The first step of my investigation would be to familiarize myself with the case file. This is to ensure that I understand the specifics of the case such as what information I will be searching for and what types of devices I will be searching. The next step of my investigation will be to conduct interviews with people that have worked closely with Randy or on the same projects as him. I will ask them questions such as “What does Randy do in the company?”, “What projects has Randy worked on before?”, “Have you seen Randy talking about his work with unknown people over the phone or computer?”, “Has Randy ever asked you about projects he was not involved with?”, etc. I will also prepare my equipment that I will be bringing to the site. Items I plan to bring on site are a camera for taking pictures of the site, a smartphone for accessing information off of the internet, multiple imaging devices to take copies of the files present on Randy’s devices, target drives to store the imaged data from Randy’s devices, write blockers to prevent accidental modification of the data on Randy’s devices, a faraday bag and internal charger set for Randy’s phone, a headlight for increased visibility, a pencil and paper for recording information found at the site, suction cups for the removal of device drives, a magnifying glass for reading serial numbers and other labels on device components, three flash drives each loaded with a program for RAM collection, bags and loading straps to secure and transport equipment and evidence, and a standard toolbox containing screwdrivers, tape, pliers, scissors, and wire cutters. I will ask the owners of Wright Research and Tech what days Randy has off. I will make my plan to arrive at the office that day. This is because Randy is known to be protective of his devices, and his presence while I am at the site would be detrimental to the investigation. When arriving at the site of Randy’s workstation, the first thing I will do is begin documenting the scene using the camera to take pictures and video of the area, along with drawn diagrams and written descriptions. After documenting the state of the scene on arrival, I will check if any of Randy’s devices are currently powered on. Any that are I will use the RAM capturing flash drives to copy any data currently in the RAM of the device. Then I will get Randy’s phone to be placed in a faraday bag with a charger. I will leave Randy’s personal tablet alone because as it is not company property, I do not have the required legal permissions to search it for the investigation. Afterwards I grab Randy’s computer and take it out to my vehicle. I will then locate all of the company owned external drives and USBs in Randy’s workstation to be collected and brought out to the vehicle. Once everything has been loaded inside of the vehicle, I will take it all back to the lab. The reason for this is, again, that I have been told Randy is very resistant to having people inspect his items. By removing all of the relevant items from the site and taking them back to the lab, there is no way that Randy could interfere with the investigation. Once I have gotten back to the lab, the first thing will do is set up my computer and write blocker to start looking through any RAM data that was recovered on site. I could find very helpful information in these drives, such as passwords or recently deleted files. These passwords could be used to enter Randy’s secure accounts, and he could have deleted something incriminating recently. I will then begin to remove the drives from Randy’s work computer using the screwdrivers and suction cups. I will record the labels present on the drives. Then, using my imaging device, I will copy the data from Randy’s drives to my empty target drives, placing Randy’s drives back into his computer. I will then use my own response computer along with a write blocker to begin inspecting the data copied to the target drives. The first thing that I will do is take the hash value of the drives. This will be useful later for verifying that I have not modified any information present on the drives. After getting the hash value, I will locate and reveal any deleted or hidden partitions of the drives. It is very important that I do not miss any files that Randy has tried to hide from view. Then I will begin with some keyword searches on the drives. Keywords that I would like to search for include Wright Research and Tech, the names of any projects that Randy is suspected of selling information on, and the name of the company Randy is suspected of selling information to. Files with these phrases are likely to be involved with the possible crime being committed and are of interest to me going forward in the investigation. The next step of the investigation will be to investigate Randy’s work email for any messages pertaining to the previously mentioned keywords. Hopefully I was able to find the password somewhere in the RAM drives, but if not, I will need to use a password decryption method like rainbow tables before gaining access. Once inside the email account, I can look for messages either sent or received by Randy regarding the transfer of company files, or a confirmation of payment from the rival company for the information. Next, I will search for any chat messaging applications present on the drives. Searching these applications will have similar benefits to searching the email, as these may have been used to communicate with the buyers of Randy’s information. After that, I will check if the drives possess any of the necessary programs needed to use BitTorrent sites. If these are found to be present on the drives, I will search for the names of popular BitTorrent sites in Randy’s search history. These sites are used for p2p file sharing and are often involved in the sharing of illegal files, so Randy’s presence on one of these sites could be very important. Then, I will check the times that any files I found of interest were modified, accessed, created, or deleted so I can make a timeline of events that happened on the computer. Finaly, I will get the hash value of the drives a second time to make sure that nothing has been modified during the course of my investigation. With Randy’s computer done I will move on to his smartphone. I will connect to the phone using a compatible mobile forensics tool. Unless it is already unlocked, I will either get the password from Wright Research and Tech or use a rainbow table to get into the phone. Next, I will get the model information of the smartphone, which will be needed to prepare the forensics tool. Once it has all been set up, I will begin searching the phone for information. I will first check the phone’s call history and look for a number that is repeatedly called when Randy has one of his “family emergencies”. Once found I will determine who the number belongs to, as this person might be involved in the purchasing of the company data. I will then go on to perform a similar search on the phones messaging apps, looking for any mention of the projects Randy is suspected of selling data on, or the company Wright Research and Tech said he sold it too. Next, I will search for any stored files on the phone that could be related to any projects of Wright Research and Tech, and if they have been recently shared with any other devices. I will check the camera for any pictures Randy might have taken of physical records detailing any projects and if they were shared with anyone. Finally, I will check the phone’s location data to see where Randy went during his “family emergencies”. He may have gone to the other company in person to deliver his information instead of sending it over electronic communications. Now that I am done with the phone, I will move on to the independent drives, which can all be checked with an imaging device and write blocker setup like the main computer, and be searched for the same information, like program files. Once all the devices have been investigated, I will bring them back to Wright Research and Tech along with the finalized report of all my findings.

Resources used:

Digital Forensics Explained: Second edition by Greg Gogolin.

In class lecture presentations