,” where a Champlain College fourth or third year student leads a team of students working on cases at The LCDI.

The LCDI is open to all Champlain College students who need a place get help on forensic projects.

LCDI - Senator Patrick Leahy Center for Digital Investigation

Champlain College
Phone: (802) 865-5744
Email: LCDI@champlain.edu
Address: 175 Lakeside Avenue,
300A Burlington, VT 05401

Our faculty, staff and students are here to help!

Visit our Website

http://lcdi.champlain.edu

Find us on Facebook

http://www.facebook.com/LeahyCDI

follow us on twitter

https://twitter.com/@champforensic

Contact LCDI

http://computerforensics.champlain.edu/contact-info-computer-forensics

Editor: Joseph Williams | Designer: Bonnie Bohan