IUP Proudly Presents:

Cybersecurity Skills Enhancement Camp

JUNE 4 TO JUNE 8, 2018

ATTENTION: MIDDLE AND HIGH SCHOOL STUDENTS!

- Expand your cybersecurity and technical knowledge
- Learn essential communication and critical thinking skills
- Do any of these topics interest you? Apply today by visiting www.iup.edu/caecexpansion and then clicking on summer camp in the left menu!

Location

IUP Main Campus

Questions?

cae-c-expansion@iup.edu

Program Directors

Waleed Farag, PhD
Computer Science

Ben Rafoth, PhD
English

Crystal Machado, PhD
Education

Mac Fiddner, PhD
Policital Science

Advantages

- Offered at no cost!
- Electronic device for each participant!
- Instruction and mentorship from IUP faculty and other experts!
- Skills and knowledge for a growing career field!
- Hands-on learning!

Apply NOW space is limited!

IUP

www.iup.edu/caecexpansion

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

PROUDLY AFFILIATED WITH

NSA

IUP

ADVANTAGES FOR STUDENTS

- Offered at no cost!
- A Raspberry Pi 3B+ Kit for each participant!
- FREE lunch!
- Instruction and mentorship from IUP faculty and other experts!
- Expand your knowledge of Cybersecurity and gain technical knowledge!

HOW TO APPLY

Applications are accepted online only. To apply or view other important information, please visit:

www.iup.edu/caecexpansion

CAMP DATES

June 4th to June 8th, 2018

PROGRAM DIRECTORS

Dr. Waleed Farag
Professor of Computer Science

Dr. Ben Rafoth
Professor of English

Dr. Crystal Machado
Professor of Education

Dr. Mac Fiddner
Professor of Political Science

IUP 2018 Cyber Security Skill Enhancement Camp

PRESENTED BY IUP AND NSA

IUP CAE-C EXPANSION PROJECT

SUMMER 2018 PROGRAM

This program supports projects that address cybersecurity education in the following areas:

- Integration of hands-on learning experiences into cybersecurity curriculum.
- Innovative approaches to cybersecurity education.
- Initiatives focused on increasing the availability of qualified cybersecurity educators.
- Initiatives focused on expanding the student pool.
- Collaboration and engagement in cybersecurity education programs.
- Study correlation between commercial certification courses, government-sponsored cybersecurity designation programs, and the CAE-C KUs/focus areas.

THE FUNDED GRANT

Under the leadership of Waleed Farag, grant PI; Ben Rafoth, co-PI; Crystal Machado, co-PI; and Mac Fiddner, co-PI, IUP, along with a selected group of national universities, has been awarded funding to start an innovative project to enhance cybersecurity education in Western Pennsylvania.

This project has the following objectives:

- To develop a cohesive set of services to innovatively address known challenges facing cybersecurity education. Proposing effective solutions to such challenges will facilitate the development, retention, and expansion of a skillful cybersecurity workforce to meet the increasing demand.
- To incorporate an interdisciplinary approach in designing and implementing the services mentioned above that will appeal to diverse cyber talent—including women and minorities—and serve a geographical area that is predominantly rural.

CAMP PROGRAM SUMMARY

Among the activities in the IUP Expansion of CAE-C project is to host a Cybersecurity Skill Enhancement summer camp for middle and high school students. This camp is a free (no cost to participants), five-weekday day camp offered in summer 2018. Instruction will be delivered by a team of professors, security experts, and middle/high school instructors. This camp will address both technical and non-technical skills needed to pursue a successful career in the Cybersecurity field.

- Upon completion of the camp, participants will have a strong understanding of Cybersecurity in addition to mastering necessary technical and non-technical skills.
- 30 projected participants from surrounding middle and high schools.
- An engaging content delivery approach that focuses on hands-on learning, carefully designed group activities, and empowering participants to be able to explore the field of Cybersecurity further.

2018 IUP Cybersecurity Skills Enhancement Camp

DAY 1 - JUNE 4, 2018

9:00 a.m. to 9:15 a.m.	Camp Introduction with Dr. Farag in Stright 112A
9:15 a.m. to 10:45 a.m.	Cybersecurity 101: Threats, Vulnerabilities, and Hands Excercises with Dr. Porche in Stright 112A
10:45 a.m. to 11:00 a.m.	BREAK
11:00 a.m. to 12:30 p.m.	Cybersecurity Basics (Programming and Raspberry PI) with Dr. Farag in Stright 112A
12:30 p.m. to 1:30 p.m.	LUNCH
1:30 p.m. to 3:00 p.m.	Speak Up: Or Forever Hold Your Peace with Dr. Rafoth in Stright 340

2018 IUP Cybersecurity Skills Enhancement Camp DAY 2 - JUNE 5, 2018

9:00 a.m. to 10:30 a.m.	Interactive Problem Solving with Dr. Fiddner and his students in Stright 112A or Outside (Weather Permitting)
10:30 a.m. to 10:45 a.m.	BREAK
10:45 a.m. to 12:15 a.m.	More Than Words: Writing for Cybersecurity with Dr. Rafoth and Ms. Sarraf in Stright 112A
12:15 a.m. to 1:30 p.m.	LUNCH
1:30 p.m. to 3:00 p.m.	Cyber Clash With China I with Dr. Fiddner in Stright 112A

2018 IUP Cybersecurity Skills Enhancement Camp

DAY 3 - JUNE 6, 2018

9:00 a.m. to 10:30 a.m.	Computational Thinking Lab! with Mrs. Gentile in Stright 112A
10:30 a.m. to 10:45 a.m.	BREAK
10:45 a.m. to 12:15 a.m.	Giving a Great Not Boring Presentation: Three Steps to Killing It with Dr. Rafoth and Ms. Sarraf in Stright 340
12:15 a.m. to 1:30 p.m.	LUNCH
1:30 p.m. to 3:00 p.m.	Raspberry PI and Cybersecurity Applications with Dr. Farag in Stright 112A

2018 IUP Cybersecurity Skills Enhancement Camp

DAY 4 - JUNE 7, 2018

9:00 a.m. to 10:30 a.m.	New Wireless Security and Emergency Communications Opportunities for You with Mr. Jesson in Stright 112A
10:30 a.m. to 10:45 a.m.	BREAK
10:45 a.m. to 12:15 a.m.	Work Session for Cyber Clash with China with Dr. Fiddner in Stright 112A and 112B
12:15 a.m. to 1:30 p.m.	LUNCH
1:30 p.m. to 3:00 p.m.	Intorduction to Digtial Forensics Investigation I with Dr. Farag in Stright 107A

2018 IUP Cybersecurity Skills Enhancement Camp DAY 5 - JUNE 8, 2018

9:00 a.m. to 10:30 a.m.	Digital Forensics Investigation II (Analyzing a Ubuntu System) with Dr. Farag in Stright 107A
10:30 a.m. to 10:45 a.m.	BREAK
10:45 a.m. to 12:15 a.m.	Cyber Clash with China Presentations I with Dr. Fiddner and Dr. Rafoth in Stright 340
12:15 a.m. to 1:15 p.m.	LUNCH
1:15 p.m. to 2:45 p.m.	Cyber Clash with China Presentations II with Dr. Fiddner and Dr. Rafoth in Stright 340
2:45 p.m. to 3:00 p.m.	Camp Evaluation in Stright 112A

Communicating

Speaking, writing, reading, and listening are the lifeblood of every human endeavor, particularly those in applied fields like computer science and cyber security. Without communication, there would be no research journals, books, lectures, or meetings. No theories, programming languages, or video games, and no one to teach, learn, or play them. Verbal communication makes just about everything we know about computers and computing possible, every bit as much as integrated circuits and wireless signals.

Communication often results in confusion and misunderstanding, however. How do we achieve *effective* communication? This week you will learn and discuss what listeners expect of good speakers, what readers look for in clear writers, and what audiences want from effective presenters. The learning will be active, and the instructors— Krista Sarraf and Ben Rafoth—will help you to apply effective communication strategies both to Dr. Fiddner's "Cyber Clash with China" simulation and to other situations as well.

The first session, "Speak Up: Or Forever Hold Your Peace," focuses on three settings where speaking occurs most often: to a large group or audience, in a small-group discussion, and in an interpersonal or one-to-one setting. Speakers and listeners behave very differently in each of these settings, and you will participate in scenarios that require you to examine your assumptions about speaking and speakers.

The second session, "More Than Words: Writing for Cybersecurity," introduces the concept of the *rhetorical situation*, which encourages you to ask, What is the message and its purpose? Who is delivering it? Who is it intended for? Though they may seem simple, these questions probe the essence of every communicative act and reveal answers to why communication succeeds or fails. In this session, we look at why some messages can do as much harm as good.

Finally, "Giving a Great Not Boring Presentation: Three Steps to Killing It" will help you learn to make your points in an effective and focused way so that you come across as credible and confident speakers and writers. That recommendation about China to the President? You'll learn to kill it.

Title: Computational Thinking Lab!

With the motivation of future careers in technology and cybersecurity in their minds, students will team up in "friendly competition style" to discover several clues needed to solve a mystery! These clues will come from collaboration on strategies employed in both technical and nontechnical problem solving. Students with 21st Century superpowers in communication, collaboration, critical thinking and creativity will triumph in the lab (and hopefully in their careers some day)! References to cyber-security principles will be woven throughout the activities and strategies applied, and a discussion of trends in college majors will conclude our exploration!

Cyber Clash with China

https://modeldiplomacy.cfr.org/#/simulations/20181/

Exercise to practice:

1. Collaboration
2. Critical thinking - disciplined thinking that is clear, rational, open-minded, skeptical, and unbiased analysis or evaluation of factual evidence (Dictionary.com Unabridged).
3. Writing
4. Oral Communication

GENERAL ADVISOR TO THE PRESIDENT

The **general advisor** offers analysis and recommendations that are unconstrained by the interests of any department or agency. He or she is tasked with providing a comprehensive assessment of the situation at hand and ideas for policy options that serve U.S. interests.
The general advisor's goals are to

- understand the breadth of the issue and outline its stakes for the United States; and
- advise the president on the range of policy options.

The president needs to decide, after receiving advice from, how the United States will react to the attack. You will consider three types of responses, alone or together:

1, cyber responses, such as disrupting Chinese networks in a manner proportionate to the hack against the Nasdaq;

2. economic sanctions on Chinese government entities and state-owned enterprises connected to the recent hacks; and military responses, such as increased freedom of navigation operations and

3. a larger U.S. military presence more broadly in the South China Sea.

Tasks:

1. Develop a position memorandum of your recommendations to the President on what he should do in this situation.

2. Prepare and deliver an oral briefing to the President on the contents of your position memorandum.

The Issue

Cyberspace is a new domain of conflict, one with few accepted rules or standards of behavior. After years of official silence, the U.S. government has gradually become more transparent about its development and use of cyberattacks. The 2015 Defense Department cyber strategy, for example, explicitly recognizes offensive missions, directing the Pentagon to develop cyber capabilities that can support military operations. Although it is widely believed that the United States and Israel were behind Stuxnet, the malicious software (malware) designed to slow Iran's nuclear program by damaging centrifuges at the Natanz nuclear facility in 2009, the United States did not admit any role. Instead, the first public acknowledgment of the United States' use of cyber weapons came in February 2016 when Pentagon officials announced that U.S. Cyber Command had launched attacks against the self-proclaimed Islamic State, also known as ISIS. U.S. Cyber Command has grown from approximately nine hundred personnel to more than six thousand, and total requests for cyber operations in the 2017 defense budget were $6.7 billion, an increase of more than 15 percent from 2016.

Offensive cyber operations are an attractive tool for policymakers because they are relatively inexpensive, may be less destructive than kinetic strikes (i.e., those against physical targets), and may provide a high degree of anonymity to the attacker. The vast majority of attacks are cyber espionage (theft of military and political secrets or intellectual property) and political disruptions (website defacement or distributed denial of service [DDoS] attacks that flood a website with so much data that it can no longer respond). The White House's 2011 International Strategy for Cyberspace warns that the "United States will respond to hostile acts in cyberspace as we would to any other threat to our country." However, although it is widely assumed that a cyberattack that caused death or physical destruction would be considered an armed attack, the threshold for a military response to other forms of cyberattacks remains uncertain.

Indeed, cyberspace is an environment of high strategic instability. Defending against cyber threats is extremely difficult. Would-be defenders need to worry about millions of lines of computer code, hundreds of devices, and scores of networks, but an attacker needs to find only one vulnerability. Attribution of cyberattacks is difficult and slow, which makes them vastly different from other weapons. Attackers can hide their tracks, routing attacks through multiple computers in numerous countries, and the attacks can happen in minutes, if not seconds. Many countries rely on proxies, criminal groups, or patriotic hackers to conduct operations. Thus, even if hackers are located within a state, it may remain unclear who authorized an attack. This can greatly complicate efforts to retaliate and prevent further attacks.

Yet uncertainty about the efficacy and advisability of cyberattacks is considerable. Attacks may spread from the target networks to those of uninvolved third parties. Determining the effects of an attack requires analysis and interpretation of an event at multiple targets. Defenders can respond quickly to successful attacks, patching software and changing network configurations, so cyber weapons are likely to be "one and done."

Moreover, successful attacks are likely to risk escalation. To weaken the enemy's ability to fight, attackers will take out the computers that control opposing forces. Such attacks impair enemy leaders, limiting their ability to order forces in the field to pull back or cease combat. If commanders believe they will lose the use of important weapon systems early on in a conflict, they have an incentive to use them preemptively, further destabilizing the situation.

Decision Point

China, Taiwan, Vietnam, Malaysia, Brunei, and the Philippines have competing territorial and jurisdictional claims in the South China Sea. In recent years, China has exerted authority over the area by increasing the size of existing islands or creating new islands, as well as by constructing ports, military installations, and airstrips. The United States has promoted the right of military vessels to operate in China's claimed two-hundred-mile exclusive economic zone and has rejected China's claim to a twelve-mile territorial zone around the artificial islands China has built. Since 2015, the United States has signaled its opposition by flying military aircraft and sending U.S. naval ships near some islands.

Over the past several weeks, there have been several near misses in the South China Sea involving U.S. and Chinese military vessels and aircraft. So-called patriotic hackers—individuals who act out of nationalist pride or anger—in China and the United States have defaced websites in both countries. The Pentagon recently announced that its website had been breached, and in the last two months China-based hackers have stolen a trove of electronic documents from U.S. military networks, including information about an upcoming joint exercise with the Philippine Navy.

Last week, the U.S. Air Force conducted a flight near a shoal claimed by China in the South China Sea. Three days later, the Nasdaq Stock Market suffered a hack that damaged computers and forced the suspension of trading for two days, imposing significant costs on various U.S. companies and denting confidence in the U.S. economy. The Zheng He Squadron, an underground hacker collective based in China, has taken credit for the hack. The group has known ties to the People's Liberation Army (PLA), China's military. U.S. intelligence agencies assess with 90 percent certainty that the hack occurred with the knowledge or support of parts of the Chinese government. Beijing, however, claims that it has no knowledge of the attack and warns Washington that "irresponsible, unscientific" attempts at attribution are a distraction from the United States' own hacking and will heighten mistrust between the two countries.

More To Watch

Study: China Flirts With War in South China Sea

Right now, we've got about three billion people online, and they are using anywhere from five to fifteen million devices. And all of these devices are connected and all those connections represent doors … Most of these devices have vulnerabilities in them, and so that creates backdoors, and somebody's going to find them.

— Dorothy E. Denning, distinguished professor at the Naval Postgraduate School, October 9, 2015

Additional Reading

These 5 Facts Explain the Threat of Cyber Warfare

Fact Sheet: The Department of Defense (DOD) Cyber Strategy

Why Is the South China Sea Contentious?

The Context

The United States and China have significant disagreements over cyber espionage, cyberattacks, and internet governance. These differences have intensified in recent years as cyber issues have become more significant on the bilateral and global agenda.

In late 2009 or early 2010, Iran replaced about one thousand of the nine thousand centrifuges deployed at its fuel enrichment plant at Natanz. The centrifuges had been damaged by sophisticated malware, eventually known as Stuxnet, which was allegedly developed and launched by the United States and Israel to slow down Iran's nuclear program. The Natanz plant seriously concerned these two countries because its centrifuges were producing enriched uranium, which can, if properly processed, be used in a nuclear weapon. Sometime in the summer of 2010, Stuxnet escaped into the wild, eventually spreading to more than 115 countries, though it did no damage to other systems. The United States also reportedly developed a cyberattack plan, code-named Nitro Zeus, to be used if negotiations failed to limit Tehran's nuclear program and military conflict erupted. U.S. Cyber Command reportedly planned attacks on air defenses, communications, and parts of the power grid. The United States, Iran, and other powers reached a deal over Iran's nuclear program in 2015, and the apparent cyberattack plan has never been used.

After Stuxnet was discovered, Iran retaliated with its own cyberattacks. Between September 2012 and June 2013, an activist group called Izz ad-Din al-Qassam Cyber Fighters took credit for roughly two hundred distributed denial of service (DDoS) attacks on almost fifty Western financial institutions, including SunTrust, JPMorgan Chase, CitiGroup, Wells Fargo, U.S. Bancorp, Capital One, PNC, and HSBC. These attacks made websites unavailable for a few hours but did not threaten the integrity of the financial system.

In August 2012, the Shamoon malware struck Saudi Aramco, Saudi Arabia's state-owned oil company, which supplies about a tenth of the world's oil. Shamoon corrupted tens of thousands of hard drives and shut down the employee email service. The company had to replace thirty thousand computers but the malware did not affect systems involved with technical oil operations. A subsequent attack damaged RasGas, a joint venture between Qatar Petroleum and ExxonMobil. Data was destroyed but production continued. A group calling itself the Cutting Sword of Justice claimed responsibility, but in this case, as in the earlier financial attacks, U.S. officials speaking off the record blamed the Iranian government. Saudi Arabia, predominantly Sunni, and Iran, predominantly Shiite, often compete for influence and leadership in the Middle East.

During Thanksgiving week in 2014, employees of Sony Pictures lost access to the company's computer networks and their email accounts due to a massive hack. The hackers, operating under the name Guardians of Peace, not only stole one hundred terabytes of internal data but also damaged two-thirds of the company’s servers and computers. On December 19, 2014, the FBI announced that the Guardians of Peace were North Korean government hackers. Pyongyang had previously expressed outrage over the Sony film The Interview, which depicts the assassination of its supreme leader, Kim Jong-un. This was the first time the U.S. government had explicitly and directly named another government as responsible for hacking.

On January 2, 2015, the United States levied economic sanctions on the Reconnaissance General Bureau, a North Korean intelligence agency; the Korea Tangun Trading Corporation, which acquires military-related materials and technology for North Korea; and the Korea Mining Development Trading Corporation, the country’s main exporter of ballistic missiles and conventional weapons. The United States also reportedly asked the Chinese government for help with identifying and controlling North Korean hackers, some of whom were reportedly based in a hotel in northeastern China, but public statements from Beijing were noncommittal. Around this time, North Korea (formally the Democratic People’s Republic of Korea, or DPRK) disappeared from the internet. The few DPRK websites available to the outside world were knocked offline by a DDoS attack. Despite some suspicion that the U.S. government was responsible, the attack was more likely conducted by individual hackers or a group of activists.

In March 2016, the United States indicted seven Iranians working for entities affiliated with the Islamic Revolutionary Guard Corps for conducting cyberattacks in 2012 and 2013 against the U.S. financial sector, and also charged one of them with unauthorized access to the control systems of a New York dam. The United States also announced that Cyber Command was engaged in offensive operations against the Islamic State. According to the *New York Times*, U.S. military hackers first placed “implants” in the militants’ networks to learn about commanders, then began to alter messages to make fighters more vulnerable to attack by U.S. drones. In other cases, Cyber Command disrupted the Islamic State’s financial transactions.

The 2016 U.S. presidential election was marked by repeated hacking incidents. In July, thousands of emails from the Democratic National Committee (DNC) were leaked and subsequently published by Wikileaks. The fallout was significant, leading to the resignations of DNC chairwoman Debbie Wasserman Schultz, representative from Florida, and many top party aides. In the fall of 2016, thousands of emails from the personal Gmail account of John Podesta, the chairman of Hillary Clinton’s presidential campaign, were also released. Researchers concluded that hackers linked to Russian intelligence were behind both the DNC and the Podesta hacks. The U.S. government also denounced the incidents as Russian-directed hacking, accusing Russia of attempting to interfere in U.S. elections. In December 2016, the White House announced that it was expelling thirty-five Russian spies from the United States and sanctioning nine individuals and organizations linked to the hacking: the FSB and GRU, four intelligence officers, and three companies that provided material support to the hackers.

Since 2005, a small group of governmental experts has gathered at the United Nations (UN) to discuss cyber threats. The group, which includes government representatives from China, Russia, and the United States, signed a nonbinding report in 2013 agreeing that international law applies in cyberspace. This means, among other things, that cyberattacks can be considered a use of force, that a state can exercise the right to self-defense if it is the victim of a cyberattack, and that the laws of armed conflict apply to cyberwar. The 2013 report also asserted that states are responsible for and should act against cyberattacks that originate within their territories. In 2015, the same group agreed to a set of peacetime norms promoted by the United States. These norms include the idea that states should not attack each other's critical infrastructure or target each other's computer emergency response teams—national agencies that defend against and help recover from cyberattacks. The norms also hold that countries should assist other nations investigating cyberattacks and cybercrime. However, the 2017 round of negotiations ended with the participants unable to identify new norms or agree whether international law applied to cyberspace.

Additional Reading

The Inside Story of the Biggest Hack in History

U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict

Iran Learns From U.S. Cyberattacks

Recent History

Chinese cyberattacks in particular are often driven by the desire to collect political and military intelligence. According to a *Washington Post* report, Chinese hackers have stolen information relating to over two dozen U.S. weapons programs, including the Patriot missile system, the F-35 Joint Strike Fighter, and the U.S. Navy's new littoral combat ship. The State Department, the White House, the Office of Personnel Management, and NASA have been breached. China's cyber espionage, however, has not been limited to U.S. targets. Embassies, foreign ministries, and the government offices of India, South Korea, Indonesia, Romania, Taiwan, and Germany, among others, have also been breached.

Cyberattacks are also motivated by the need to move Chinese industries out of labor-intensive, energy-inefficient, highly polluting manufacturing sectors to cleaner, more technology-intensive ones. The Chinese fear being caught in a technology trap, dependent on U.S., Japanese, and European firms for core technologies. Cyberattacks are intended to acquire information that could help Chinese firms develop such technologies themselves. Attacks on Google, Yahoo, Adobe, Symantec, Juniper Networks, Disney, Sony, Johnson & Johnson, General Electric, General Dynamics, and DuPont have been publicly reported. Chinese hackers have also reportedly targeted the negotiation strategies and financial information of energy, banking, law, and other sectors.

In response to U.S. claims of Chinese hacking, China has noted that it is also a victim of cybercrime, with the majority of attacks originating from IP (Internet Protocol) addresses in Japan, the United States, and South Korea (formally the Republic of Korea). The Chinese press was quick to echo claims by the National Security Agency (NSA) contractor Edward Snowden that the United States hacks targets on the Chinese mainland and in Hong Kong.

Chinese cyber strategy has a military dimension as well. PLA analysts write frequently of seizing information dominance early on in a conflict by conducting cyberattacks on an enemy's command and control centers. These centers allow commanders to collect information, issue orders, and monitor operations. Follow-up attacks would target transportation, communication, and logistics networks to slow down an adversary. To prepare for this strategy in any potential conflict with the United States, Chinese actors appear to be surveilling and entering military networks as well as some critical U.S. infrastructure, such as power grids and oil and gas pipelines. U.S. military doctrine—in particular the Air-Sea Battle doctrine (now known as Joint Concept for Access and Maneuver in the Global Commons), adopted to defeat cruise missiles, submarines, and cyber capabilities—also assumes cyberattacks on an adversary's sensors, networks, launchers, and weapons in the beginning stages of a conflict.

As with economic policy and national security, Chinese President Xi Jinping has consolidated control over cybersecurity by creating a so-called small leading group, an ad hoc body that advises the Politburo and implements decisions. Moreover, on December 31, 2015, China's Central Military Commission overhauled the organizational structure of the PLA, establishing three new branches. One of them is the Strategic Support Force, whose operations remain unclear but whose responsibilities will reportedly include intelligence, technical reconnaissance, electronic warfare, cyber offense and defense, and psychological warfare.

Beginning in 2013, Washington publicly increased pressure on Beijing over cyber espionage. In March 2013, for example, National Security Advisor Tom Donilon spoke of the "serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." Two months later, the Defense Department went further, and, in a break from the past, directly blamed the Chinese government and military for espionage.

In May 2014, the Department of Justice charged five Chinese hackers with stealing the business plans, internal deliberations, and other intellectual property of Westinghouse Electric, United States Steel Corporation, and other companies. The department claimed the hackers were members of the PLA's General Staff, Third Department, Unit 61398, located in Shanghai. The indictment incensed the Chinese government, which quickly suspended a high-level bilateral cyber working group.

In April 2015, President Barack Obama signed an executive order that declared a national emergency to deal with the threat of "significant malicious cyber-enabled activities," allowing for economic sanctions against companies or individuals that profited from cyber theft. The order threatened to block financial transactions routed through the United States, prevent exports to the United States, and prevent executives from the companies that benefit from the hacks from traveling to the United States. After departing the United States, Xi signed similar agreements with the UK and at the G20 meeting in Turkey.

In August 2015, the *Washington Post* reported that the Obama administration planned to levy these sanctions against Chinese companies in the lead up to the summit the next month between Presidents Obama and Xi. Perhaps because of the threat, the summit produced a breakthrough agreement. Both sides pledged that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." Washington and Beijing also agreed to identify and endorse norms of behavior in cyberspace and establish two high-level working groups and a hotline between the two sides.

Following the September summit between the two presidents, the cybersecurity firm FireEye reported a sharp decline in the number of Chinese cyberattacks, though it also suggested that actors might have become stealthier and more difficult to detect. U.S. Assistant Attorney General John Carlin confirmed the company's findings that attacks were less voluminous but more focused and calculated.

The US-China group on security issues only met once before the end of the Obama administration, but the cyber crime group reported some small progress. The two sides established a point of contact and a designated email address, and successfully cooperated on taking down fake websites.   After President Trump met President Xi at Mar-a-Lago in April 2017, the Washington and Beijing agreed to a United States-China Comprehensive Dialogue that will have four pillars, including one on law enforcement and cybersecurity.

We know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity, and water plants, and those that guide transportation throughout this country.

— Leon Panetta, then U.S. Secretary of Defense, October 12, 2012

Other Interested Parties

Other Asian countries: The countries involved in maritime disputes with China—Japan, Malaysia, Taiwan, Vietnam, Brunei, and the Philippines—all have an interest in how this dispute and the broader issue of cyber behavior are managed or resolved. Japan, Vietnam, Taiwan, and the Philippines have also been the targets of Chinese cyber espionage campaigns as well as DDoS attacks and website defacements.

In 2002, China and the Association of Southeast Asian Nations (ASEAN) signed a Declaration on the Conduct of Parties in the South China Sea. The agreement called on all claimants not to resort "to the threat or use of force" in pursuing their objectives in the area, and to work on a code of conduct. ASEAN ministers tried to reinvigorate the code in 2012, but little progress has been made. No code of conduct has emerged. ASEAN has struggled to find a coherent diplomatic position that supports the four members (Brunei, Malaysia, the Philippines, and Vietnam) who have disputes with China, some of which are more willing to compromise than others, given the reality that China is the largest trading partner of many ASEAN states. ASEAN has also been active in trying to develop confidence-building measures for cyberspace, holding a number of regional and bilateral (ASEAN-China and ASEAN-Japan) conferences on cyber norms. Acting individually, the Philippines in 2013 brought a claim against China over the sovereignty of the Spratly Islands to the Permanent Court of Arbitration (PCA), a tribunal in The Hague. In July 2016, the court ruled unanimously in the Philippines' favor, dismissing China's claims to territorial rights over a large expanse of the South China Sea. The court also "found that China had violated the Philippines' sovereign rights" by building artificial islands and meddling in fishing and oil exploration. China had previously stated that it would "neither accept nor participate in the arbitration unilaterally initiated by the Philippines," and rejected the ruling.

U.S. Allies: The European Union has expressed support for U.S. freedom of navigation operations in the South China Sea, as well as a vision of the internet that is global, open, and secure. The United Kingdom, Germany, and the Netherlands have been particularly vocal proponents of developing norms of state behavior in cyberspace. In 2011, the U.S.-Australia alliance was extended to cover cyberattacks and, in the summer of 2014, NATO declared that cyber defense was part of alliance's "core task of collective defense." Depending on the severity of the attack, both treaties could create a mutual defense obligation for cyberattacks.

U.S. Competitors: Russia, North Korea, and Iran will take a keen interest in Washington's response to this case given that they have all reportedly launched attacks on the United States and may do so again in the future. In addition, Moscow and Beijing signed a cybersecurity pact in May 2015 in which they stated they would not conduct cyberattacks on each other but would exchange technology and information on threats.

United Nations: The UN has also been increasingly focused on cybersecurity and international peace. In September 2011, Russia, China, Tajikistan, and Uzbekistan collectively proposed an international code of conduct for information security to be considered by the UN General Assembly, and have reintroduced it in subsequent years. It is also the basis of an agreement on cybersecurity adopted by the Shanghai Cooperation Organization, a regional organization that includes China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan (and India and Pakistan by 2016). In 2013, a group of governmental experts at the UN agreed in a report that international law, and the UN Charter in particular, applies in cyberspace. In 2015, the same group, which includes representatives of China, Russia, and the United States, agreed to a set of peacetime norms, including that states should not attack each other's critical infrastructure.

Guide to the Memorandum

A major goal is to strengthen your ability to write concise, articulate, and persuasive documents that busy colleagues can quickly absorb. You will write a position memorandum. This will improve your writing skills and give you a taste of how U.S. foreign policy is conceived, coordinated, and executed.

What is a memorandum?

- A memo is a succinct written message from one person, department, or organization to another. It is an important means of formal, written communication in the workplace. Business, government, law, and many other disciplines will prefer that you be proficient in memo-style writing. A memo is generally short, to the point, and free of flowery language and extraneous information. A memo is typically informative or decision-oriented and is formatted in a way that helps readers quickly grasp the main points.
- The NSC's role is to advise the president by generating and weighing policy options and overseeing the implementation of the president's policy decisions. The proposed options and recommendations need to be considered, coordinated, and articulated through some form of written communication. Memos do exactly that: they help analyze, evaluate, advocate, and channel policy options and decisions within the government bureaucracy.
- Memos also serve as a historical record. Many memos related to NSC discussions and presidential decisions are filed in the government's archives. Some are later declassified and released for future generations to understand how policy was devised at a given time in U.S. history. You can access historical examples of memos by searching online. One such resource is maintained by the Federation of American Scientists and offers links to memoranda and directives issued by various U.S. presidents.

Position Memo

- The memo you will write is called a position memo. This memo is written from the perspective of your assigned role. In about two single-spaced pages, it presents a set of policy options for consideration by the NSC and recommends one of them to the president.
- The position memo should provide brief background on the issue at hand; outline the United States' strategic objectives; present and analyze several policy options; and, finally, recommend and justify a particular course of action. Although conveying complex ideas in a concise way can be challenging, it will help your fellow NSC members consider the issue efficiently and facilitate decision-making by the president. Equally important, it will help you clarify your understanding of the case by forcing you to identify the essential facts and viable policy options.
- Make sure to take into account the pros, cons, and ramifications of each option as it pertains to your role, and as informed by your reading of the case materials and further research. Also anticipate critiques of your proposed policy and incorporate your response into the memo.

- The position memo below gives you a sample template to follow as you write your own memo. When reviewing the sample memo, pay attention to how they are structured, how much information they include, and how they advance their analysis and argument.

Position Memo Template

- **Subject and Background (two short paragraphs):** Briefly summarize the significance of the issue for U.S. foreign policy and national security and identify the central policy question(s) to be decided. Provide just enough information about the crisis so the reader can understand your memo's purpose and importance. Do not summarize the case in depth since your readers are already well-informed.
- **Objectives (bullet points):** Succinctly state your department's objectives in the current crisis. These can be general national security objectives (such as preventing war), or more specific goals tied to your department's mission (such as protecting U.S. citizens). They should be important to U.S. national security, directly tied to the case, and feasible. These objectives should guide the policy analysis and recommendation that make up the rest of your memo. This section requires exceptional clarity of thought.
- **Options and Analysis (one paragraph for each option):** Present and analyze several options for U.S. policy. Discuss their costs, benefits, and resource needs where possible. Be sure to acknowledge the weaknesses or disadvantages of each proposed option in order to illuminate the trade-offs inherent in complex policy decisions. No option is likely to be perfect.
- **Recommendation and Justification (several paragraphs):** Identify your preferred policy option(s) and provide more details about it or them. Explain your reasoning, keeping in mind that you aim to convince the president that he or she should follow your recommendation. Addressing the weaknesses or disadvantages you identified in the Options and Analysis section can help strengthen your argument.

SAMPLE POSITION MEMO

Office of the Secretary of Defense

Washington, DC

October 19, 1962

TOP SECRET

MEMORANDUM FOR: the President

the Vice President

the Secretary of State

the Secretary of the Treasury

the Attorney General

the National Security Advisor

the Director of Central Intelligence

the Chairman of the Joint Chiefs of Staff

SUBJECT: Options for a U.S. response to Soviet missiles in Cuba

This memo outlines options for U.S. action against Soviet missile installations in Cuba. On October 14, an American U-2 plane photographed Soviet construction of medium-range ballistic missile (MRBM) sites in Cuba, some of which contain missiles that could be launched within eighteen hours. Failure to swiftly eliminate this threat would encourage Soviet aggression and increase the risk of a nuclear attack on the United States.

BACKGROUND: U-2 reconnaissance has provided evidence of offensive Soviet military activity in Cuba, including the presence of MiG fighter jets, IL-28 bombers, and sites for SS-4 and SS-5 missiles with ranges between 1,000 and 2,200 nautical miles. These distances encompass Washington and other major U.S. cities. U.S. intelligence services estimate that the MRBMs will be ready to launch in eighteen hours and that the longer range SS-5 missile sites could be operational in December.

OBJECTIVES:

This agency has two principal objectives in this matter:

- eliminate the missiles located in Cuba
- avoid nuclear war with the Soviet Union

OPTIONS AND ANALYSIS:

In order to accomplish the aforementioned objectives, this agency proposes two options:

1. Implement a naval quarantine around Cuba.

   The United States could implement a naval quarantine on offensive military equipment bound to Cuba, thwarting the further growth and development of missile sites. A quarantine is a limited military response that takes direct action while reducing the risk of significant casualties, and it leaves room for additional U.S. action in the future. It would not, however, eliminate missiles already in Cuba, nor would it halt construction or operationalization of existing sites with equipment already delivered. It also risks escalation of the conflict due to miscommunication between ships or unpredictable Soviet behavior. To that end, if the president orders a quarantine, he should ask Chairman Khrushchev to preemptively stop Soviet ships en route to Cuba.

2. Order air strikes against missile sites in Cuba.

   The United States could carry out air strikes against missile sites in Cuba. These could entail surgical strikes targeting only MRBM sites or broader strikes that would also target other Soviet military assets, including IL-28 bombers, MiG jets, patrol boats, tanks, and airfields. Broader air strikes would eliminate missile sites and limit Soviet capability to retaliate against U.S. forces and U.S. bases in Florida. However, no air strikes guarantee 100 percent elimination of the missiles, making several rounds necessary. Moreover, sustained military action carries a relatively high risk of Soviet retaliation and the capture or death of U.S. pilots. This could set off a chain of events that necessitates a U.S. invasion of Cuba. Such an invasion, involving as many as 250,000 U.S. troops, could begin within seven days of air strikes. Though an invasion would be the most direct means of eliminating the threat in Cuba, it would also be the most costly.

RECOMMENDATIONS AND JUSTIFICATIONS:

This agency's first priority is to eliminate the missile threat from Cuba. To do so, it recommends that the president implement a naval quarantine on offensive military equipment headed to that island. The quarantine is a measured response that will inhibit Soviet plans in Cuba with significantly lower risk of casualties and escalation than air strikes. Moreover, if accompanied by dialogue with the Soviet Union, a quarantine could effectively lead to Moscow's removal of the missiles. The United States should seek approval of the quarantine from the Organization of American States in order to lend it further diplomatic weight.

Operationally, the U.S. Navy would establish a quarantine line and signal ships approaching it to stop for boarding and inspection. As a first warning, a nonresponsive ship would receive a shot across the bow, and as a second warning, a shot fired into the rudder to stop the vessel. Any ship determined to be delivering offensive weapons to Cuba, regardless of port of origin, would be turned back.

Although this agency prefers a quarantine, it recommends simultaneously preparing for air strikes and invasion in case such measures become necessary to eliminate the missile threat. The United States should reinforce its naval base at Guantanamo Bay, raise military alert levels, and take steps to protect U.S. shipping interests in the Florida Strait. The Joint Chiefs of Staff have separately identified such preparatory measures.

As part of any response, this agency supports continuing reconnaissance missions over Cuba and strengthening air defenses in the southeastern United States. Finally, the United States should advise the Soviet Union that any attack from Cuba will be seen as an attack from the Soviet Union itself and will prompt a commensurate U.S. response.

Critical Analysis

1. What is at stake in the conflicts among China and other Asian countries regarding the South China Sea? What interests does the United States have in the situation?
2. What are the chief characteristics of cyberspace as a domain of conflict? What advantages and disadvantages arise when governments and other entities contemplate using or defending against cyber weapons?
3. What have been the main achievements and shortcomings in the effort to develop rules and norms for how countries should behave in cyberspace?
4. What are some notable uses of cyber weapons by governments or other actors against either government or private targets? What has their impact been? What lessons, if any, can be drawn from this history for this case?
5. What are the principal motivations underlying Chinese cyber strategy? How has China sought to implement this strategy?
6. How has the United States reacted to Chinese cyber activities? What policy steps has the United States pursued with China in the cyber realm more broadly? What does this history suggest for a policy decision in this case?
7. What are the root causes of the conflict presented in this case?
8. What options are available to the United States in this case? What are the potential benefits and drawbacks of each option?
9. What other parties are interested in this case? How do their interests intersect with those of the United States? What do these parties and intersecting interests suggest for a U.S. policy decision?
10. What are the goals of a U.S. policy decision in this case? How do these goals align or conflict with each other? What trade-offs might you be willing to make to pursue them?

Title: Cybersecurity 101: Threats, Vulnerabilities, and Hands Exercises

Abstract:

This session will review the basics of cybersecurity by discussing common threats and vulnerabilities from Russian botnets to common malware. The session will include a hands on component that uses web-based and common PC tools to explore threat sources and basic cybersecurity situational awareness techniques.

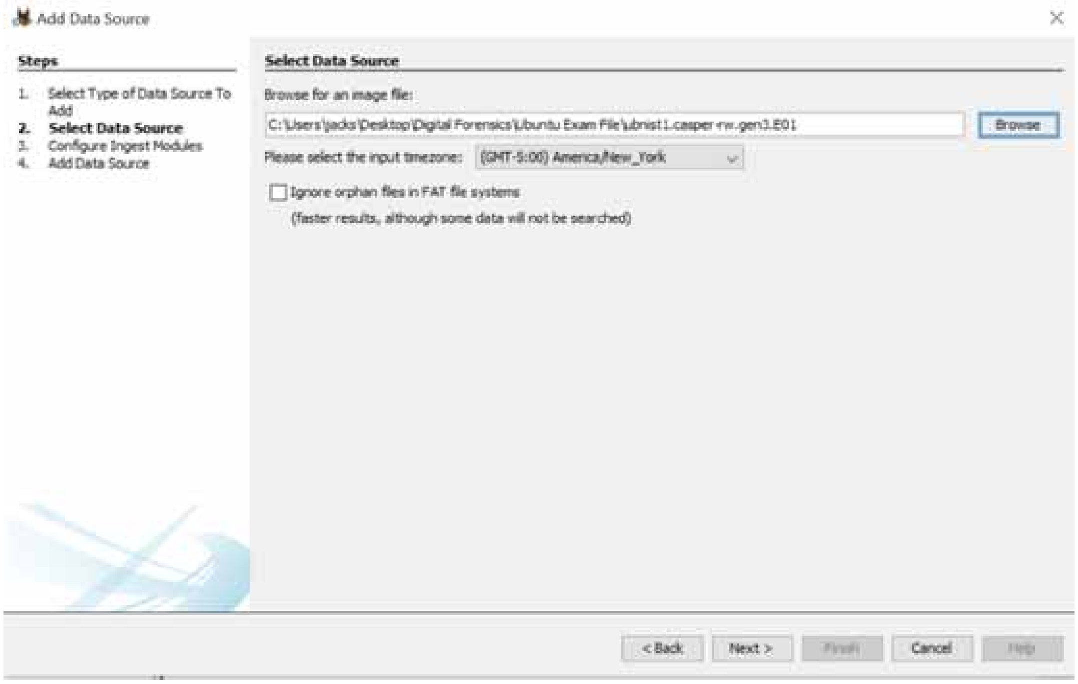
BIO:

Isaac Porche is a senior engineer at the RAND Corporation and program director for the Homeland Security Operational Analysis Center (HSOAC). His areas of expertise include acquisition, homeland security, cybersecurity network and communication technology, intelligence, surveillance, and reconnaissance (ISR); information assurance, big data, and cloud computing. He has led research projects for the U.S. Navy, U.S. Army, the Department of Homeland Security (DHS), the Joint Staff, and the Office of the Secretary of Defense. He is a member of the U.S. Army Science Board, serving on the data-to-decisions panel and the tactical cyber panel. He has assessed collaboration and information-sharing issues, and modeling and simulation of tactical network communication technologies. For the Navy, he studies ISR issues and led the TCPED study as well as the AoA for the DCGS-N and MTC2 programs of record. He has published articles in the Military Operations Research on "The Impact of Networking on Warfighter Effectiveness" (2007) and "Game-Theoretic Methods for Analysis of Tactical Decision-Making Using Agent-Based Combat Simulations" (2009). His RAND publications include The Impact of Network Performance on Warfighter Effectiveness (with Bradley Wilson, 2006); Navy Network Dependability: Models, Metrics, and Tools (Porche et al., 2010); and Finding Services for an Open Architecture: A Review of Existing Applications and Programs in PEO C4I (Porche et al., 2011). Porche has served as a consultant for Automotive News. He received his Ph.D. in electrical engineering and computer science from the University of Michigan.

Digital Forensics Investigation II

The second digital forensics module continues the examination of evidence files. It starts of by having the students create a second case and upload a new evidence file. While it loads, it explains how data analysts securely generate an evidence file from a hard drive or USB drive, along with the importance of using a write blocker when generating these files. This module also gives a brief introduction to data carving, or the process of extracting information from deleted files. Moreover, it teaches students how to access archived files, and extract files from a zip file as an example. In addition, the module explains how to view the data after it is sorted by file type and discusses how to view documents based on the system it was created in, such as documents from Microsoft Office. This module shows students how to use the media viewer to view images and videos. It also demonstrates how to generate a timeline from the timestamps Autopsy extracts from the data in the evidence file. The session concludes by showing the students how to generate a report from all the materials they viewed.

1. We will begin this module by opening a new case. So first open Autopsy. Then click create new case and select a directory of wherever you want the file to be located. Then fill in the examiner information, and finish creating the new case. Next, we will want to upload the evidence file for examination. The file we'll be using for this case is titled "ubinst1.casper-rw.gen3.E01"



Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

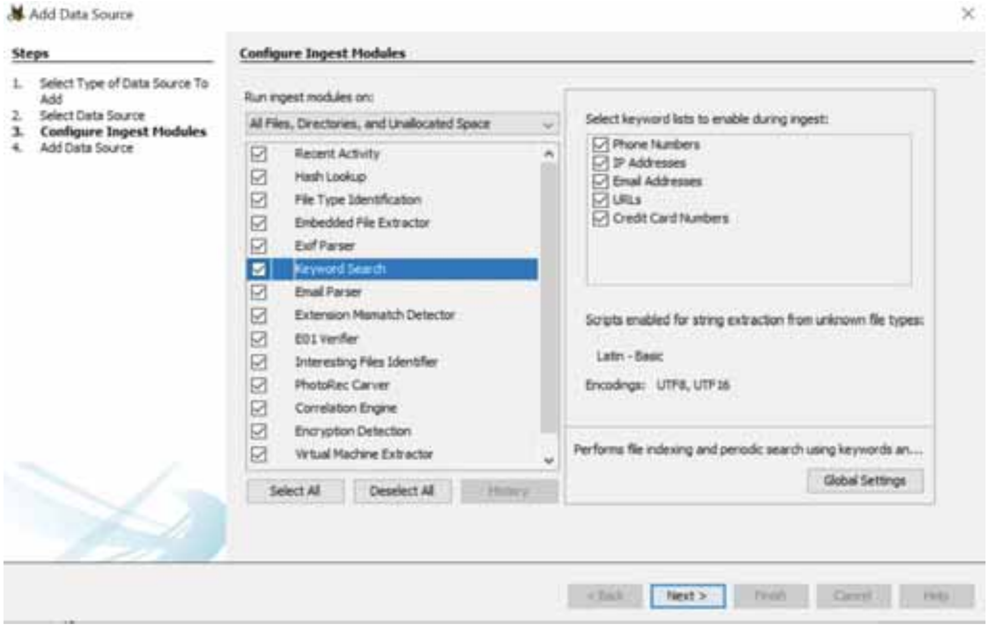
Select Data Source

Browse for an image file: C:\Users\jacks\Desktop\Digital Forensics\Ubuntu Exam File\ubinst1.casper-rw.gen3.E01

Please select the input timezone: (GMT-5:00) America/New_York

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

2. After selecting the file, make sure that all the boxes on the screen titled "Configure Ingest Modules" are checked. Scroll down to where it says, "Keyword Search", and make sure all the sub boxes are checked as well. Then, click next and finally finish.



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ Correlation Engine
☑ Encryption Detection
☑ Virtual Machine Extractor

Select keyword lists to enable during ingest:

☑ Phone Numbers
☑ IP Addresses
☑ Email Addresses
☑ URLs
☑ Credit Card Numbers

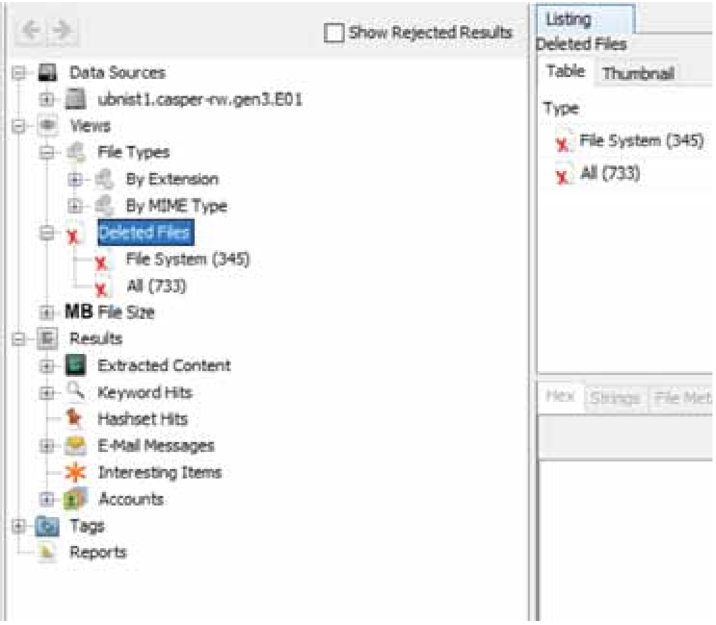
Scripts enabled for string extraction from unknown file types:

Latin - Basic

Encodings: UTF8, UTF16

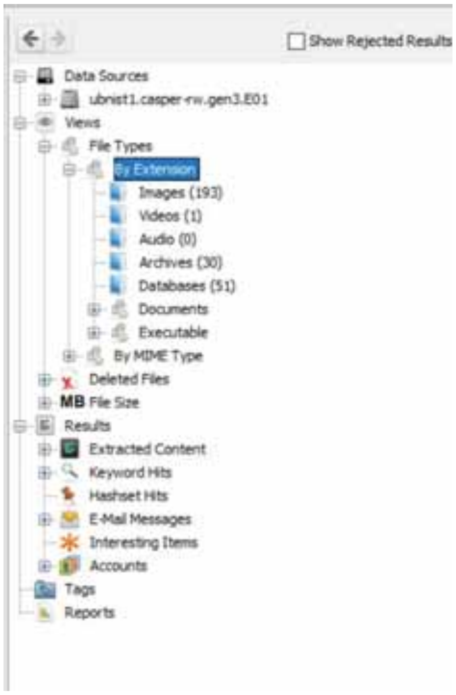
Performs file indexing and periodic search using keywords an...

3. This will take a couple minutes to load in the mean time we will discuss a few things. Last time, we examined a basic evidence file. But how are evidence files made? Evidence files are what are referred to as “Images” of a hard drive. Using a tool like FTK Imager (Forensic Toolkit Imager) this allows a data analyst to take a suspect hard drive or flash drive and convert it into a file that can be analyzed.
4. In the real world and forensic analyst would use something called a write blocker. A write blocker is a device or a piece of software that would allow you to access the data for file conversion, but not allow the device to access your computer. The purpose of this would be to keep any viruses, malware, or other harmful data from entering your computer.
5. File Carving is the process of analyzing known file types, in the internal file management system. Data Carving is the process of analyzing files that are not known. Most of the time it is because the files have been deleted but not re-written over yet. In the standard spinning disk hard drive, data is stored in sections using a process that converts data into magnetized sections which holds the data. When information is deleted, it still lingers there until data is written back over it. When it never gets rewritten, this allows Autopsy to extract the “deleted” data.
6. As you might imagine criminals are not going to want to keep data around that could incriminate themselves, so they delete it. Sometimes this deleted data is what can make or break a case. It could link someone to a crime, or in cases of owning things like child pornography could prove their quilt. This is a tool many different cases are going to need to help them prove or disprove their case.
7. Hopefully by now, the files are fully loaded in, so we can start our examination. First let’s look at deleted files. Let’s expand where it says “Views”, then “Deleted Files”. As you can see there is 345 in the File System, but 733 overall. Take a couple minutes to look through these and see what you can find.

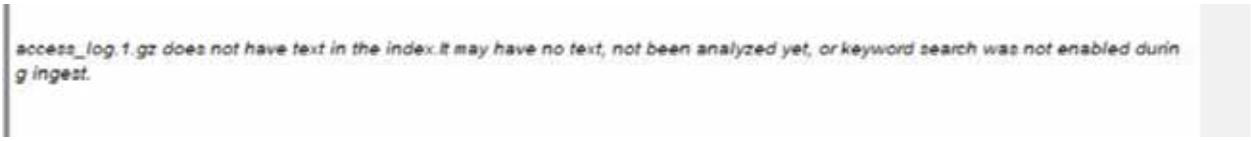


8. As you might notice some of these files don’t really make any sense. This could be for several different reasons. The file could be encrypted, the file may not be complete, part of the file could have been written over resulting in a incomplete file, or the file may be for system settings, or part of some program. Like the .xml extension is for web development.

9. Autopsy likes to make data as easy to view as possible. By clicking “Views” then “File Types” and finally “By Extension”, this allows you to see what file types are available. For example, there is 193 images, a video, 30 archives (Things like Zip files), and 51 Databases. Take some time to look through these files.

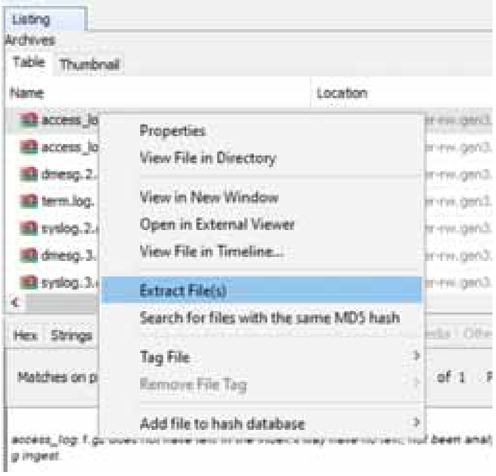


10. Many of the archive files give you a message like this:

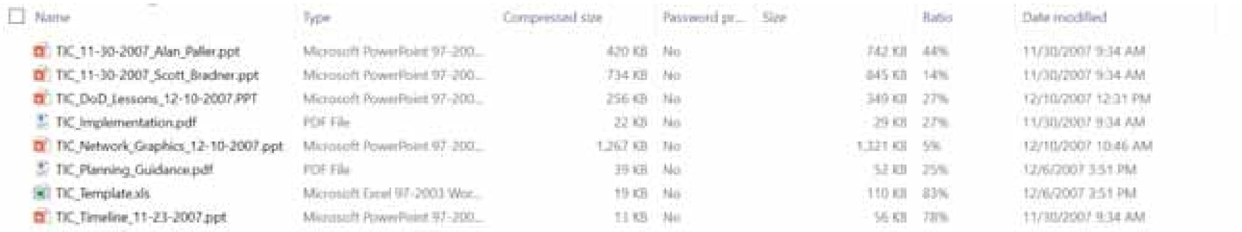


access_log.1.gz does not have text in the index.It may have no text, not been analyzed yet, or keyword search was not enabled durin g ingest.

11. However, we can still look through these files. In order to do this let’s make a folder on the desktop, and label in Autopsy Things or something along those lines. You can make a folder by right clicking on the desktop, clicking new, and then folder.

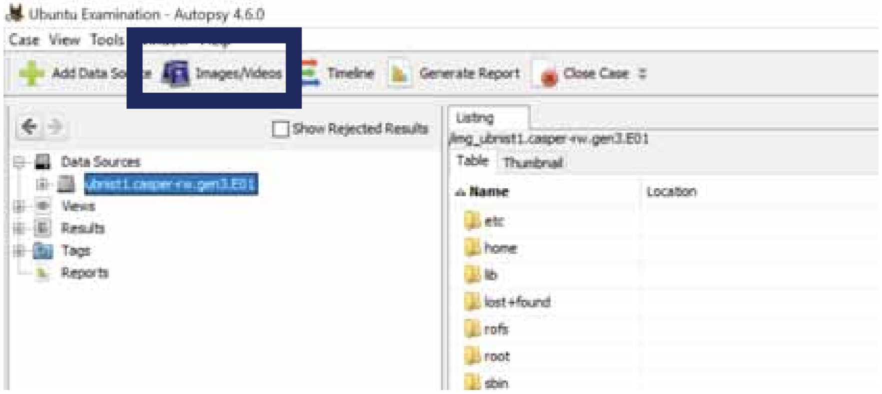


12. Next, lets right click on one of the archive files in Autopsy. I recommend the "Trusted_Internet_Connections.zip". Then click on where it say's "Extract File(s)". Then select the folder you just made on the desktop. And finally click save. You can now open the Zip file and view the contents like you would anything else in windows. We can gain some useful information here, such as the file name, file type, and the date it was modified.

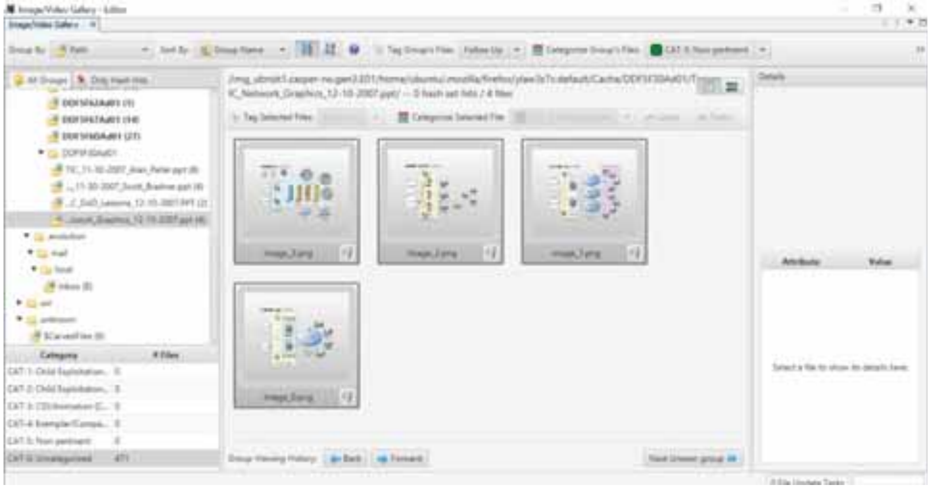


Name	Type	Compressed size	Password pr...	Size	Ratio	Date modified
TIC_11-30-2007_Alan_Paller.ppt	Microsoft PowerPoint 97-200...	420 KB	No	742 KB	44%	11/30/2007 9:34 AM
TIC_11-30-2007_Scott_Bradner.ppt	Microsoft PowerPoint 97-200...	734 KB	No	845 KB	14%	11/30/2007 9:34 AM
TIC_DoD_Lessons_12-10-2007.PPT	Microsoft PowerPoint 97-200...	256 KB	No	349 KB	27%	12/10/2007 12:31 PM
TIC_Implementation.pdf	PDF File	22 KB	No	29 KB	27%	11/30/2007 9:34 AM
TIC_Network_Graphics_12-10-2007.ppt	Microsoft PowerPoint 97-200...	1,267 KB	No	1,321 KB	5%	12/10/2007 10:46 AM
TIC_Planning_Guidance.pdf	PDF File	39 KB	No	52 KB	25%	12/6/2007 3:51 PM
TIC_Template.xls	Microsoft Excel 97-2003 Wor...	19 KB	No	110 KB	83%	12/6/2007 3:51 PM
TIC_Timeline_11-23-2007.ppt	Microsoft PowerPoint 97-200...	11 KB	No	56 KB	78%	11/30/2007 9:34 AM

13. Instead of using the file extension tab to view images, Autopsy provides a built-in tool to do this. In the upper left- hand corner you can see a button called "Images/Videos".



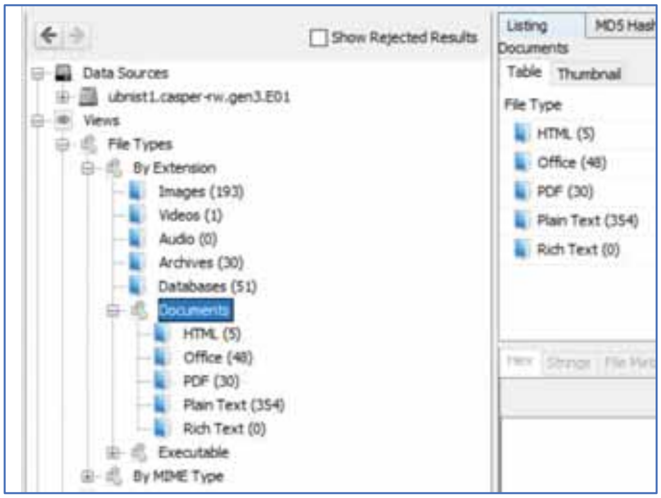
14. When you click it, it should bring you to a screen like this…



15. Here you can see how many photos there are, and what category they fall in. This can be a useful tool, for finding photos, where they are, and a secure place to view media.

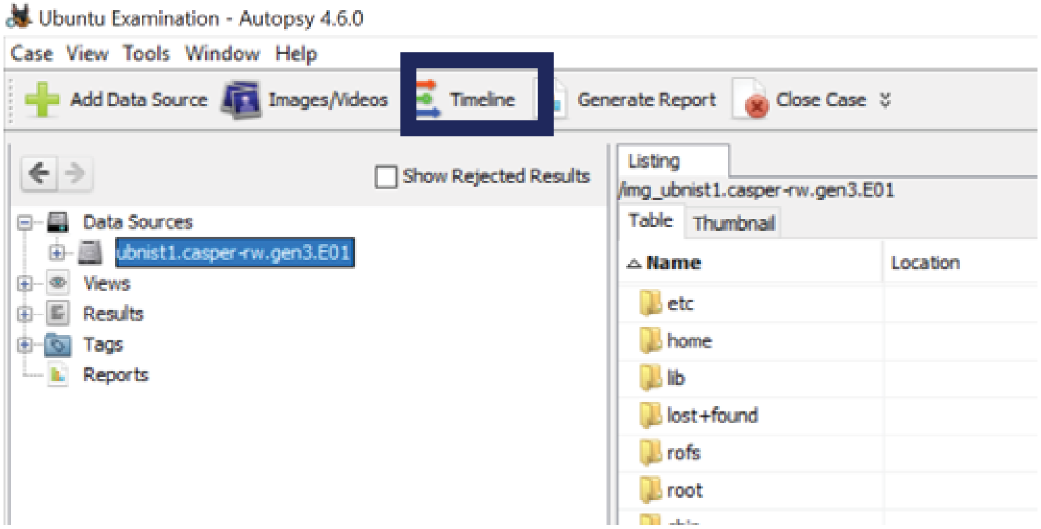
16. Going back to viewing data by file type, you can also view documents by what program was used to create them. By expanding the tab named "File Types", Then "By Extension", and finally "Documents". Here you can see that there are 5 HTML documents, 48 Office Files, 30 PDF's, and

354 Plain Text documents. Take a few minutes to look through these documents and see what you can find.

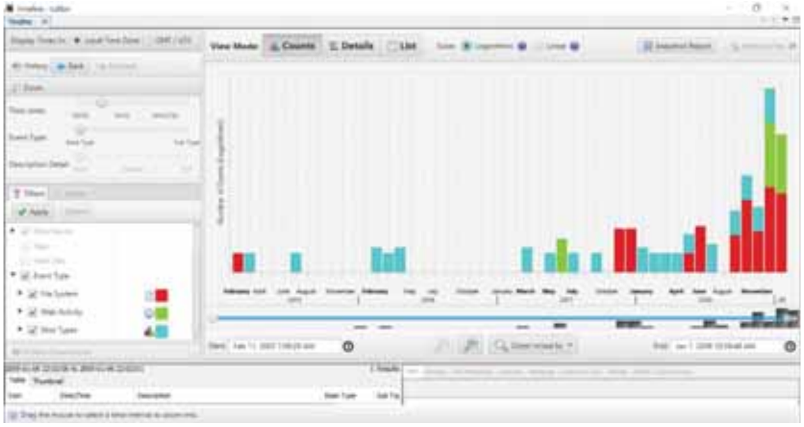


17. As you can see this tab includes files that have been deleted. It also shows files that may be in other languages, so you may need a translation program if you want to fully read and understand what the file says.

18. In the upper left corner there is a button labeled “Timeline”, and it allows you to see when all the files were accessed.



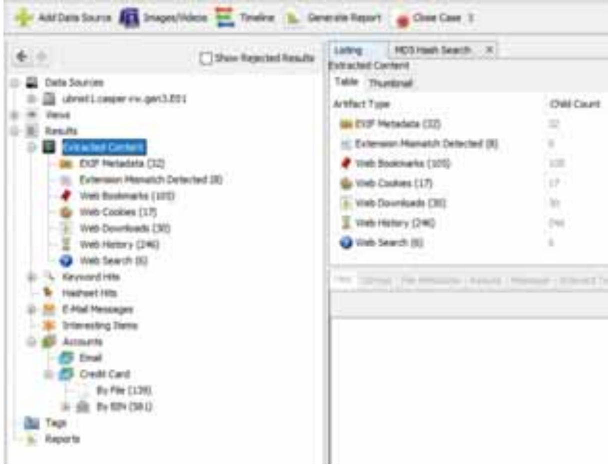
19. After clicking it, you should see this screen.



20. This is useful for seeing when data was accessed and gives a nice color-coded scheme for viewing different data types. Take a few minutes and see what you can gather from this data.

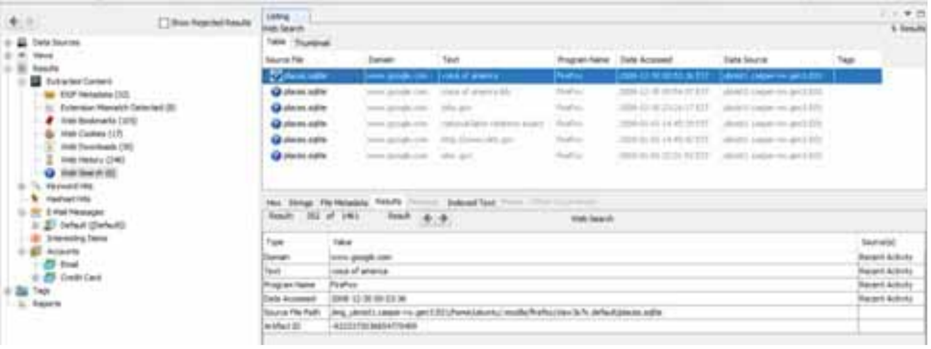
21. By changing from the logarithmic scale to a linear scale, you can see a physical change in the picture. The detail list also offers a unique look. Each of these modes has their own advantages. The standard bar graph style view offers a good perspective for viewing the timeline as a whole. The detail view is great for viewing the data if you want to see the day, month, and year it was accessed.

22. Much like the previous module we can view the extracted content. If you expand the “Results” tab, then “Extracted Content” you can view more content. In this file, we can see content that a web browser would generate.



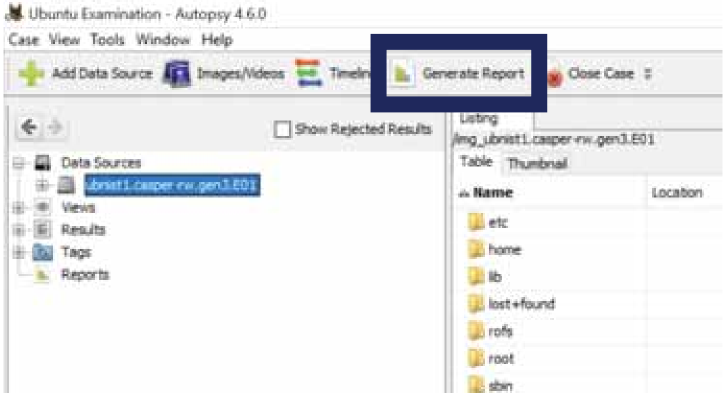
Artifact Type	Child Count
EXIF Metadata (32)	32
Extension Mismatch Detected (8)	8
Web Bookmarks (105)	105
Web Cookies (17)	17
Web Downloads (30)	30
Web History (246)	246
Web Search (6)	6

23. This content includes: EXIF Metadata, Extension Mismatches, Web Bookmarks, Web Cookies, Web Downloads, Web History, and Web Searches. If we look at web searches we see this. As you can see this person used the Firefox web browser, they searched “voice of America”, into Google and you can see the date they did this.

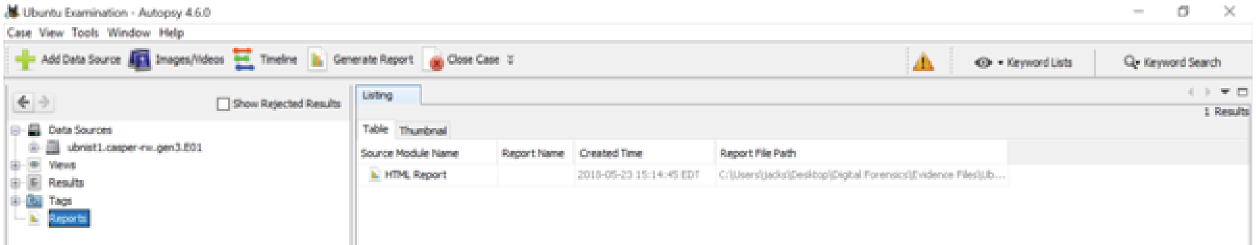


Type	Value	Source(s)
Domain	www.google.com	Recent Activity
Text	voice of america	Recent Activity
Program Name	FireFox	Recent Activity
Date Accessed	2008-12-30 00:13:36	Recent Activity
Source File Path	[illegible] places.sqlite	
Artifact ID	[illegible]	

24. By clicking the “Generate Report” button, you can view a report of the file you just looked through.



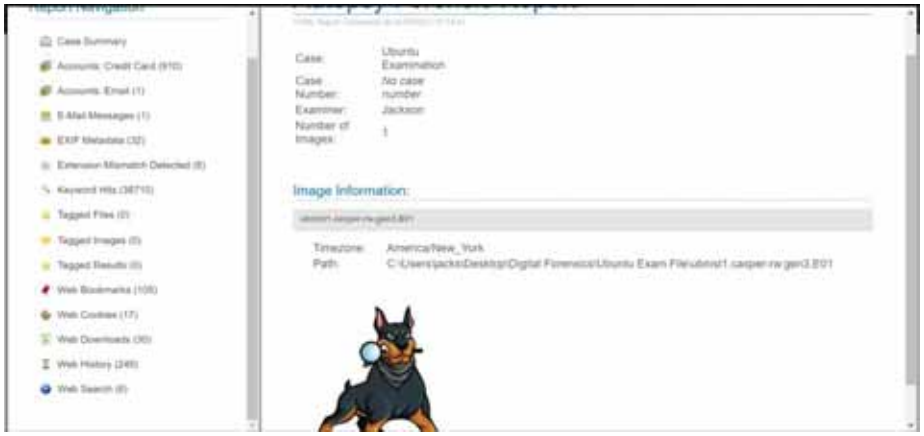
25. After clicking it you should see this…



Source Module Name	Report Name	Created Time	Report File Path
HTML Report		2018-05-23 15:14:45 EDT	C:\Users\jacks\Desktop\Digital Forensics\Evidence Files\Ub…

26. Keep the report format as HTML and then let it process. When it’s done you can find it under the reports button. After clicking on the report, it should open it up in an internet browser.

27. It should look like this



Case: Ubuntu Examination
Case Number: No case number
Examiner: Jackson
Number of Images: 1

Image Information:

ubnist1.casper-rw.gen3.E01

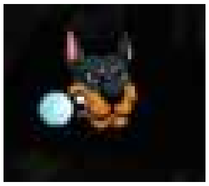
Timezone: America/New_York
Path: C:\Users\jacks\Desktop\Digital Forensics\Ubuntu Exam File\ubnist1.casper-rw.gen3.E01

28. If you want to learn more, Google is a great place to start. This is just the tip of the iceberg, there is so much more to learn and hopefully this developed interest in Digital Forensics. You can also find more information in a handout in this binder.

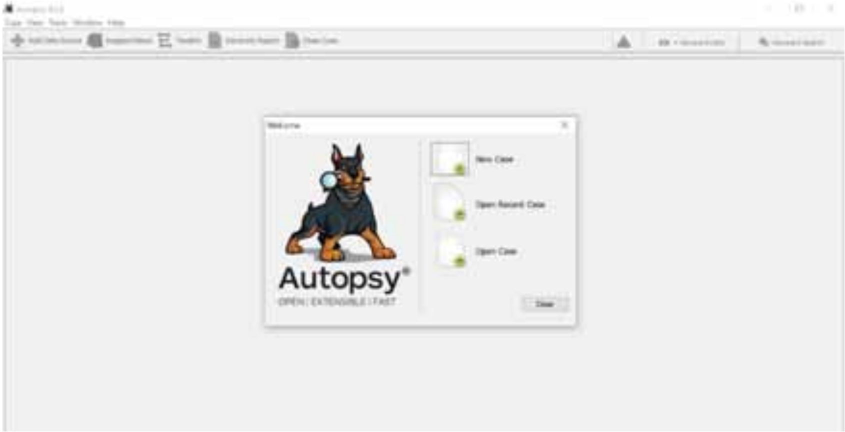
Introduction to Digital Forensics Investigation I

The first digital forensics module gives a brief history of digital forensics and how it progressed into the modern-day version. It also explains what digital forensics is, the role it plays in our society, and an understanding of the professionals who uses it. This module uses the free tool Autopsy to analyze an evidence file to teach students about digital forensics. It teaches students how to open a new case, upload an evidence file and start analyzing it. It also gives a brief explanation of the hexadecimal system and how it correlates with computer files. This includes the explanation of how numbers can be used to represent letters and symbols by using ASCII code. Moreover, it teaches students how to learn from the information that Autopsy extracts such as email addresses and how to view detailed information about them. This detailed analysis continues with phone numbers, URL's, credit card numbers, and banking identification numbers. This session also explains how Autopsy uses an advanced series of keyword searches to find these things, and the files that it extracts them from.

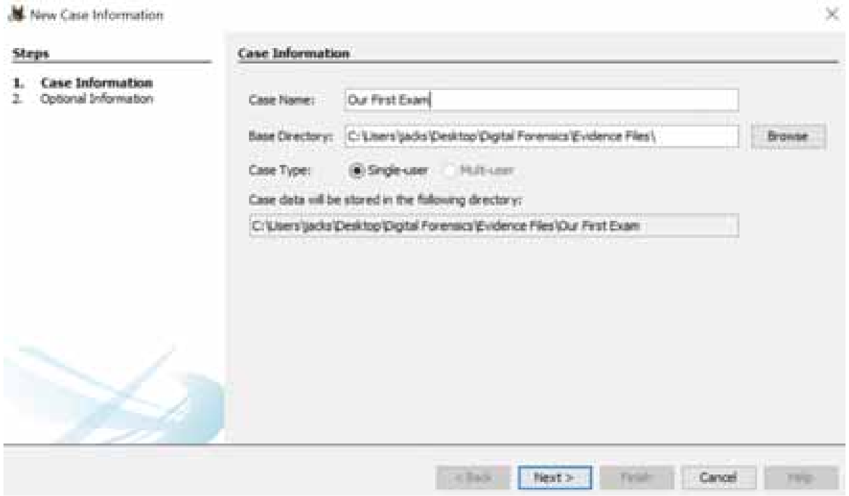
- In this module we will learn about digital forensics through a program named Autopsy. You can find a download link for it here, https://www.sleuthkit.org/autopsy/ . The version you will need will depend on the type of windows you are using at home. It comes in both a 32-bit and 64-bit version.
- So, what is digital forensics?
  - Digital forensics is a branch of forensic science that involves the recovery and investigation of materials found in digital devices. Digital forensics can be used to investigate networks, hard-drives, data bases, mobile devices, and many more things.
  - This is important because computers are everywhere and almost everyone uses them. Digital forensics is used to link criminals to crime by tracking their digital footprint (we all have one). It is used to help aid the criminal justice system by linking people to forms of cybercrime or can link them to a physical crime. It all depends on the crime being committed.
  - The police, various forms of the government (such as the FBI, DEA, NSA and others), and cyber security professionals use digital forensics in their day to day routines.
- Getting started
  - To get started with a digital forensic investigation we first need to launch Autopsy. There should be an icon on the desktop that looks like:



  - When it opens you should see this screen:



  - You are going to want to click on the button that says, “New Case”, you should then see this:



Case Information

Case Name: Our First Exam

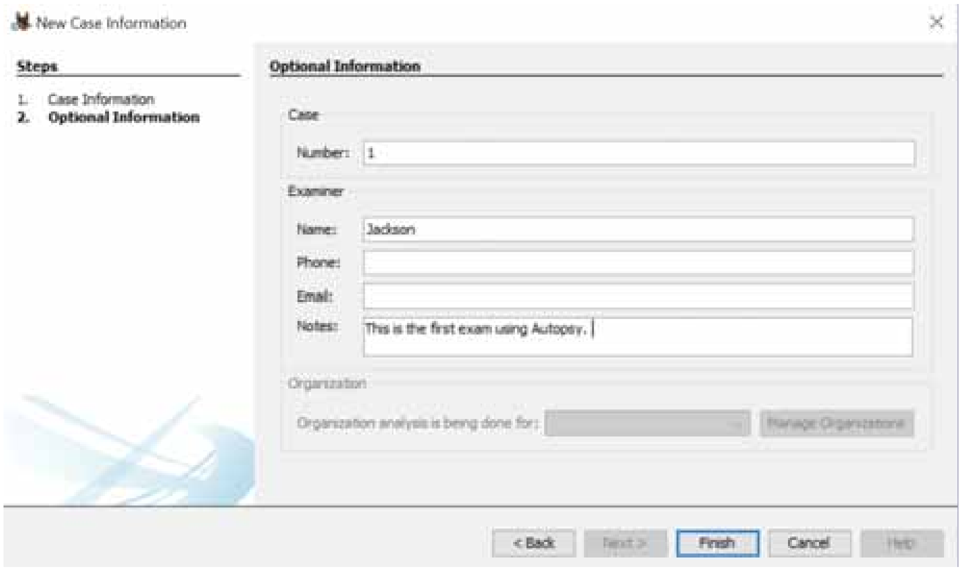
Base Directory: C:\Users\jacks\Desktop\Digital Forensics\Evidence Files\

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\jacks\Desktop\Digital Forensics\Evidence Files\Our First Exam

- o You should now name your case. Then you will want to select a folder to put the Autopsy file in, I recommend making a folder on your flash drive, so that way you can open it on any computer you want. Then click next.



Optional Information

Case

Number: 1

Examiner

Name: Jackson

Phone:

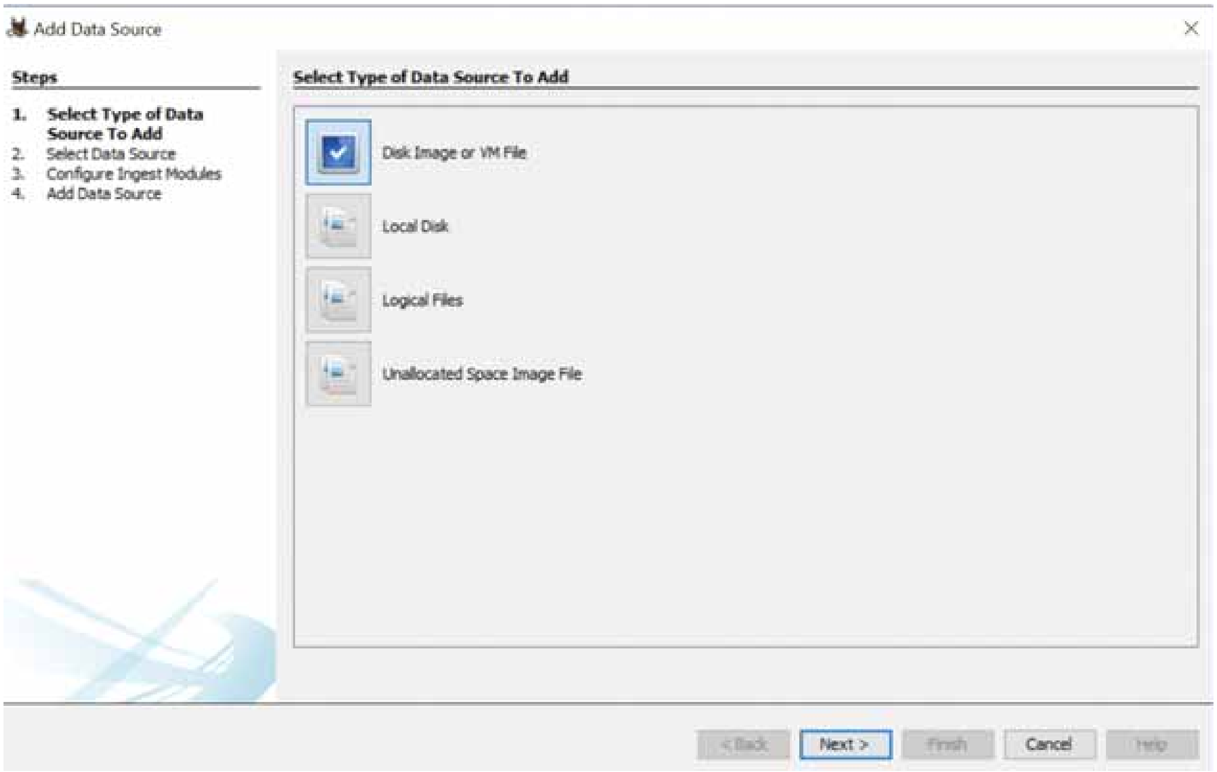
Email:

Notes: This is the first exam using Autopsy.

Organization

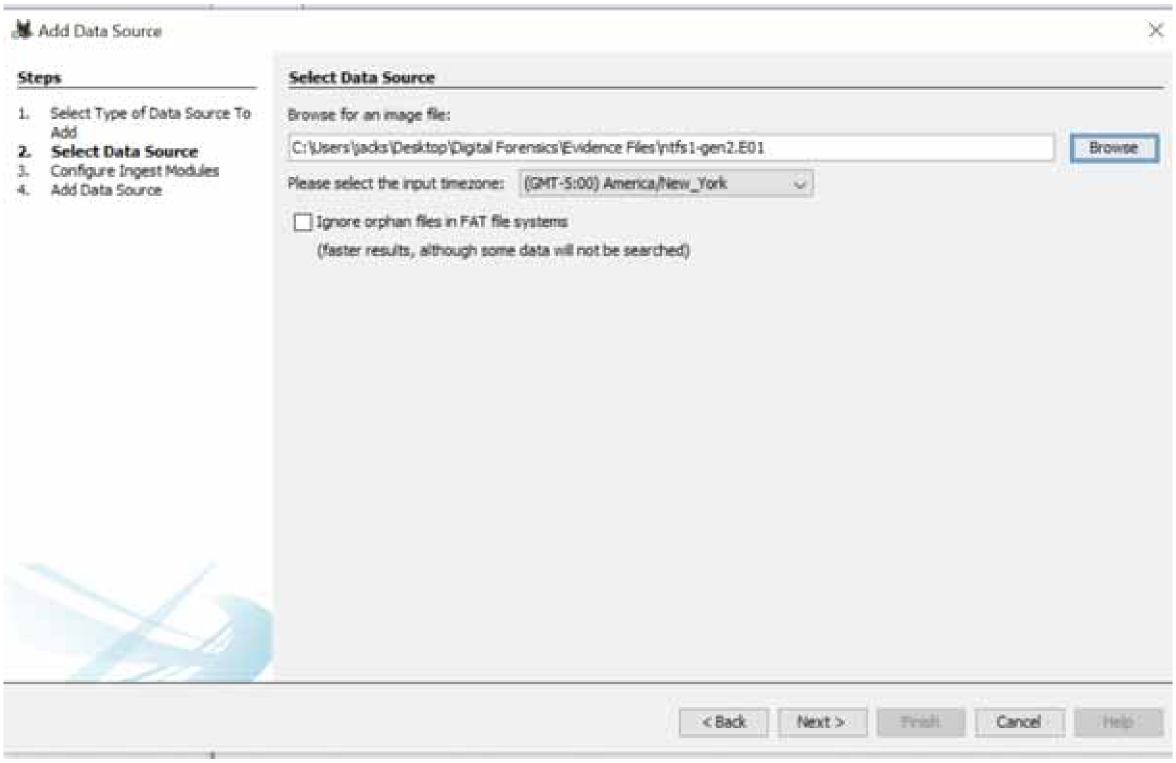
Organization analysis is being done for:

- o On this next screen enter in information such as the case number, examiner name, a phone number, email address, and any notes you want to include that may be useful to identify the case.


Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
Local Disk
Logical Files
Unallocated Space Image File
< Back
Next >
Finish
Cancel
Help

☑ Disk Image or VM File

- Next, we need to load in our evidence file. Start off by making sure "Disk Image or VM File" is selected, then click next.

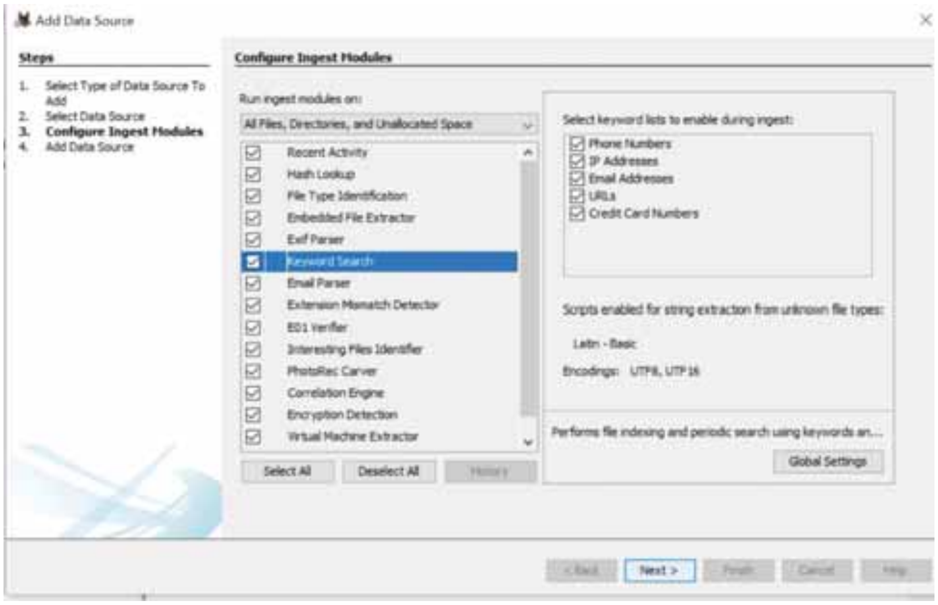


Browse for an image file: C:\Users\jacks\Desktop\Digital Forensics\Evidence Files\ntfs1-gen2.E01

Please select the input timezone: (GMT-5:00) America/New_York

□ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

- Click where it says "Browse", then navigate to the "Evidence Files" folder on your flash drive, and select the file titled "nfts-gen2.E01". Then click next.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ Correlation Engine
- ☑ Encryption Detection
- ☑ Virtual Machine Extractor

Select keyword lists to enable during ingest:

- ☑ Phone Numbers
- ☑ IP Addresses
- ☑ Email Addresses
- ☑ URLs
- ☑ Credit Card Numbers

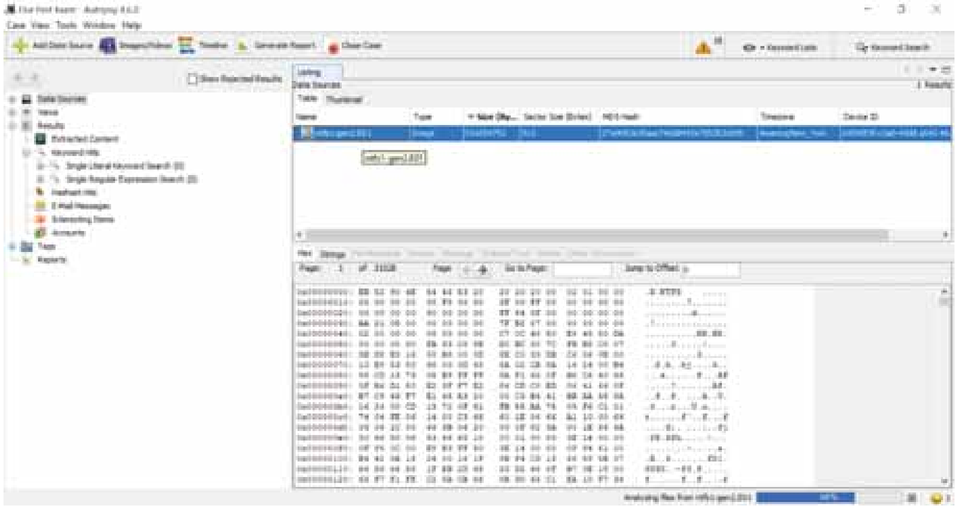
Scripts enabled for string extraction from unknown file types:

Latin - Basic

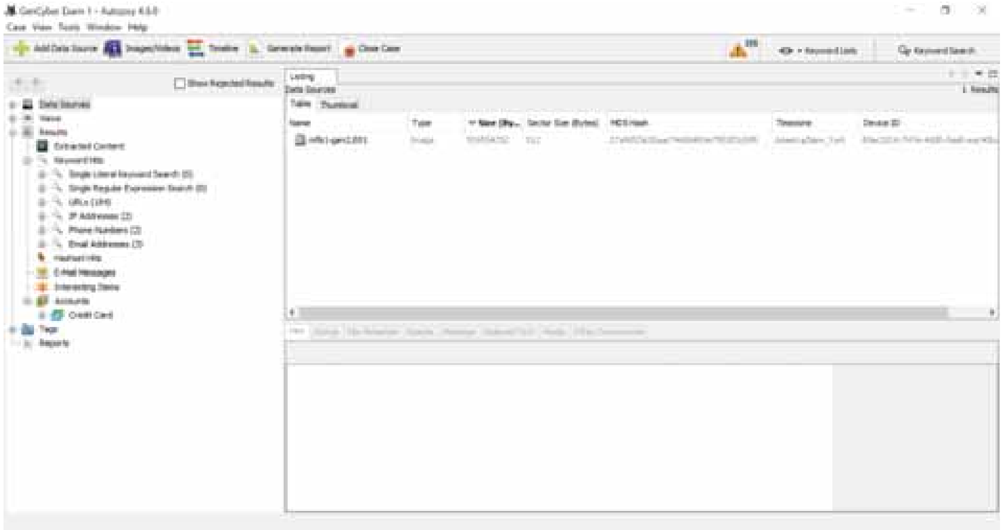
Encodings: UTF8, UTF16

Performs file indexing and periodic search using keywords an...

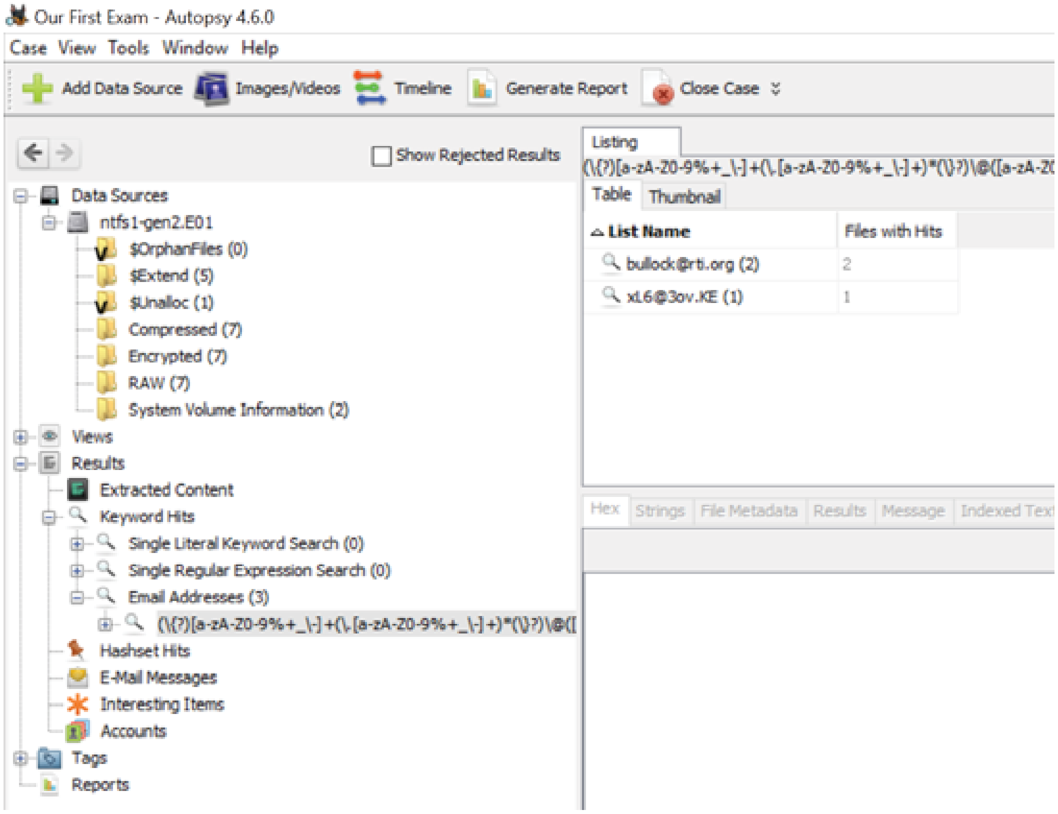
- On this screen leave everything clicked. You need to scroll down to where it says, “Keyword Search”. Make sure everything under this tab is selected, including Phone Numbers, IP Addresses, Email Addresses, URL’s, and Credit Card numbers. Then click “Next” and finally “Finish”



- When it loads, you should screen like this one above.
- In the window to the bottom right you will see a bunch of numbers and letters. Such as “00” or “AA” or combinations of the two like “D0”. These are hexadecimal numbers. It is a method used to turn letters, and symbols into numbers. So instead of using digits 0-9, it uses 0-9, and A-F. For a nice video explaining the binary and hexadecimal system check out, https://www.youtube.com/watch?v=aB__6e6WkFQ
- Using hexadecimal (or hex for short) we can encode letters and symbols. For example, the number 68 has a hex code of 44. In the ASCII encoding scheme, this represents the letter D.
- This is how computers store information, so it is important to understand how this works, if wish to further understand how data is stored and manipulated in computers.
- After the computer is done analyzing the evidence file the screen should look like this:

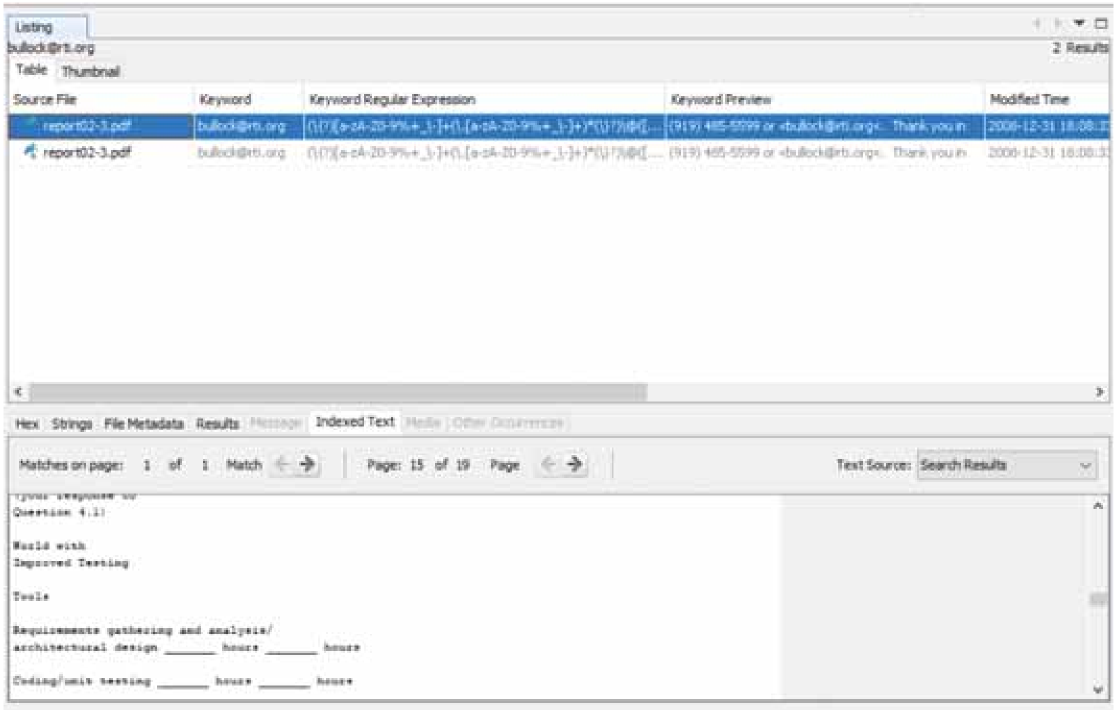


- Now let’s use autopsy to look at email addresses. Let’s first click on where it says Results, and then scroll down to where it says Email Addresses (3). Then click on the magnifying class to expand the tab.



List Name	Files with Hits
bullock@rti.org (2)	2
xL6@3ov.KE (1)	1

- If you click on the first email address bullock@rti.org, it shows two different files that appear.
- We see two files named “report02-3.pdf”. Then if you look you can also see a phone number in the Keyword Preview area.



Listing

bullock@rti.org

2 Results

Table Thumbnail

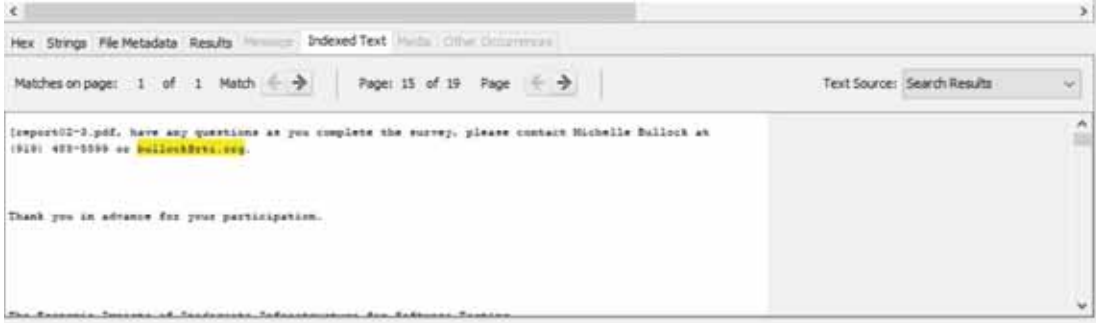
Source File	Keyword	Keyword Regular Expression	Keyword Preview	Modified Time
report02-3.pdf	bullock@rti.org	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)@([...	(919) 485-5599 or «bullock@rti.org«. Thank you in	2006-12-31 18:08:3
report02-3.pdf	bullock@rti.org	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)@([...	(919) 485-5599 or «bullock@rti.org«. Thank you in	2006-12-31 18:08:3

Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences

Matches on page: 1 of 1 Match Page: 15 of 19 Page Text Source: Search Results

```
(your response to
Question 4.1)

World with
Improved Testing

Tools

Requirements gathering and analysis/
architectural design ______ hours ______ hours

Coding/unit testing ______ hours ______ hours
```

- By moving the scroll bar over to the right, we can see some other interesting things. Like the time it was modified, accessed, and changed. Along with the file path.
- If we look in the box underneath the area we were just looking at we can view the email by moving the vertical scroll bar up and down.
- We can also view other information such as the hexadecimal values for the strings in the file, we can view just the strings with no blank lines in between the strings, the file metadata (Which is an informational panel describing the file), the results, and the indexed text which you are looking at now.

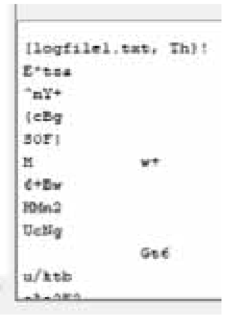


Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences

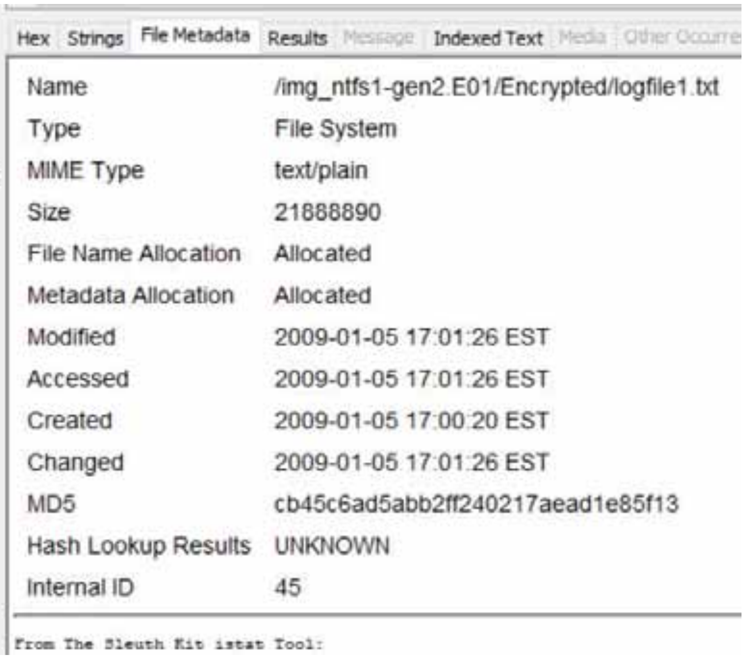
Matches on page: 1 of 1 Match Page: 15 of 19 Page Text Source: Search Results

```
(report02-3.pdf. have any questions as you complete the survey, please contact Michelle Bullock at
(919) 485-5599 or bullock@rti.org.


Thank you in advance for your participation.



The Economic Impacts of Inadequate Infrastructure for Software Testing
```

- We can view that data by clicking the corresponding tabs on the top left section of this window.
- Now lets click on the other email address. Labeled xL6@30v.ke. This address contains a file named “logfile1.txt”. If you view the contents of this email, you will see this.
- This looks like this because this file is encrypted.
- If we look at the File Meta-Data for this, we can learn something useful.
- As you can see in the name, this file belongs to the encrypted folder.
- A little bit further down, you can see the MD5 hash.



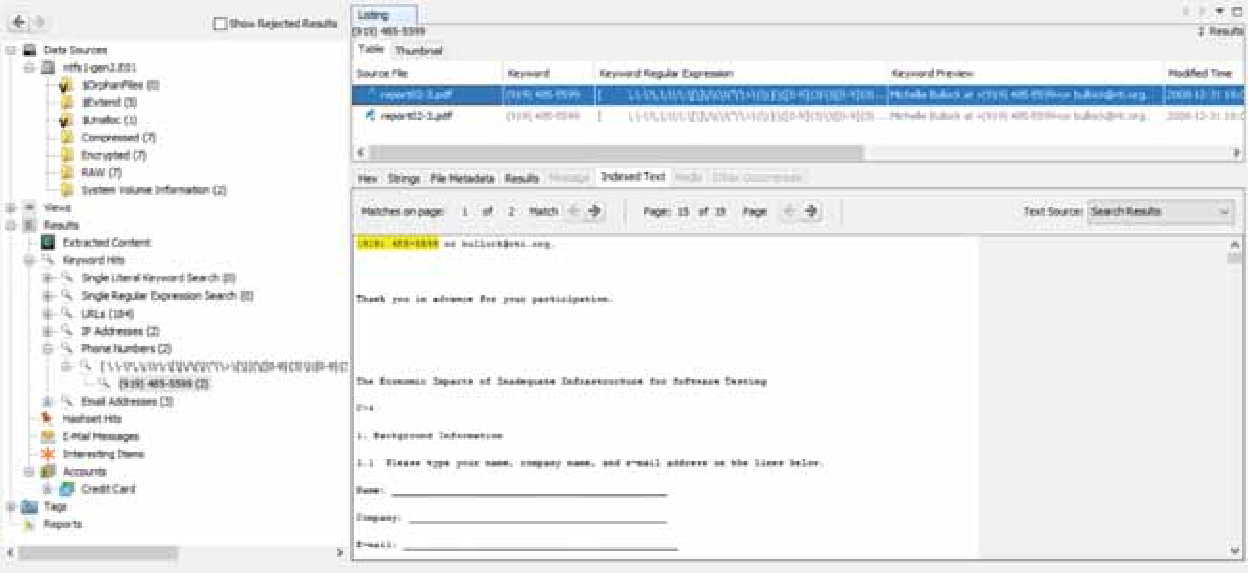
```
[logfile1.txt, Th}!
E*tsa
^mY+
{cBg
3OF|
M            w+
¢+Bw
M6n2
UcNg
             Gt€
u/ktb
```



Name	/img_ntfs1-gen2.E01/Encrypted/logfile1.txt
Type	File System
MIME Type	text/plain
Size	21888890
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2009-01-05 17:01:26 EST
Accessed	2009-01-05 17:01:26 EST
Created	2009-01-05 17:00:20 EST
Changed	2009-01-05 17:01:26 EST
MD5	cb45c6ad5abb2ff240217aead1e85f13
Hash Lookup Results	UNKNOWN
Internal ID	45

From The Sleuth Kit istat Tool:

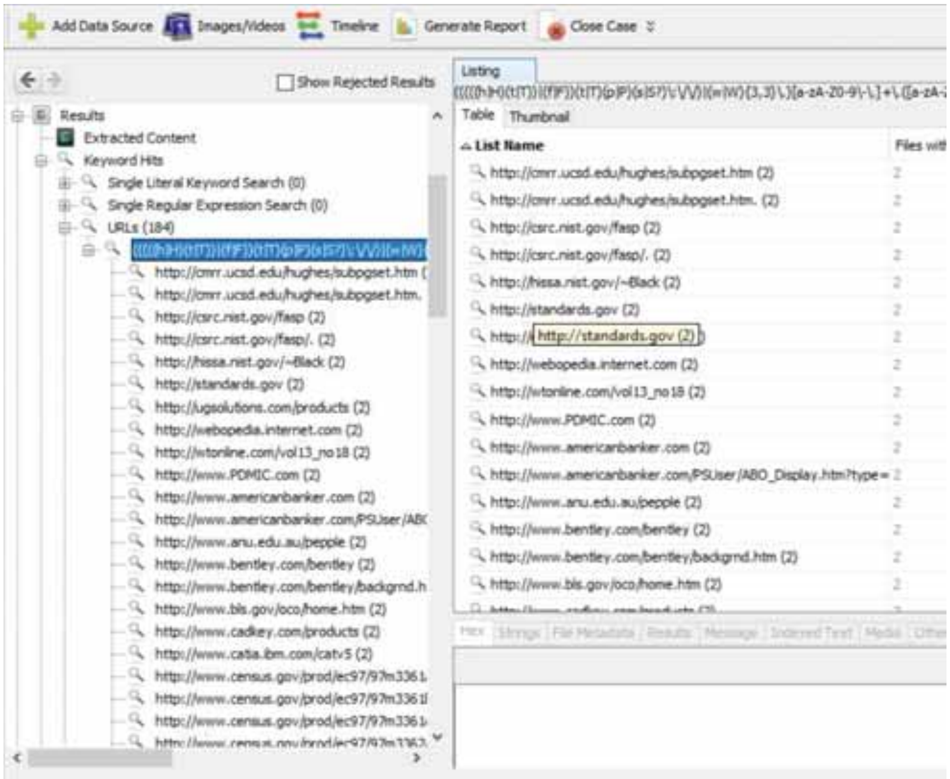
- o The MD5 hash is a way on encoding a whole file into a 32-bit hash. This is used to ensure that files are the same, this is particularly useful when two people are downloading the same value. Instead of having to download the whole file, they could download this. If the hashes match, this means that the file the people downloaded is the same.



Source File	Keyword	Keyword Regular Expression	Keyword Preview	Modified Time
report02-1.pdf	(919) 485-5599	[illegible]	Michelle Bulloch at +(919) 485-5599 or bulloch@rti.org.	2008-12-31 18:[illegible]
report02-1.pdf	(919) 485-5599	[illegible]	Michelle Bulloch at +(919) 485-5599 or bulloch@rti.org.	2008-12-31 18:[illegible]

```
(919) 485-5599 or bulloch@rti.org.


Thank you in advance for your participation.



The Economic Impacts of Inadequate Infrastructure for Software Testing

2-a

1. Background Information

1.1  Please type your name, company name, and e-mail address on the lines below.

Name: ______________________________

Company: ___________________________

E-mail: ____________________________
```

- o If you click on where it says phone numbers, then expand the directory underneath that tab you can see the files that we found in the email section.
- o These phone numbers match what we previously found.
- o What this tells us is that Autopsy, scans the files search by search.



□ Show Rejected Results

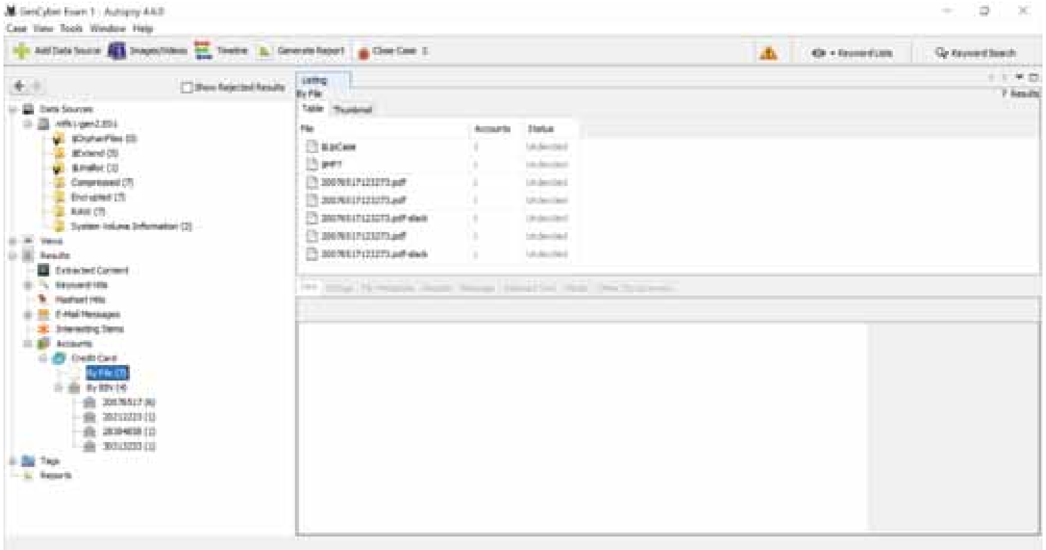
- Results
  - Extracted Content
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - URLs (184)
      - ((((h|H)((t|T))|(f|F))(t|T)(p|P)(s|S?)\:\/\/)|(w|W)
        - http://cmrr.ucsd.edu/hughes/subpgset.htm (
        - http://cmrr.ucsd.edu/hughes/subpgset.htm.
        - http://csrc.nist.gov/fasp (2)
        - http://csrc.nist.gov/fasp/. (2)
        - http://hissa.nist.gov/~Black (2)
        - http://standards.gov (2)
        - http://ugsolutions.com/products (2)
        - http://webopedia.internet.com (2)
        - http://wtonline.com/vol13_no18 (2)
        - http://www.PDMIC.com (2)
        - http://www.americanbanker.com (2)
        - http://www.americanbanker.com/PSUser/ABC
        - http://www.anu.edu.au/pepple (2)
        - http://www.bentley.com/bentley (2)
        - http://www.bentley.com/bentley/backgrnd.h
        - http://www.bls.gov/oco/home.htm (2)
        - http://www.cadkey.com/products (2)
        - http://www.catia.ibm.com/catv5 (2)
        - http://www.census.gov/prod/ec97/97m3361
        - http://www.census.gov/prod/ec97/97m3361
        - http://www.census.gov/prod/ec97/97m3361
        - http://www.census.gov/prod/ec97/97m3362

((((h|H)((t|T))|(f|F))(t|T)(p|P)(s|S?)\:\/\/)|(w|W){3,3}\.)[a-zA-Z0-9\-\.]+\.([a-zA-

Table Thumbnail

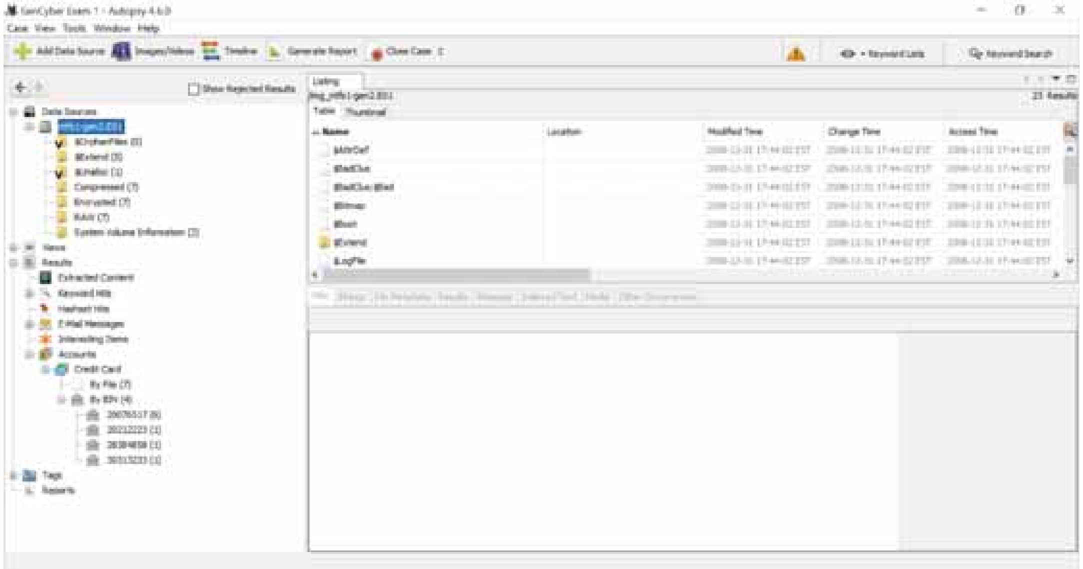
List Name	Files wit
http://cmrr.ucsd.edu/hughes/subpgset.htm (2)	2
http://cmrr.ucsd.edu/hughes/subpgset.htm. (2)	2
http://csrc.nist.gov/fasp (2)	2
http://csrc.nist.gov/fasp/. (2)	2
http://hissa.nist.gov/~Black (2)	2
http://standards.gov (2)	2
http:// http://standards.gov (2)	2
http://webopedia.internet.com (2)	2
http://wtonline.com/vol13_no18 (2)	2
http://www.PDMIC.com (2)	2
http://www.americanbanker.com (2)	2
http://www.americanbanker.com/PSUser/ABO_Display.htm?type=	2
http://www.anu.edu.au/pepple (2)	2
http://www.bentley.com/bentley (2)	2
http://www.bentley.com/bentley/backgrnd.htm (2)	2
http://www.bls.gov/oco/home.htm (2)	2

- Next lets take a look at URL's.
- Click on where it says URL's and expand the directories.
- There is 184 results that pop up. Take a few minutes and look through them and see what you can find.
- You may notice that many of the file names that the URL's are found in match.
- This is because many of the files are reports, and have references listed somewhere in the file.
- This goes to show that though Autopsy does a thorough search through the files, but it makes it appear as if there is more data than their actually is.
- Although there is 184 URL's listed, there is not that many files in our system.



- In the file directory to the left-hand side of the screen there is a tab labeled "Accounts".

- Expand the directory underneath it to reveal something titled "Credit Card", then expand it. You can then view the information by card, or BIN (Banking Identification Number)
- This allows us to view credit card numbers and bins.



- If you want to view every file available in the system click on "nfts-gen2.E01" in the top left of the directory. This shows every file available for examination
- Take some time and see what else you can find.

- Conclusion
    - We learned how to open Autopsy, create a new case, and load in an evidence file. We also examined some introductory data that Autopsy was able to find.
    - Autopsy has many different tools for data analyzation. If you would like to learn more there are several tutorials on the internet. There are also free evidence files for analyzation that can be found online.

- We will continue our analysis in the next module.

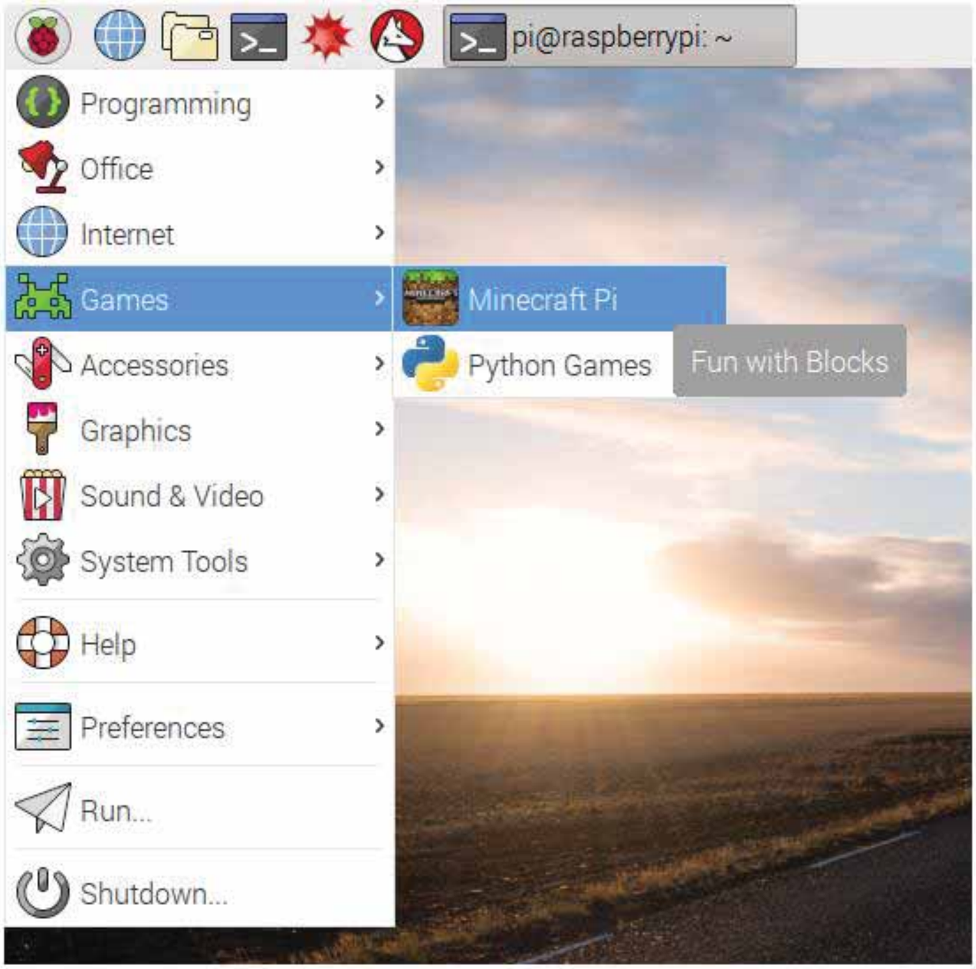
Module 1: Cybersecurity Basics (programming / Raspberry PI)

The main goal of this module is to understand importance of computer programming and how it relates to Cybersecurity. The module will presents interesting hands-on exercises in which participants will setup, run and use a Raspberry Pi. We will first understand that a Raspberry Pi is a small computer that runs an operating system installer called NOOBS (New Out Of Box Software). Each camper will be instructed on what the Pi is, the parts of it, and the first time setup. During this time, the chosen operating system will be completing the first boot up. Since this takes some minutes, each camper will be instructed on the basics of computer science. This will include an explanation as to what hardware and software is, what a computer needs to run, and basic types of operating systems. Once the installation is completed, each camper will be given a tour of his/her Raspberry Pi. This will include navigating the main menu of the device, creating a text file on the main screen, and learning basic Linux commands in the terminal and syntax. Finally, the campers will be instructed to launch "Minecraft"; they will be shown where it is in the menu. They will be given a small explanation as to what Minecraft is and what we will be doing with the program. Next, they will be instructed (and shown) how to execute the "Python 3 (IDLE)" program. They will use this to modify and augment the current game of Minecraft they are in. To correctly proceed, each camper must have an instance of Minecraft running as well as a "world" created that they are currently using. From here, each camper will be instructed as to what Python is and what scripts will be used to modify Minecraft in real time. Once all scripts have been written the campers shall proceed to the next area for the next activity.

Minecraft Activity Instructions

Section 1: Running Minecraft

1) Run Minecraft and create a new world
   - To run Minecraft open it from the desktop menu
   - To create a new world, click **Start Game** then **Create new**. The new world will begin to generate



2) The movement controls are similar to the PC edition of Minecraft
   - The WASD keys are movement. E is inventory. SPACEBAR is jump. To fly press the SPACEBAR twice. Do the same if flying to fall. The Esc key is used to pause the game. The Tab key is used to focus on the mouse.

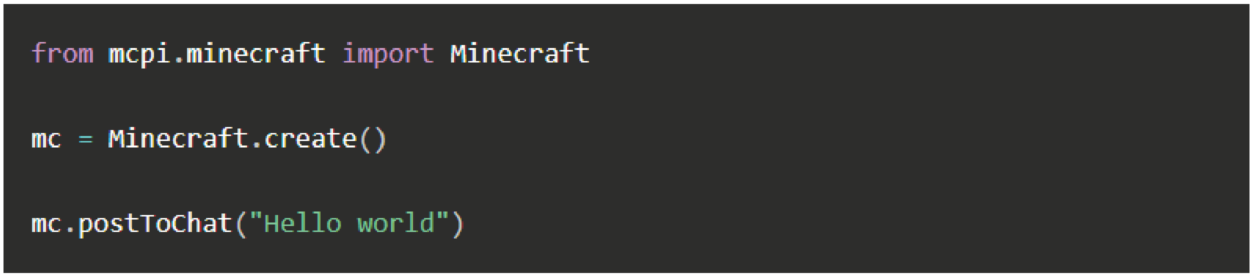
Section 2: Basic Python Commands

3) You will have to create an instance of the Python 3(IDLE) from the Raspberry Pi menu. Click the raspberry, click Programming, then Python 3(IDLE)

4) If you have not, make sure you have an instance of Minecraft running and make sure you are the world you created. This will not work otherwise.

5) Make sure to hit the ENTER key after each line

6) Here is the first command that we will run. It will print a “Hello world” into the chat of the current game



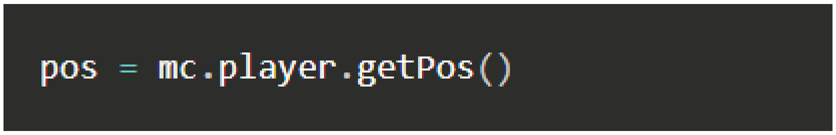
```
from mcpi.minecraft import Minecraft

mc = Minecraft.create()

mc.postToChat("Hello world")
```

7) Enter the previous into the Python 3 (IDLE) window.

8) After each line, hit enter. Once the final line is written, the “Hello world” message will appear in your game

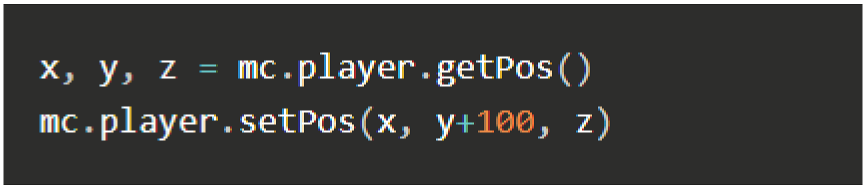
9) Next we will find the current position you are at. To do this type the following statement into the Python window

10) Next type pos into the same window and you will get a message in blue giving coordinates. These are your current coordinates. If you move you will need to rewrite the same lines of code to get your new current position



```
pos = mc.player.getPos()
```

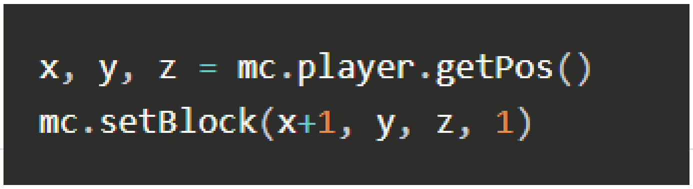
11) Next, lets teleport to a new location. Type the following into the Python window



```
x, y, z = mc.player.getPos()
mc.player.setPos(x, y+100, z)
```

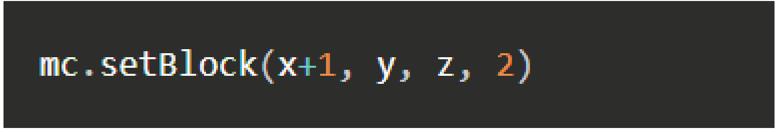
12) Notice what happen? You got teleported 100 blocks into the air. Pretty cool, right? We are only just beginning and scratching the surface of what you can do with Python and this Minecraft

13) For the next code, we will be placing a simple stone block. To preface the code, each block in Minecraft is assigned a number. Stone in this version is 1. The following code will complete this process. NOTE: if you do not see the block appear in front of you, turn around and it should be behind or beside you.



```
x, y, z = mc.player.getPos()
mc.setBlock(x+1, y, z, 1)
```

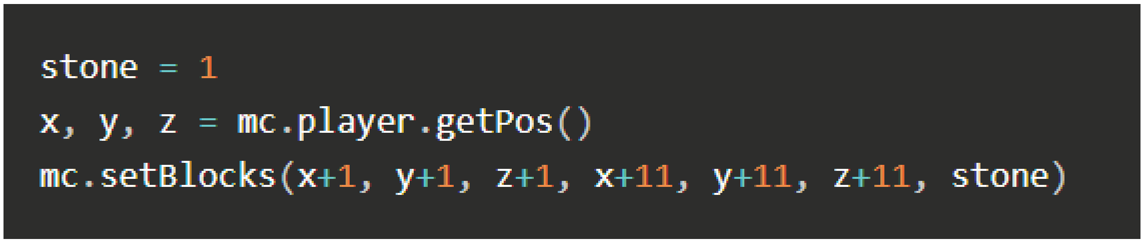
14) Now let’s be a magician and change this stone block to a dirt block without destroying it. The following code will make us amateur magicians. Make sure you are looking at the stone block you just placed.



```
mc.setBlock(x+1, y, z, 2)
```

15) And abracadabra! You have just transformed solid stone into dirt! You can look any block and have it turn into dirt! This is a great trick for parties.

16) Next let’s create a floating cube of solid stone. To do this, type the following code



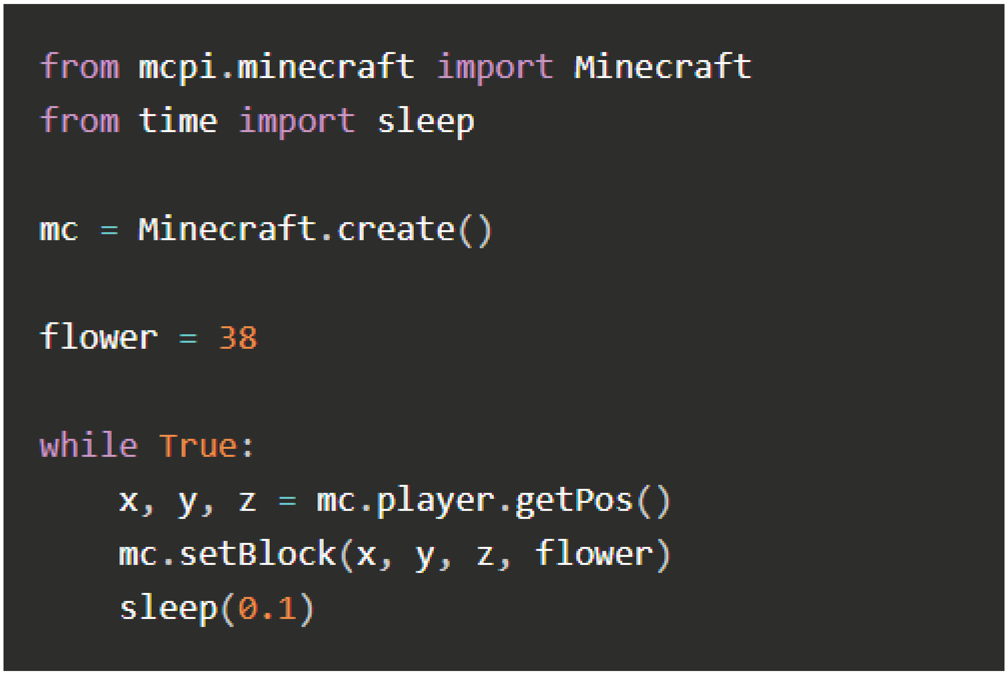
```
stone = 1
x, y, z = mc.player.getPos()
mc.setBlocks(x+1, y+1, z+1, x+11, y+11, z+11, stone)
```

17) Awesome right? This can be done with any block id and any (almost) any size. Just remember, the bigger you make it, the longer it will take to render the cube.

Well, that was everything for the basic commands. Let’s move on to more advanced scripts.

Section 3: Python Logic

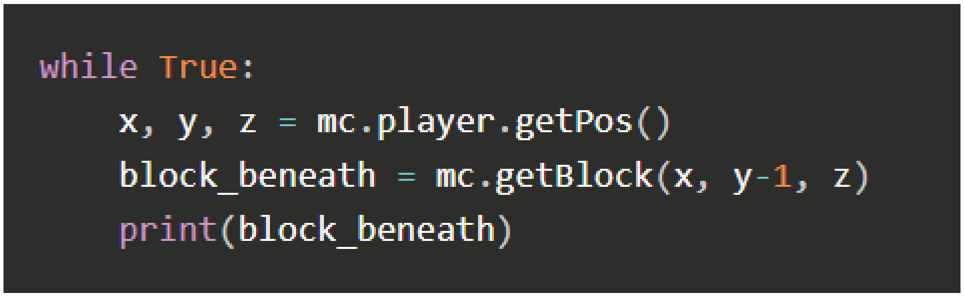
18) Exit out of the Python 3 (IDLE) window and open a new one up. For this first code, I need to explain what we will be creating. For this part, we will have a blue flower drop every time we walk. We will be using our current location to drop a flower on the ground (or even the air). We will be using loops and the “while” loop in particular. This loop will execute certain code if a condition is true (or sometime false). The code works by saying if you move it’ll drop a flower. Enough explanation, let’s write the code and see it in action!



```
from mcpi.minecraft import Minecraft
from time import sleep

mc = Minecraft.create()

flower = 38

while True:
    x, y, z = mc.player.getPos()
    mc.setBlock(x, y, z, flower)
    sleep(0.1)
```

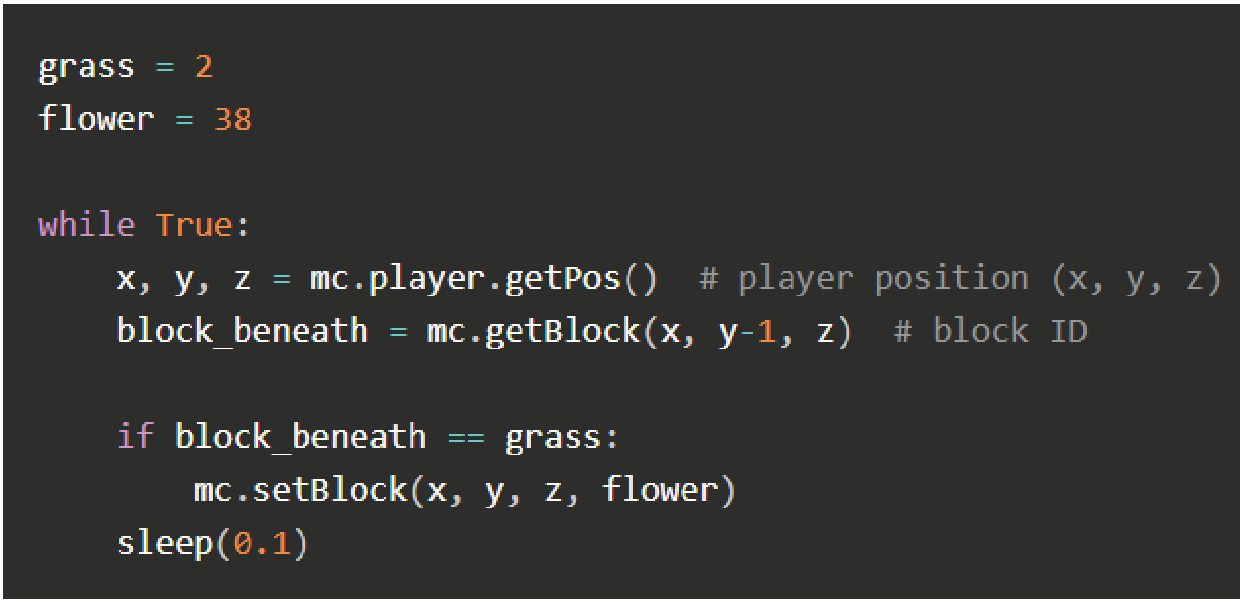
19) Awesome right! Although cool, I ask you to press **CTRL + C** keys on your keyboard in the Python window. This will end the script from running. The sleep(0.1) is the rate of flowers being dropped. You can change this number to see more or less flowers being dropped. Just remember to retype for it to take effect

20) What if we want to see the block we are standing on? The next code fragment will grant this wish. Inside of the while True: is the next part goes. Exclude the first while True: at the top of the code



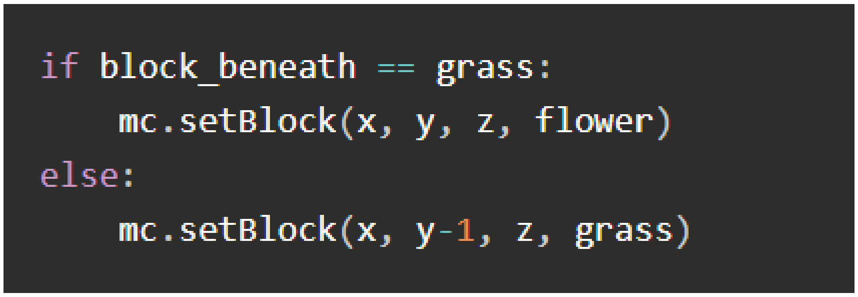
```
while True:
    x, y, z = mc.player.getPos()
    block_beneath = mc.getBlock(x, y-1, z)
    print(block_beneath)
```

21) For the next part, we will be modifying the previous code. What are we modifying it to do? Thank you for asking. We will be adding a thing called an **if** statement. Why are we doing this? Because it is very cool. Anyway, the way the if statement will work is if we are standing on a grass block we will plant a flower. If it is not a grass block the flower will not be planted. Here is the code



```
grass = 2
flower = 38

while True:
    x, y, z = mc.player.getPos()  # player position (x, y, z)
    block_beneath = mc.getBlock(x, y-1, z)  # block ID

    if block_beneath == grass:
        mc.setBlock(x, y, z, flower)
    sleep(0.1)
```

22) This is nice. We made a little garden. Now let’s defy physics. For this last activity, we will be modifying the previous code (yes again). This time will be adding an **else** statement to the if statement. The logic behind it is again, if we are on a dirt block we will plant a flower. Then if we are not a dirt block, the block below us will become a dirt block. Just a note, if you fly random dirt blocks will begin to appear behind you. This is where the physics are being defied. Code time!



```
if block_beneath == grass:
    mc.setBlock(x, y, z, flower)
else:
    mc.setBlock(x, y-1, z, grass)
```

23) If you walk over the grass you just created, a flower will be planted. We can make a sky garden now.

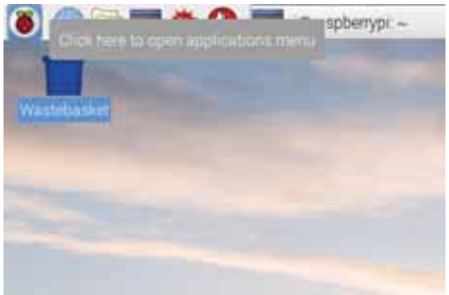
This has been the Minecraft Activity for the Raspberry Pi. Like I said before, these are just some of the things you can do with Minecraft and Python. I encourage all of you to modify the code I have given you but to also write your own and see what all you can do with the Minecraft! I hope you all enjoyed doing this as much as I enjoyed teaching it to you!

Module 2: Cybersecurity and the Raspberry Pi

The main goal of this module is for the campers to understand the some basic concepts of cybersecurity through the Raspberry Pi. To accomplish this, the campers will learn the basic definition of cybersecurity, learn about hacking (and hackers), learn a few basic Linux commands and write and test an encryption program all on the Raspberry Pi. The campers will learn what exactly cybersecurity is and how it applies to the world. Along with this, they will learn the difference between white-hat, black-hat and grey-hat hackers. From this, the explanation of hacking will commence. The definition of hacking as well as examples of ethical and non-ethical hacking will also be described. One of the examples of hacking is penetration testing, which will be explained to the campers. This will lead into why Raspberry Pi's can be utilized for cybersecurity tasks. From here, the basic Linux commands will be demonstrated on the Raspberry Pi's. Next, the basics of encryption will be explored. Once the concept is understood, Caesar Cipher will be explained and the activity for the campers will begin. They will write a program that will utilize the Caesar Cipher and practice with encryption and cryptography on the Raspberry Pi. Once the program is written, they will add a decryption method to decrypt several encrypted messages and words. Finally, the campers will participate in a Kahoot that will recap the basics of cybersecurity, Raspberry Pi and the basics of computer science.

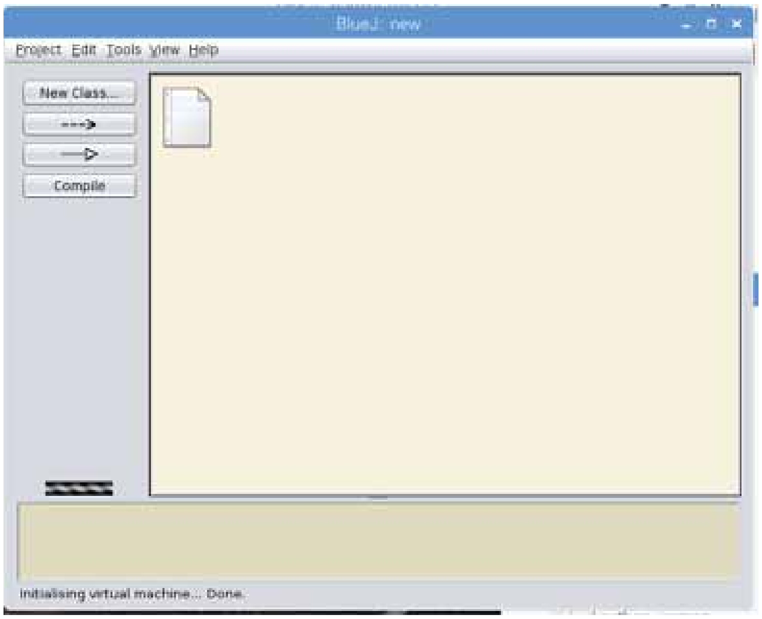
Encryption Activity Instructions (Module 2)

1) Navigate to the main menu and click Programming
    - You will want to find the one that is called BlueJ



2) Next you will need to execute the program. Click on it and the following window will appear

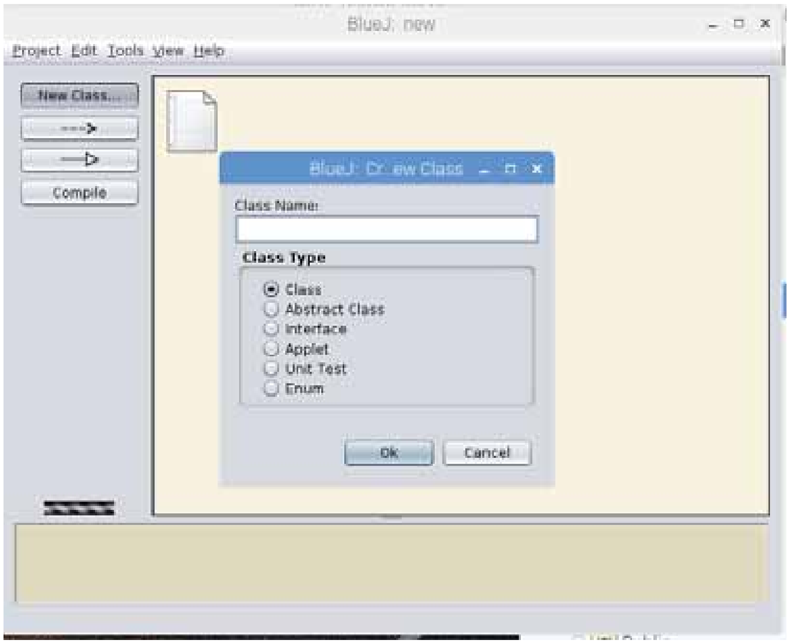
3) Next you will want to create a project. To do this click new on the top left of the window and create a folder. After you create it, the following window will appear. New will be the project name you created



Initialising virtual machine... Done.

4) Next you will need to create a class. To do this, click the new class button

- Name the class CaesarCipher and keep the class type as Class

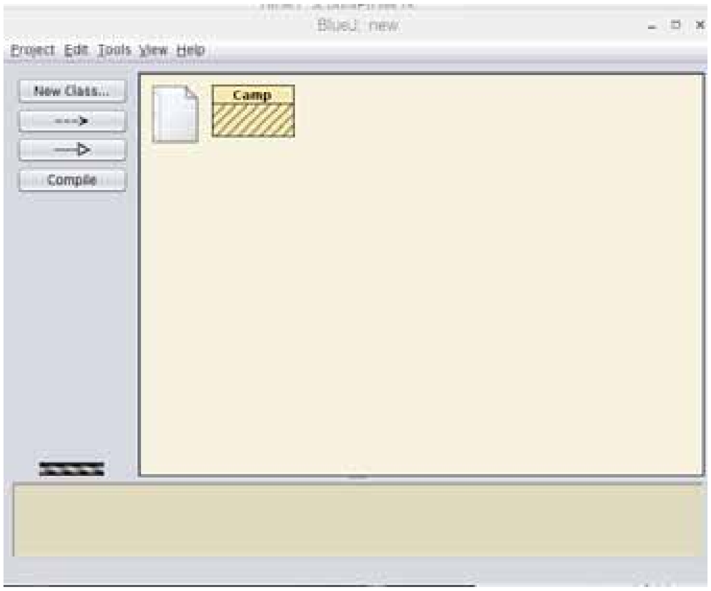


Class Name:

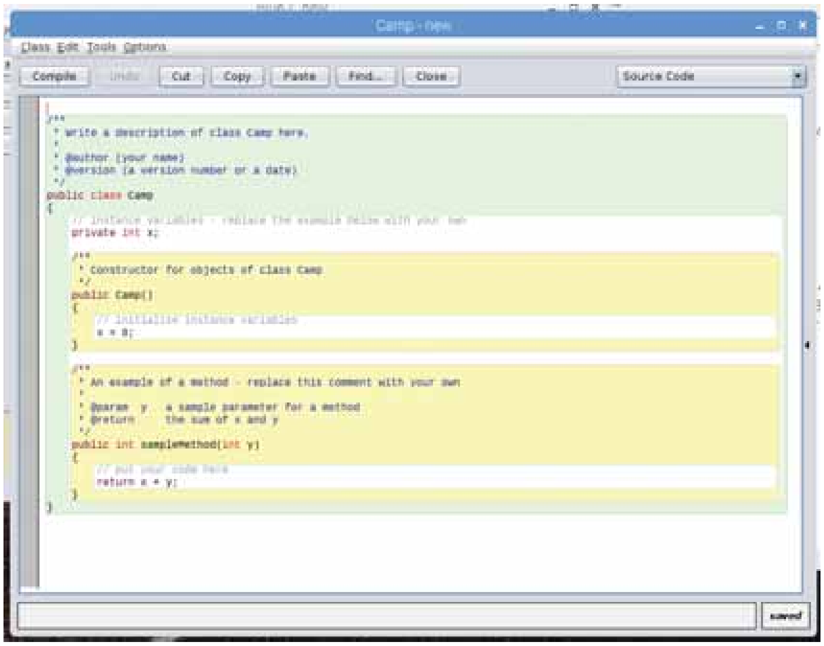
Class Type

● Class
○ Abstract Class
○ Interface
○ Applet
○ Unit Test
○ Enum

5) The following page will appear. It shall say CaesarCipher instead of Camp



6) Click on CaesarCipher and the following default code will be written



```
/**
 * Write a description of class Camp here.
 *
 * @author (your name)
 * @version (a version number or a date)
 */
public class Camp
{
    // instance variables - replace the example below with your own
    private int x;

    /**
     * Constructor for objects of class Camp
     */
    public Camp()
    {
        // initialise instance variables
        x = 0;
    }

    /**
     * An example of a method - replace this comment with your own
     *
     * @param  y   a sample parameter for a method
     * @return     the sum of x and y
     */
    public int sampleMethod(int y)
    {
        // put your code here
        return x + y;
    }
}
```

7) The code for the cipher will be given below. NOTE: this is not the exact code I will have you write

```
import java.util.Scanner;

public class CaesarCipher {
        static String code;
        static int offset;
        static String decrypt = "ebe";

        public static String encrypt(String text, int offset) {
                StringBuffer result = new StringBuffer();
                for (int i = 0; i < text.length(); i++) {
                        if (Character.isUpperCase(text.charAt(i))) { // tests for upper case
                                char character = (char) (((int) text.charAt(i) + offset - 65) % 26 + 65);
                                result.append(character);
                        } else { // tests for lower case
                                char character = (char) (((int) text.charAt(i) + offset - 97) % 26 + 97);
                                result.append(character);
                        }
                }
                return result.toString();
        }

        public static String encode(String text, int offset) {
                StringBuilder encoded = new StringBuilder();
                for (char i : text.toCharArray()) {
                        if (Character.isLetter(i)) {
                                if (Character.isUpperCase(i)) {
                                        encoded.append((char) ('A' + (i - 'A' + offset) % 26));
                                } else {
                                        encoded.append((char) ('a' + (i - 'a' + offset) % 26));
                                }
                        } else {
                                encoded.append(i);
                        }
                }
                return encoded.toString();
        }

        public static String decrypt(String text, int offset) {
                return encrypt(text, 26 - offset);
        }

        public static String decode(String text, int offset) {
                return encode(text, 26 - offset);
        }
```

8) I will now instruct you as to how to use the code
    - To run the code you will need to compile, which is at the top left of the code screen
    - After this, open an instance of the terminal
9) From here navigate to the folder where you created the java project
    - The navigation should be cd [location]. This may be different for everyone. I will help you find the location of the file
10) To run the project, you will need the following command
    - javac [project name]
    - java [project name]
    - After the “java [project name]” line the program will run
    - This can be done in Windows machines as well

Title: New Wireless Security and Emergency Communications Opportunities for you

Abstract:

Wireless knowledge is needed today since this is a fundamental skill, along with programming and embedded hardware, to design Internet-of-Things (IoT) products. Examples of IoT products include remote internet-based cameras, remote temperature house control, and any monitoring device, or sensor, with a WiFi links. The Internet of Things (IoT) is a rapidly growing field, and this requires students and engineers with wireless expertise. Joe discusses and demos cool wireless programming tools and wireless security through live software-defined radio visual demos of aircraft digital and voice communications. Joe will also show how students can gain valuable disaster and emergency wireless communication knowledge through an Amateur Radio FCC License. In the recent Puerto Rican and Houston Hurricane disasters, licensed Amateur Radio operators were the FIRST to establish communications for the police, firefighters, the Red Cross, and other hurricane disaster victims. In fact, after 175 mph hurricane cat 4 & 5 winds quickly destroyed cellphone and even police communications in Puerto Rico (hurricane Maria), amateur radio operators as young at 15 rode with the police providing emergency communications!

BIO:

Joseph Jesson has 25+ years in the embedded wireless system, Telemetry, Telematics, M2M, and the Internet of things (IoT) space. Joe is currently the Chair of the Princeton IEEE Life Group and CEO of RFSigint, a wireless & IoT patent/IP portfolio analystics company. Joe has held the Chief Technology Officer (CTO) position at General Electric, where he was awarded the GE Edison Award in 2007. Currently, he is Adjunct Professor at The College of New Jersey (since 2013) and teaches Digital Design, Circuit and Electronics Lab, Embedded Systems and Embedded Labs, Control Theory and Controls

Lab, etc. Joe has held CTO positions at Able Devices, Assurenet, Software and Systems Architecture positions at Amoco/ BP, Product Manager at OAK Technology, and staff engineering positions at Motorola and The University of Chicago. Joe has a Master's degree from DePaul University in Chicago and is currently working on his PhD dissertation at NJCU in Jersey City, NJ.