Chapter 5: The Fog of War Four days later

Whiling away the late afternoon on the FreeCAD design of dove tail puzzle box, Lionel's mind drifts back to Liz Spotoc, her wound, and coded communication. He begins to wonder if Prof Yakubu and his band of merry software engineering students has made any progress at NCSU.

Suddenly there is a woophum sound. Lionel is popped upside the head by a Nerf bullet. Once again he has been attacked by that lone rogue assailant, Sandi.

"Heh geek the home-made turkey chilli's ready." she laughs as she fires another two Nerf rounds into the office. "Time to come-up for air.

"Don't forget the trash goes out after supper."

"On my way," replies Lionel as he shuts down the video camera and places it in charge mode while he eats supper. "Almost fifty years of marriage and you would think I would get a little respect from my wife."

Returning from supper and 'taking-out the trash' Lionel checks his email traffic. Near the top of one of his accounts' inbox is an email from Aminu. In that email Aminu announces, "Prof Yakubu team has identified the key for the archive treasure. Drop by the office tomorrow and we can discuss the next steps."

The next day after morning coffee at Claude's with the brew crew, Lionel and Sandi drive to Aminu's import/export warehouse. Aminu is not there. But Delo hands Lionel a closed, sealed envelope.

"Thanks Delo. Let Aminu know I will call later in the afternoon if I have questions or the check bounces."

"No worry, dey cheek e goot." replies Delo.

Back at the Acura RDX Lionel opens the envelope. A single piece of paper has 'spotoc' handwritten.

"Nuts, I should have guessed that password," issues a frustrated Lionel. "Anyway I am out of it now. NCSU has the resources, talent, and man-hours to throw at the rest of the blank canvas.

"Let's head home so I can make a couple of prototype runs on my puzzle box for Will's birthday present. It is beginning to look like I will have it done well before his March birthday."

Back in the workspace/office Lionel makes a couple of simulation passes on the dovetail puzzle box project he has been designing for a grandson. Just past Noon he takes a brief break for lunch.

At lunch he tells Sandi, "The puzzle box for Will is ready for milling. Let me know if you want me to add any scripting, scrolling, or printing to it. Otherwise it will just be a puzzle box with a twist lock, optical illusion with sliding dovetail mating surface at forty-five degrees, and a magnetic tap-locking pin.

"With FreeCAD and the CNC we can 'mimic' or create almost any surface writing, scrolling, engraving you want. Or we can just go for simplicity."

“Geek, let’s just keep it simple with a nice wood stain,” Sandi wisely cast her vote.

“We can put a couple of coins and a Jackson in the ‘safe-well. Will can use the puzzle box to keep his mementos safe from Zack. We both know how little brothers and sisters can be.”

Finally in the late afternoon he reaches a point of satisfaction in the simulated runs using the desktop running LinuxCNC.

Following supper he moves his FreeCAD designed puzzle box to the CNC milling machine in the garage’s workroom First he has to setup and tram the wooden work piece. Then he loads the gcode program for milling the puzzle box to the CNC computer. One last check and it is time to make sawdust. Lionel fires-up CNC milling machine.’s spindle which makes the first cuts along the x, y, z axes. He stays vigilant watching the physical progress on the work piece. As the milling bit progresses he tracks a shop vacuum to collect dust. This continues for some time.

Just after completing the second pass on the bottom half of the puzzle box, Sandi enters the garage’s workroom and gives the ‘cut-sign’ by making a ‘T” with her hands. As both of them remove their shop/shooting earmuff protection Sandi announces, “They have a fire going on State’s Centennial Campus. WRAL has a couple on-site reporters and as well as one in their helicopter. It looks like they are having a very busy night there. NCSU just started a home basketball game with UNC at the PNC Arena so the reporters were just down the road a couple of miles.”

“That’s a rough couple of miles between PNC and the Centennial Campus,” notes Lionel. Andrew and I ran in that stretch of road during a couple of marathons. The races would take us out to Ulmstead on the hills and then bring us loop towards PNC and then to Centennial Campus. PNC to Centennial Campus is flat until just before the campus. When they finish a marathon that last mile at Centennial Campus is a killer. I am glad I do not do marathons any more.

“Have they mentioned whether anyone was hurt or what building was involved? They have a lot of Engineering classes and labs there as well a sponsored research grant money projects and start-ups. That is where “Red Hat” was for a long time after it split from IBM.

“I’ll check it out at breakfast. I need to finish the bottom half of the puzzle box this evening to have it ready for Will’s birthday.

“But thanks for the update,” he says while replacing the ear protection. He blows a kiss to Sandi and restarts the LinuxCNC program session.

A bit later he calls it an evening and ‘closes up shop’ for the day…...

Rising early Lionel quietly prepares a yogurt blue berry based breakfast. Then he begins scanning his Samsung S2 Tab Android. Normally his scan path includes Dilbert, emails, WRAL, NYT briefing, Bloomberg, AP, and finally Foxx political cartoon. This morning that path is interrupted by the WRAL reports on the NCSU Centennial Campus fire. Apparently, there was a minor explosion followed by a rapidly burning fire that engulfed two floors along the Northern wall of Engineer Building 1…..

Later in the morning after normal coffee with the brew crew Lionel receives a call from Aminu.

“Prince Jones did you hear about the fire at State last night.?”

“Yes, Sandi gave me a quick report while I was playing with a CNC project in the garage.”

“Well Prof Yakubu called me this morning to say that the computer lab was on the floor just above where the fire started. They do not know yet how the fire started. But there appears to have been a bottle of propane stored in an unused locker used by robotics lab. Apparently, there was undefined ignition and the bottle went-up. The bottle appeared to be the type you might use for camping or a small BBQ. It should not have been in the building. The authorities are attempting to determine whether this was an accidental ignition or arson. The lab locker had not been used since early last semester. At that time it had been assigned to grad student working as teaching assistant for the robotics lab.

“Now Prof Yakubu says that it appears like the project is dead. The original micro-SD card and the two controlled copies were logged into a locked file cabinet. Unfortunately, the cabinet appears to be a complete loss between the fire, toxic melted plastic, the overhead sprinklers, and RFD attempt to quell the fire. Prof Yakubu holds no hope of continuing. He is releasing the team of students to other projects.”

“Well at least no one was injured. They were probably all at the PNC game last night.

“Call me when you need a cup of coffee or a break.”

“As you say ‘roger that’ ole friend.”

Lionel finishes breakfast and toils in the kitchen briefly and starts his day while Sandi continues to catch a few more winks.

Once Sandi finishes her breakfast routine they head to Claude’s for a rally cup of coffee with the brew crew. Discussion is lively but focused on the State Centennial Campus and loss to UNC at the PNC Arena. “A four point loss is still a four point loss,” lauds ‘Smoooth’. It seems that COVID and politics has dropped to a distant third and fourth place on the topic list.

Upon returning from coffee call Lionel restarts his CNC puzzle box project. With completion of the bottom half of the puzzle box, he moves to milling the top half. He basically repeats last nights activities but with a new work piece for the top. About the most difficult part of this half is the ‘upside-down’ view that is required. Lionel notes that it is like building a small wooden row boat or skiff.

Pushing forward with the milling of the top of the puzzle box, his mind begins to wander. Suddenly, Lionel recalls that he has an exact copy of the original micro-SD card.

“This is an ethical dilemma. The authorities are satisfied, the parents are moving forward as best they can, and the resources at State have been scattered to other projects. But I have a copy of the original SD card.

“I should be done with everything on the milling side of the puzzle box before Noon. I could start sanding and fitting the magnetic locking pin this afternoon. After that it would be a cycle of light, fine sanding, staining, drying, and re-do as needed.

“I see what Sandi thinks at lunch.”

Over a peanut butter sandwich with blue berry spread at lunch, he lays-out the ethical dilemma to Sandi.

"I would really like to know whether the original SD card just had embarrassing pictures or some detail that would help explain why the two adults with diabetes disappeared. But everyone is moving forward now that the original Rosetta Stone has been destroyed."

"May be you can accommodate that perception of duty and still respect Stacy's and Frank's families' need for privacy. How about quietly continuing to hover over the copy you have? That way you can exercise whatever resources you have to fulfill that duty. If you find something of potential value you can hand it off to the authorities and make the family aware that something of value was recovered from the residuals of your original effort.

"If you find anything that would embarrass the memory of the couple, you can just discard your remaining copy.

"You would have four to six weeks to 'root-around' like geeks do. May be even longer. There does not seem to be any rush for answers."

"As with everything I touch it always takes longer than I estimated. So this afternoon I will return to the milling of the top of the puzzle box. The dovetail groves need just a little bit of mill shaving to give the lid a smooth forty-five degree slide.

"I anticipate starting the sanding and magnetic locking pin embedding by mid-afternoon.

"Before I head back to the garage I will marinade the chicken for tonight's barbecue…..

A little before 5PM Lionel has completed the first cycle of sanding and staining of Will's puzzle box. He shuts down operation in the garage and starts pulling together the implements and components for this evening's barbecue chicken. The gas 'barbee' is running, the marinaded chicken has been laid on on a long sheet of aluminum foil isolating it from the flame.

Glancing occasionally at the 'barbee' and checking the chicken occasionally, he resumes reading Song Yet Sung. His mind drifts back to Liz Spotoc, her wound, coded communication and then Stacy and Frank.

"Now suppose that one of the two, Stacy or Frank, had a large file on a storage media of any type, what data might it contain?

"For Stacy it would most likely be either one or more stories on which she was working, a collection of pictures and videos from family and friends, or may be a system backup. For Frank it would be a copy of his software development projects, a collection of his development tools and environments, or a backup of his system.

"What we know is that the file is a large RAR compression file. First because of its size it will be difficult and time consuming to manage. Second access to the compressed file is guarded by a password or pass phrase. Third, Prof Yakubu team discovered the password to unlock the '210203_dahlonega.rar' archive file. "Knowing that would have saved a few days of probing. But then it really takes a good computer to slow things down."

After cleanup from supper he migrates to the workshop/office to start a second 'go-at' at 210203_dahlongerga.rar'. As he did previously he starts the audio and video recording equipment.

Still playing it safe, Lionel uses the “Internet isolated” older, slower LinuxCNC Simulator computer instead of his ‘faster’ laptop. On that machine he opens a Nautilus file manager session. Then he double clicks on the ‘210203_dahlongerga.rar’ archive file. That actions pops the Ubuntu Archive Manager which immediately demands a password. Lionel enters ‘spotoc’ and clicks the ‘OK’ button.

That instantly displays a folder named 210203_dahlongerga. Opening that folder displays a long list of files within that base archive folder. Lionel returns to the top folder of the archive and keys the ‘Extract’ button. As the extraction operation begins The Archive Manager program displays a query window asking for the destination into which the archive artifacts is to be placed. Lionel directs the Archive Manager program to place the extracted artifacts into a folder he names 211227_workDir. Pnce the Archive Manager stated, its work a status window is shown indicating that the process will extract 61 files from ‘210203_dahlongerga.rar’. A slow , steady process extracts the contents of the 167 GB archive file.

Because of the mammoth size of the archive file, Lionel utters “This is going to take a while. I might as well return to reading ‘Sony Yet Sung’.”

In a Terminator like accent Lionel say to no one in particular, “I’ll beee bacck in the morning.” With that he leaves the workshop/office for the garage and finalizing Will’s puzzle box. After an hour or so he completes the staining of the top and bottom of Will’s puzzle box. He the calls it a day.

Mid-morning the next day, he returns to the workspace to find that the extract has completed. Before going further he halts to prepare for his deep dive. First he verifies that his Sony Digital Video Camera Recorder is fully charged, that a second battery for the camera is charged and within arms reach, that the Camera is loaded with with a micro-SD card with about eight hours of record time available and that a second micro-SD card with another twelve hours is within arms reach. He mounts the camera on a boom tripod and adjust the location to cover the main display screen and audio pickup from the desk chair. Then he briefly tests the audio/video setup.

He plans to use the of Nautilus file manager so he can manually search down the listing of extracted files . He plans to focus specifically on file type and size. He anticipates discovering that some files are text files of a manageable size and other are binary files.

From long experience working with text and binary files, Lionel knows that a files is manageable if there are applications that allow the user to quickly view and work with the contents of a text or binary file. An unmanageable is one which is so large that it consumes massive amounts of time and resources to view and manipulate using a tool or application. Technology-wise he plans to use an application called geany to view text files. For binary files he will rely upon an application called gHex.

Completing preparations he begins to examine the file listing of sixty-one extracted files. Near the top of the list he identifies a file name he has seen many times, ‘clonezilla-img’. The ‘clonezilla-img’ is a human readable text files that serves as a log for an archive operation that a user might have performed. Using the geany editor application he is able to view the text content of the file. As he views the an abstract he sees the pattern of a line number followed by a line of information associated with the creation of the Clonezilla image of a computer.

If his knowledge of the Clonezilla image creation and restoration is correct he can rebuild an exact copy of the computer as it was on February 3 at 9:50PM. Because of the sophistication of the archive file he is certain that the image will be that of Frank's computer. But to gain access to any computer that he restores he will need either a superuser account password or a high level user's account password.

Just at that point, Sandi pops into the workspace/office. "How's it going?"

Lionel responds, "If I can guess or find the correct user/password combination then we can take a look at contents and attempt to determine whose computer image this is.

"The image was made the day before Stacy and Frank left their condo."

"Good hunting. Let me know what you find," supports Sandi "How does oven broiled flounder and rice sound for supper?"

"Flounder sounds great." Lionel answers as Sandi leaves the workspace/office.

Returning to the 'clonezilla-img' file contents display in the geany editor, Lionel delves deeper into the details.

At the very top of the displayed abstract from clonezilla-img text file:

```
1 This image was saved by Clonezilla at 2021-02-03 21:50:08 UTC.
2 Saved by clonezilla-live-2.5.2-31-i686-pae.
3 The log during saving:
4
5 Starting /usr/sbin/ocs-sr at 2021-02-03 15:24:46 UTC
6 … 88
*** Jumping To Line 89 ***
```

"Now let's see if the clonezilla-img log has any useful information or anomalies that might be helpful."

Near the bottom of the clonezilla-img text file:

```
*** Jumping From Line 88
89 This program is not started by Clonezilla server, so skip
      notifying it the job is done.
90 This program is not started by Clonezilla server, so skip
     notifying it the job is done.
91 Finished!
92 Finished!
93 ### gonza catflipper1192 ###
94 ### End of log ###
95 ### Image created time: 2021-0203-2150
```

"There are 95 lines of text. Lines 1 to 88 provide technical details of how the Clonezilla application organized and executed the building of an archive image of someones computer. Lines 89, 90, 91, and 92 report how Clonezilla closed this specific archive process.

“Line 93 is not a standard Clonezilla entry. It could be password authentication word pair. We will have to restore the full image to see if ‘gonza’ is a user name and whether the password embedded in in the ‘clonezilla-img’ file will provide access to that user account.

“The best test for whether this password authentication word pair is useful will be perform a restore using this Clonezilla image on a test PC or separate virtual machine. Then see if there is a user account called “gonza” and then just try a log-in with the password.

“If I gain access I will need to determine the user privilege for ‘gonza’.

“I will use the ‘ole’ IBM ThinkCentre, LinuxCNC simulator. That way if there is a virus in the Clonezilla image it will be isolated. But lets first start with an image backup of the LinuxCNC simulator.

“Before proceeding we are going to copy the the files we just extracted to a spare USB thumb drive.”

Completing that copy/paste operation without incident he places a label tag on the USB thumb drive and ejects it. On the label tag of USB thumb drive he just ejected he writes ‘gonza’. Then he begins new Clonezilla image backup of the LinuxCNC simulator exactly as it sits.

Once the backup image of the LinuxCNC simulator completes and is safely stored, Lionel begins restoring from the archive Clonezilla image by first powering-off the machine. Then he inserts USB thumb drive with a self-booting version of the Clonezilla application, powers the machine, and presses the F-12. The pressing of the F-12 function key interrupts the normal boot-up process. That allows Lionel redirect the boot-up process use the USB thumb-drive. Once redirected the boot-up process continues as noted by the display of text across the display. Quickly the Clonezilla start page is rendered.

Continually pressing the Enter key, Lionel proceeds through the Clonezilla process in default mode until it abruptly stops. At that point the applications needs to access the media with the sixty-one extracted files of the 210203_dahlonega folder. To achieve that Lionel inserts the archive USB thumb drive labeled ‘gonza’. After a brief pause he instructs the Clonezilla application to proceed to continue by keying the Enter key. The Clonezilla applications then pushes forward identifying devices attached by their Linux /dev/ designation. Once verifying the correctness of these designations, Lionel keys the appropriate Ctrl C key combination.

A stream of text statements across several rows scrolls down the display. A series of Clonezilla application queries allows Lionel to ‘point’ the application toward the archive USB thumb drive where the ‘archive repository folder’ is located. The Clonezilla application then seeks confirmation that a ‘restore disk’ operation desired by Lionel..

The Clonezilla application then requires confirmation that the target device for restoration is the primary drive, /dev/sda. With that instruction given, the application begins a set of question that require only a default to pass through to the actual start of the restoration process.

With the restoration running on automatic now, Lionel is about ready for lunch….

Returning from lunch to the restore operation Lionel observes that the restoration has completed. The next move is to start a clean session using a power-off. Once the power-of sequence completes, Lionel removes the USB thumb drive with the Clonezilla application and the USB thumb drive with the collection archive files. Then he powers the newly rebuilt machine.

The rebuilt machine comes back into service cleanly. It cycles through the Ubuntu startup sequence and displays a window listing three accounts. One of these accounts is ‘gonza’.

“Well after a long drought we have a little rain. ‘gonza’ was an actual account on the original PC from Stacy’s and Frank’s condo. Now will the ‘catflipper1192’ unlock the kingdom?”

Lionel selects the user account ‘gonza’ and enters the ‘catflipper1192’ password.

The operating system of the machine responds. Shortly a desktop display is rendered with icons arrayed along the left in totem pole fashion. In the desktop itself there are a number of other application icons. Many of these icons Lionel has seen and used previously. Some he uses daily for general user tasks and some for development work on his regular Ubuntu systems.

Returning to the array of icons along the left, Lionel selects the ‘Terminal’ icon from the task bar. That opens a standard Ubuntu terminal for entering command line statements. The Terminal’s prompt shows ‘gonza:~$ ‘ plus a blinking cursor. With a sigh of relief Lionel exclaims “Houston we have lift-off.”

Quickly he enters: ‘groups’ and presses the Enter key. He receives the response: ‘gonza root adm tty dialout cdrom sudo dip www-data plugdev input lpadmin sambashare docker svn mbot’.

Lionel shouts “Bingo. We have a ‘coverall’ winner with B14.” The response in the Terminal tells him that the user gonza is a member of the root and sudo groups. He knows that he now has the keys to the kingdom. It is just a matter to searching for answers in a haystack of 164GB of ‘hay’.

“Heh Sandi come see what I did,” he yells down to his wife.

“I am on my cell. I’ll be there shortly,” Sandi calmly answers.

“That’s okay. The real work starts now” acknowledges Lionel in a mood of growing frustration as he realizes that he has a large hay stack to push through to find anything useful. “Where to start? He asks himself. “Let’s see whether gonza has any email or social media accounts. Then we will look at the system logs.”

“Let’s go to gonza’s home directory and look at his web browser and email applications. It seems that he has FireFox web browser application and Thunderbird email application. Let’s try Thunderbird first. We should expect to find more significant information about Frank from his email artifacts than from his web browser artifacts.”

“The user gonza Thunderbird application shows that three accounts were active at the time the archive was created. Those are frogclaw@anetswarf.com, frana248@spectrum.com, and frana892821@gmail.com.

“I am familiar with the spectrum.com and the gmail.com. I am not familiar with the anetswarf.com email domain. I did not see any new incoming emails land in the inbox folders so the accounts must have been terminated or deactivated at the domain hosting sites.

‘Checking the local Thunderbird email account settings seems to indicated that at the time of the archive was created the local email application had contact with all three email servers or domains. The local Thunderbird email accounts were set to ‘push’ to a folder in gonza’s home directory called ~/archive_local. We will put that folder on our todo-list. May be can pass a grep search through it for key search terms. But we need to create the key search terms first.

“Just to check that the spectrum and gmail accounts are in-active I will send an email from my normal email accounts.

“But first to be safe let’s switch from the ‘ole’ IBM ThinkCentre, LinuxCNC simulator to another computer running Ubuntu that is actually tied to the Internet. In that way we will insure that nothing leaks from the ‘ole’ IBM ThinkCentre, LinuxCNC simulator. “

To accomplish this security action, he merely switches the buttons on the KVM TK409 switch. That flips the keyboard, speaker, microphone, and display to a laptop that is linked to the Internet. Now he proceeds using the laptop via the TK-409 switch as the user “gonza@mypond”.

“Now let’s ping the anetswarf.com domain to see if it is touchable today. First, we will test with ibm.com and then anetswarf.com.”.

First IBM test ping verifies that we have a good Internet connection:

```
gonza@mypond :~$ ping ibm.com
PING ibm.com (104.122.183.82) 56(84) bytes of data.
….
--- ibm.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time
     7010ms
rtt min/avg/max/mdev = 23.201/29.569/35.881/5.430 ms
```

Attempt anetswarf.com test ping:

```
gonza@mypond:~$ ping anetswarf.com
ping: unknown host anetswarf.com
gonza@mypond:~$ ping anetswarf.com
ping: unknown host anetswarf.com
gonza@mypond:~$ ping anetswarf.com
ping: unknown host anetswarf.com
```

“We know from earlier information that Stacy worked for AP as a freelance reporter so let’s ping AP.”

```
gonza@mypond: ping ap.org
PING ap.org (23.217.28.70) 56(84) bytes of data.
64 bytes from a23-217-28-
     70.deploy.static.akamaitechnologies.com
     (23.217.28.70): icmp_seq=1 ttl=52 time=32.4 ms
...
--- ap.org ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time
     6007ms
rtt min/avg/max/mdev = 31.486/34.405/44.227/4.101 ms
```

With the pinging done he switches back to the ‘olle’ IBM ThinkCentre, LinuxCNC simulator that remains isolated from the Internet.

“The attempts to ‘ping’ anetswarf .com failed to confirm touching that email host domain. To see what anetswarf.com really is or was we can search the Internet to see if there are any hits. If we find hits it might be a nefarious or a suspect site that we do not want to notify of our existence. So at this time we will not send any traffic to that email host even if that email host is still active.

“When we start to look through the ‘old’ email traffic to and from the email host we will look behind the email into its text version with it header and body information. That may provide additional insight.

“As stated earlier we need to take a stab at triaging our search across the 167GB clone of Frank’s and Stacy’s computer.

“We must continue to work with the assumption that Frank’s and Stacy’s email behavior was similar to most email and social media users. By that we assume they received and sent email traffic through the gonza Thunderbird Email client application. Some of the traffic remained stored within the hidden Thunderbird email application’s folder:

`‘/home/gonza/.thunderbird/pgetamc0.default/Mail’ Size 313MB.`

“The email application's folder is typically used for short-term retention of email artifacts. Stacy or Frank may have periodically elected to use the archive folder identified in the Account Preferences for longer term retention of their email artifacts of interest:

`‘/home/gonza/Local_Folder’ Size 1.7GB.`

“We will quickly scan through the gmail.com and then the spectrum.com email folders residing in gonza home email directory. We are going to assume that the anetswarf.com is an email host that was associated with contract work on which Frank may have been working. We are going to limit our search just to the period prior to February 4, 2021 back to Early October when he was hired.

“The scanning we are going to do will be in two phases. In the first phase we will perform a visual scan of each of the three email accounts’ draft, sent, junk, and delete sub-folders. In the second phase we will perform detail automated scan for ‘terms of interest’ which may be found in the email files.

“During the first phase the Thunderbird email client will be used. That client displays each of the accounts sub-folders in an easily readable html formatted artifact. We can quickly click on a sub-folder for an email account an see what is in that folder. If something looks interesting we can view the display as Frank or Stacy might have seen it. Plus we can also elect to see the email of interest in its text mode version. The text mode version is a bit harder to read. But it contains technical information regarding the origin, transport, and movement of the email. By scanning and reading any emails of interest we can begin to identify key words, patterns, human actors, etc. of interest. These we will add to a pattern file we will call ‘iii_keyfile’ where ‘iii’ is an integer from 001 to 999 used to identify a specific pattern file.. This file will grow as we gain useful insight.

“In the second phase we will demonstrate why software engineers like us are lazy. We like to do things only once and automate laborious task so we can mature it and execute it in a repeatable manner. So we will develop a shell program that we will invoke to ‘quickly scan’ through the gonza email directories. Our shell program will run a Unix utility called ‘grep’. The ‘grep’ utility searches plain text content for matching patterns. The ‘grep’ utility has various options that greatly increase its parsing, flexibility, and filtering. The ‘grep’ utility can search for simple patterns as well as complex, convoluted collections of patterns. We will first work to create a satisfactory ‘scan’ of the gonza home email directory of3.13MB in size. Once that is reasonably achieved we will bump the ‘scan’ with its ‘pattern file’ against the larger Local_Folder repository of 1.7GB in size. All it takes is time, diligence, and a little luck.

“We know this is going to take awhile to generate any satisfactory results. So we start with the simplest pattern imaginable. Because our missing software engineer of interest is Frank Rana, the first key_file pattern file, 001_keyfile, has only one pattern, ‘rana’. We couple that simple key_file with

similarly set of rules for the ‘grep’ program to follow. I am placing various technical terms that I intend ti use in an appendix called Appendix A. I am creating a second appendix, Appendix B, to augment this audio/video report. I am using Appendix B to collect the actual technical details concerning how the grep program and the pattern files grew in complexity and usefulness. In that way we can develop the shell script, dogrep4home_email.sh. Before continuing we need to add a couple of ‘grep’ parameters to help garner useful outputs. First we require ‘grep’ to recursively search for the patterns found in the key_file. Then we need to inform ‘grep’ to use a specific key_file. To increase the flexibility of ‘grep’ we must follow ‘grep’ syntax so that it will use the appropriate ‘source folder’ in which to start its recursive search. I am collecting this information Appendix B for this first “run”. I will use Appendix A to document all subsequent maturing /development of the shell script and the key_file. Note that Appendix B will ultimately contain the first shell program and the final shell program. It will also contain the final key_file.

“With our first version of the shell script, dogrep4home_email.sh, we are now ready to throw the switch, kick the cat, see what happens. We currently have the dogrep4home_email.sh shell script in the gonza home folder. The results will be displayed on the screen. We run the shell script from a Terminal command line as ‘./dogrep4home_email.sh’ . Invoking the shell script yields three messages followed rather quickly by a display of results. We want to capture the results for further analysis. Scrolling back toward the start of the grep, we see the message telling us to redirect the results to a file of our own choosing. Without changing dogrep4home_email.sh or the 001_keyfile we modify the command-line for this new invocation so it looks like ./dogrep4home.sh > 001_Key_001_Run. Running this invocation places of the previously displayed results into the gonza home folder as a file named 001_Key_001_Run.

“Using the genay editor we now see that 001_Key_001_Run lyields a ists the entire line of files that contain the search pattern ‘rana’. This listing gives us the the convenience and time to analyze the results of the search for ‘rana’ in the gonza home mail folder. This first pass through the gonza home email folder of size 313MB identified only thirteen files to ‘read’ and to analyze. From our brief review of the listed emails and analysis we have located five new key words to add to our pattern search file.

“We now modify the shell script, dogrep4home_email.sh, to use the newly revised key_file with the the additional newly located search patterns. This pass results in identifying 149 files. Now we are beginning to experience complexity. But grep has parameters that may help ease the search and our analysis. have a bigger “reading” burden in order to capture the context in which the a specific search pattern term is being used.

“I assembled Table 1: Pattern File Growth show that our analysis will begin to falter due to the growing complexity caused by our growth in knowledge and resulting new search patterns added.

Table 1: Pattern File Contents to Hits

	Rational for Adding to Search Pattern	
`002_keyfile:`	`pass001==>13hits`	`pass002==>149hits`
`rana`	Frank’s last name.	
github		Public project repository
link2link		An IT job posting site
banks		Stacy’s last name
apnews.com		AP email

ap.org AP email

&&*

"Our new search pattern file is called 002_keyfile. We modify the original 'dogrep4home_email.sh' by incrementing the pattern filename from /001_keyfile to /002_keyfile. We run this new version redirecting the results as we did just a moment ago using a different name for the output file. The new results file is named 002_Key_001_Run. This run produces 2173 hits. The 2173 hits involve numerous duplicate listing of files containing the search patterns. So we make only one copy of any file that is listed at least once. That copy is pasted place in a safe work folder that will serve as a collection bucket. With that collection we are ready to move forward.

"Now let's try using the geany editor search feature rather that attempting to read the files associated with 'hits'. We will begin to sequentially search the collected file sequentially for the five 'new" patterns. Of the five new patterns he learns that the are no hits for 'apnews.com or ap.org. That seems to indicate Stacy was not using Frank's computer to communicate with AP editors or peers. So now we are learning something about Frank and Stacy.

Finally closing the analysis of the last pass through 'grep using the 002_keyfile he wraps-up his review with seventeen new patterns in his next version of pattern file but with only one conclusion: Stacy did not use any of the gonza emails. The newly modified keyfile he renames 003_keyfile. Then he modifies the 'dogrep4home_email.sh' in two places to use the 003_keyfile.

It has been a long, fruitful evening. He has pushed a set of patterns through the home email folder for gonza. He has eliminated Stacy contacting AP via the gonza username.

But there is still work to be done before calling it a day. Now that he knows Stacy has not been using Frank's Ubuntu username and email accounts, it is time to see what if any other Ubuntu user accounts exist. He already knows that 'root" exist by default. Plus he knows he can take control of that account since 'gonza' is a member of the 'root group'.

Selecting the System Settings icon he navigates to the 'User Accounts' icon and selects that one. That action pops the User Account window. It shows that he can he can take control of two 'standard' accounts, deyfine and toerr. He uses the gonza account to search the home directories of these two accounts.

For the first account ,deyfine**,** may have been used by Stacy prior to the creation of the February 3 archive. It does have its own Thunderbird email account. The second standard account, toerr, does not have any Thunderbird account associated with it.

Before finishing for the day, Lionel writes himself a note about the plan for tomorrow. "Continue with the gonza email scan of the 1.7 GB Local_Folder . Gain control of the deyfine account to check the Thunderbird email activity."

"Time for a sip of Pinot Noir and a couple of chapters of Michael Connelly."