# ­GCU Network Forensics Demo

## Prep

* Clean VM’s desktop & documents @   
  http://174.78.93.110:48046/guacamole/#/  
  http://174.78.93.110:48047/guacamole/#/  
  http://174.78.93.110:48048/guacamole/#/
* Check what time GCU Live is due on Zoom per demo.
* kali# / lopesup root / toor
* CTL-ALT-SHIFT to logout each / CTL-ALT for keyboard issues
* kali35 or 36 usually used for demonstration.
* Zoom setup with multiple tabs: Live Map, demo machine, guacamole login screens. Record Zoom Sessions.
* guacadmin / thunderlopes to see remote screens per server.
* VMware computer ready to go in case of VM troubleshooting.
* **UAC phone number to connect with.** How many computers are students using? Help log on if needed.
* CTL-+ for zooming in various areas.
* **Everything toward a career; GCU can help get you there!**

## Introduction

* Hello everyone! Glad you could join us today. My name is Joe Urbz and I am a Cybersecurity Specialist at GCU. I work with an awesome team to find ways to share cybersecurity to students like yourself.

* I have been a long-time (Career Technical) CTE teacher in Southern California and a short time in Arizona (Deer Sandra Day O’Connor HS in North Phoenix with the Deer Valley USD).
* I am certified in multiple areas of IT and Media; A+, Network+ and Security+. My degree is in Psychology, which has helped me understand behaviors; in the classroom and with technology.
* I have assisted law enforcement with tracing stolen credit-cards as they were being used. I could demonstrate to the Sheriff, at the time, where the address was where the card was being used almost in real-time.
* Why did I get into the Cybersecurity industry?
* I’ve learned the hard way in how easy it is to be hacked, with family and friends having all of their technology and networks wide open for the sake of convenience and default settings. I have mastered how to communicate to people how to help themselves with these every day issues; to empower them to take better care of their tech as they enjoy having it.

## Needs for Cybersecurity Jobs

* See this map? This is a representation of live hacks going around the world.
* There is such a need for cybersecurity professionals. In Arizona alone, there are **around** 20,000 jobs available and with a bachelor’s degree, potential entry level jobs in Pen-Testing (red-team) and Cybersecurity Analyst (blue-team) are salaries between $70-$90,000.

## So Why GCU?

* Significant Hands-on experience within the Cyber/IT programs.
* Bachelors and Masters degrees for Cybersecurity.
* Industry driven curriculum. GCU partners up with industry leaders that tell GCU what skills are needed and wanted.
* No tuition raises in 14 years; means less debt!
* Great campus; rated very highly. Wonderful community who are friendly and helpful across campus.
* Any questions I can answer?

## Introduction to today’s Demo

* Today, we are going to explore Digital Forensics.
* **What IS Digital Forensics? The science of identifying, preserving, recovering, analyzing and presenting facts about digital evidence found on computers or digital storage media devices.**
* Do you remember any of the CSI style TV shows?
* Today’s exercise is one that the CIA uses for real, live training. So, if you could do this work, you could work for the CIA!

## Students Logging in via the UAC and Teacher

* Which screen are you on? The Apache Guacamole or the Kali logon screen?
* The logon for Kali is **root** and the password is **toor**.
* *patience for everyone to get logged on; help if needed.*

## Introduction to Kali Linux

* Has anyone seen this operating system before?
* Kali Linux is free and is predominantly used in the Cybersecurity industry.
* Go ahead and explore the applications and tools. What did you find? Quite powerful tools in there!
* **Do NOT hack anyone without a contract or court order.**
* Remember, with this kind of knowledge and skill requires ethical and legal responsibility. Do not try this at home. Repeat after me: **it is illegal to do this outside of any legal contract or scope of work for law enforcement and it will get you to jail.** At GCU, we are Hackers with Halos: **We are here to serve, protect, and educate.**

## Let’s dive into a career of a Digital Forensics Investigator

* We are going to assist a Police Chief to gather evidence.
* Remember, this is a live CIA training scenario.
* Open up the folder on your desktop called **Network Forensics**.
* You will see two files. One is a DOCX and the other is a PCAP.
* Open the DOCX file first. *Wait a few minutes for everyone.*
* Let’s go over the scenario: *read it slowly. Point out pun of Ann.*
* **What is our mission? To gather the following evidence for the Police Chief.**
* We are sitting in a van (pause); and recorded her Wi-Fi traffic. We saved this data into a PCAP file. Let’s go back to the desktop and the same folder and open up that PCAP file.
* What is a PCAP file? Packet Capture – it captures network traffic.
* See the error? Errors are our friends in cybersecurity. They will give us more clues or guidance. Click ok.

## Introduction to Wireshark

* This is Wireshark. Has anyone ever seen or used this application before? This application is a **packet sniffer; used for analyzing networks.** You can find Wireshark on wireshark.org, and it works on macOS, Windows, and Linux, but not phones running Android or iOS.
* What is a packet? A segment of data sent from one computer or device to another over a network.
* A packet contains a source, destination, data, size, and other useful information that helps packet make it to the appropriate location and get reassembled properly.
* For example: If you were to write a letter to, let’s say, your Grandparent, put it in an envelope with the proper addresses and mailed it, we could then take it out of the mail stream, look inside for its contents. This is called a **Man-in-the-Middle Attack**.
* Or, when passing notes in across in class, a friend/student opens up the note and looks first before passing it on.
* This is common with open Wi-Fi’s: Starbucks, McDonalds, stores, etc.
* How is one way to combat this? VPN’s: Virtual Private Networks which encrypt data so it is not in plain text.
* Any questions so far?

## Wireshark’s Layout

* The bottom window is for hex data. We will not be covering that area today.
* The middle window is for headers and will not need to cover that today either. You can find more information on these areas all over the web.
* The main window is where we are going to focus on today. Let’s go through the columns to understand how the data can help you.
* The first column is the **Packet Number**. In this capture file, there are 572 packets. One packet is equal to one letter you wrote your Grandparent, so there are 572 different letters, so we need to pay close attention to this.
* The next column is the **timestamp**. Why do you think this is important? This information is critical when creating a timeline of events for evidence. (pause)
* **Source**: is the IP address (external or internal) of where the data is coming from. This is would be like a return address on an envelope.
* **Destination**: is the IP address of where the data is going. This would be the address on an envelope to where you wanted it mailed.
* **Protocol**: These are a set of rules, such as TCP/IP, SMTP, ARP, that are used on networks and the internet.
* **Length**: How big is the packet?
* **Info**: What’s inside the packet?

## Let’s get digging…

* **Now, EVERYTHING must be DOCUMENTED at 110% accuracy for evidence.** Why is this very important? (pause) **Chain of authority for court of law.**
* Let’s look at the first Q on the worksheet. (read the question to find Ann’s email address).
* Go through the data and find an email. Pay attention to the packet number. (pause)
* What packet number did you find? (#**69**, 72, 80)
* Ok, click on that line, right-click, scroll to **follow** and then **TCPstream**. This is due to the protocol used in capturing this information (pause, do it again if necessary). Data transferred over the Internet is sent as one or more packets. The most common packet sent is the TCP packet.
* Now look for at least **TWO indicators** to show that this could be Ann’s email address. Remember, you need 110% accuracy! (pause) Do you see anything?
* (slowly scroll down toward [sneakyg33k@aol.com](mailto:sneakyg33k@aol.com) area)
* Highlight the area FROM: [sneakyg33k@aol.com](mailto:sneakyg33k@aol.com) “Ann Dercover”
* Did she sign the letter at the bottom? This could be an indicator.
* What about the computer name? **ANNLAPTOP** (scroll up)
* Congratulations! we found her email address for Question 1.

## Question 2 in Wireshark

* Ok, what is the next question asking for? Why do you think we would need to find her password? (pause) As investigators, law enforcement could further their research within the account.
* Let’s look for her password. We need to find her logon process.
* Can you find any information about what email service was being used? (pause and explain the top lines; AOL, Comcast, etc).
* We need to look for **Auth Login** information.
* What is the first thing you type when logging into an email service such as AOL or Gmail? What can you infer?
* The Blue is AOL’s website boxes awaiting your input to sign-in, the red is what the user types in (user input).
* All of this information is encoded. We have to figure out what algorithm is used. What is an algorithm? (pause) It is a math formula. In this case, our clue is RFC 334. (Request for Comment)
* Back in the young days of the internet, a bunch of internet engineers got together and created rules for basic security: for encoding email messages, such as MIME.
* The LOGIN mechanism is a common method to login to a SMTP server. The SMTP communication example shows how **AUTH LOGIN** can be used to make an authenticated login to a server.
* After that, the AUTH LOGIN command has been sent to the server, **the server asks for username and password by sending BASE64 encoded text (questions) to the client.** (Show) “VXNlcm5hbWU6” is the BASE64 encoded text for the word "Username" and “UGFzc3dvcmQ6” is the BASE64 encoded text for the word "Password". The client sends username and password also using BASE64 encoding. "c25lYWt5ZzMza0Bhb2wuY29t", is a BASE64 encoded username and "NTU4cjAwbHo=" is a BASE64 encoded password.
* In this case, the encoding algorithm can also be identified by 3 characters. **The equals = The forward slash \ and the plus sign +**
* Do you see these characters in the red areas?
* We can now go ahead and decode.
* Highlight the red mumbo jumbo (highlight as you do this). Right-click and copy the text.
* We want to paste this information into a Text Editor, called **Leaf Pad**. Go to Applications at the top, find Accessories, and then Leaf Pad.
* Open Lead Pad, right-click and paste. (do it again if necessary)
* Save As, click Desktop, and type pass (in lowercase).
* **Linux is SUPER sensitive toward characters, file naming, spaces, etc. So please keep it simple when saving files.**
* Everyone with me? Now we are going to find the “Black Box” AKA the Terminal, which is THE most powerful application in Linux! You have to love power-tools!
* Go to Applications and select **Terminal** Emulator. You can close Lead Pad. (CTL+, zoom in view 4x)
* What was the encoding algorithm again? (base64)
* We are going to use the base64 command, however, we have to research on how to actually that command to decode the password mumbo jumbo.
* Type in the Terminal: **man base64**
* Man is the command for Manual for every tool in Linux.
* Let’s go through the Synopsis process. base64…OPTION…and FILE.
* We will use option -d for decode, which is also a flag in Linux.
* Press Q to exit the manual.
* Type **base64 -d Des**, press TAB, which will complete it as Desktop/ and then type **pass**, since that’s the file we saved earlier in which we want to decode. TAB is a shortcut in Linux that helps with typing file paths. It finishes the rest of the word and adds the slash.   
  **base64 -d Desktop/pass** …. Press return and tell me what the password is. (pause)
* **558r00lz** right? (pause and highlight)
* Fantastic! You have decoded the password of Ann’s email account. Again, why is it important to have the password for Ann’s email? (pause) Evidence trail can be furthered by having access to the email account. Any questions?
* Let’s return to the worksheet.

## Question 3 in Wireshark

* The next question we need to answer for the Police Chief is What is Ann’s boyfriend’s email address.
* Back to the PCAP file (clear the filters?) and search the packets for another email. [#80, sec558@gmail.com] (pause) What have you found?
* Remember, you need at least two indicators! What do you think?
* What is Ann’s boyfriend’s name? Mr. X?
* Let’s go back to the Wireshark main window.
* Go to the search bar and delete the filters.
* Search the packet lines for more email addresses. (pause)
* (slowly scroll down) What did you find? [#**132**?] Two indicators are needed.
* “Hi sweetheart….” (read aloud), What is Mr. X’s email? [mistersecretx@aol.com](mailto:mistersecretx@aol.com) Congrats!

## Question about items.

* What items was Mr. Secret X supposed to bring? Why did Ann ask to bring those items? Were they leaving the country? Going to the beach?
* Next question is about finding the name of the attachment (scroll down). What is the name of the attachment? [**Rendevous Point.docx**] Pay attention that it is a DOCX file.

## Decoding the Attachment.

* See the massive amount of mumbo jumbo code? That is the encoded attachment.
* What do you think the algorithm is? (scroll down where the header shows base64) What characters tell you this? + / =
* We need to copy that massive amount of encoded data into a new LeafPad file. Drag from the beginning of the attachment code and keep going. It does take some time. (pause) At the end, be sure NOT to add any spaces or extra information. This is extremely important (highlight the area)! Right-click and select Copy.
* Go back to Applications in the top menu. Go to Accessories and find **LeafPad**; open it.
* Right-click and paste the encoded data into a new document.
* Save As, click Desktop, and name the file **location** (lowercase). (pause / redo if necessary)
* Close **Leafpad** and return to the Terminal.
* Type **base64 -d Desktop/location**
* Whoa! What just happened?! Let me explain. In this case, the base64 tool is showing the data in an XML file format using Wingdings. We need to convert this into a readable format.
* Press Control-C to cancel out, and then CTL-L to clear.
* Type **base64 – d Desktop/location > Desktop/location1**
* Press return. Minimize all of your windows. On your desktop, you should find a file called location1.zip (move to the center).
* Right-click on that file, go to Open with Other Applications and find Libre Office, which the equivalent to Microsoft Office in Linux.
* Where did they go? (pause) Mexico, right? On the Beach. What did Ann tell him to bring? (bring the worksheet up)
* Do you like that? (pause)

## Authentication.

* What is the purpose of authenticating files? (pause) It is to show the court that evidence has not been tampered with. Anyone else have your fingerprint? This is required in the evidence chain, so the defense attorney cannot question the files’ authenticity.
* We authenticate with **HASHES,** which are digital fingerprints, unique – no one has the same ones. We will be using **sha256sum (or MD5sum)**. There are many others that can be used as well: MD5, SHA512, and more.
* Back to the worksheet, let’s see what is needed. We need to authenticate the ORIGINAL file on the desktop (location), not the one we converted.
* In Terminal, **type sha256sum Desktop/location**
* Or **type MD5sum Desktop/location**
* Press return, and that LONG number is the digital fingerprint of that file.
* Let’s look at the worksheet and the last question. We need to authenticate the Map found the in the attachment.
* Go to the menu bar and select the file that had the Map location.
* We need to copy and paste the map into a new LibreOffice text file and then save it. Right-click on the Map, select Copy.
* Go to File and select New Document. Right-click and paste the map into this new file.
* Save As. Now pay attention that this file is going to be saved into the Documents (not Desktop) folder. Name it pic. The full saved name will be pic.odt
* Back to the Terminal, **type sha256sum Documents/pic.odt**
* Or, **type MD5sum Documents/pic.odt**
* There is the number that would be recorded as the digital fingerprint.
* Any questions?

## Conclusion.

* Congratulations, you did it! Do you have and Questions?
* GCU Live: here is a GCU student from the Technology hallway.
* After GCU Live… I would also like to say a word about our NEW Cyber Range in Building 57 on Main Campus. This is a place of hands-on learning on cybersecurity tools using targets. It is very exciting. We invite you to come and visit us.
* Thank you again and have a great afternoon!

[www.cyberseek.org](http://www.cyberseek.org)

[haveibeenpwned.com](https://haveibeenpwned.com)