**Saliman Zadran**

**Forensics Project – M57 Patents Case**

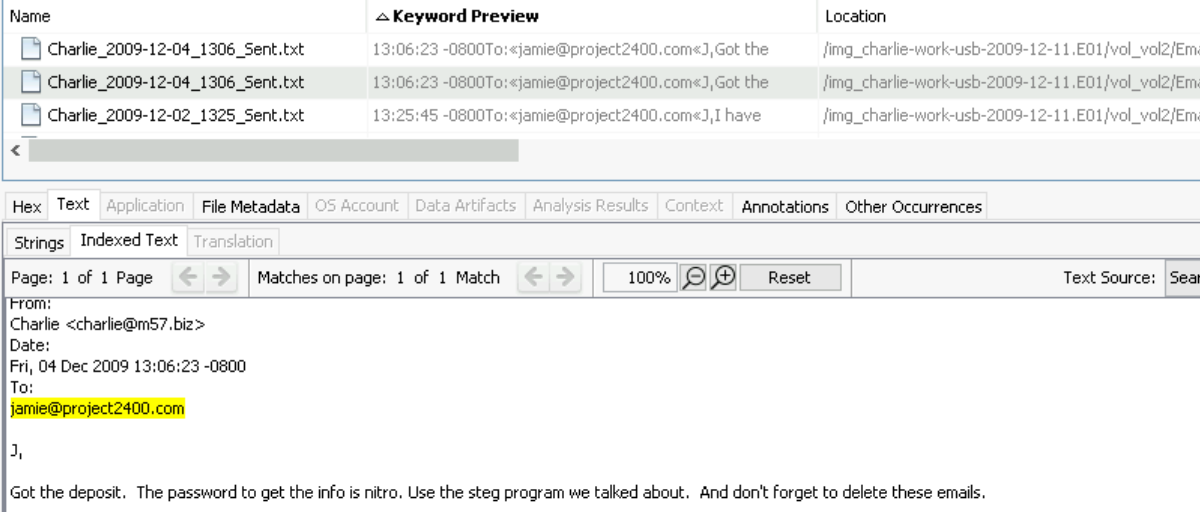
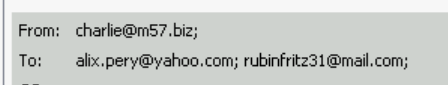
To start off, we read through the case details and the two PowerPoints provided. Granting details regarding the investigation, and what was seized legally by law enforcement. I then went ahead and created the case in Autopsy. I added all of the device/drive images to Autopsy and began an analysis of it. In all three of these situations, the three employees involved in potential criminal activity can be charged.

**Emails and Attachments:**

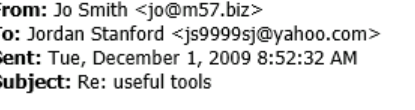
The initial look into the data available, regarding emails deleted to remove evidence. Although files were deleted by Terry successfully, they can be recovered by law enforcement.

There are quite a few other users that appear to be emailed, some of whom seem to be friends, others seem to be accomplices in criminal activity. The three employees involved in criminal activity, are Charlie, Jo, and Terry.

The list of emails with screenshots:

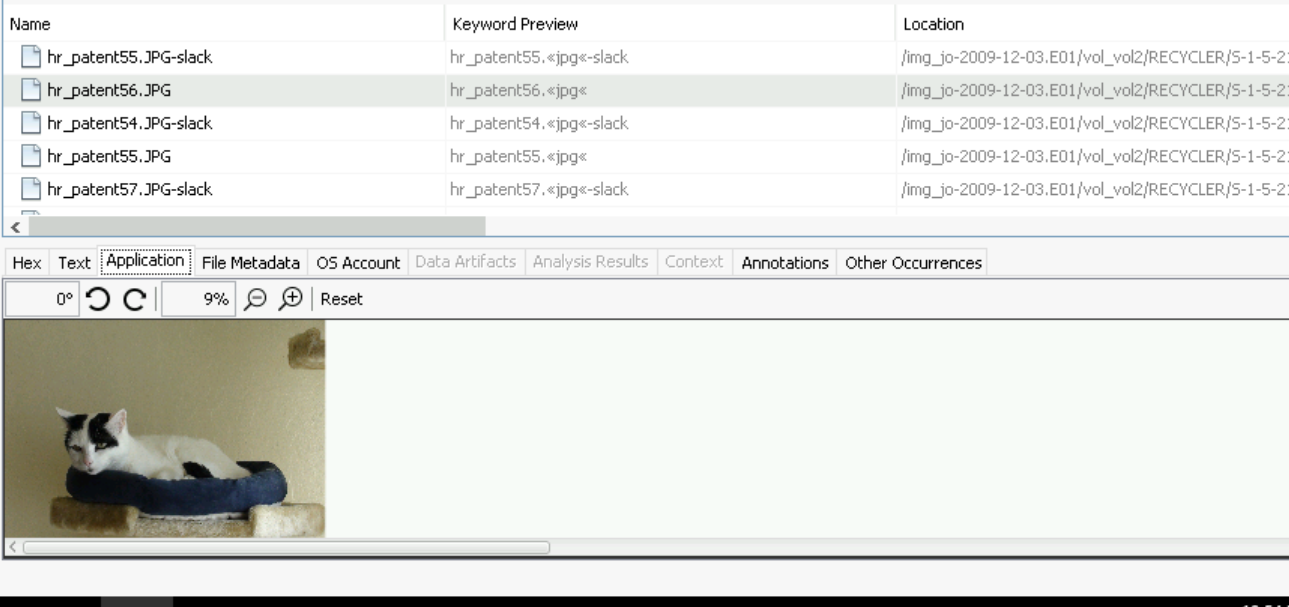
* In contact with Charlie are, [Alix.Pery@yahoo.com](mailto:Alix.Pery@yahoo.com) and [rubinfritz31@gmail.com](mailto:rubinfritz31@gmail.com) both seem to be friends of Charlie. Charlie was also in contact with a potential buyer for proprietary company information, regarding “prior art” it was Jamie@project2400.com: 
* In contact with Terry, tech.norat@hotmail.com and [ghost.wisp@live.com](mailto:ghost.wisp@live.com) who seem to be friends of Terry, however when selling Jo’s computer on craigslist he was in contact with [Aaron.Green12@gmail.com](mailto:Aaron.Green12@gmail.com), using his personal gmail account.



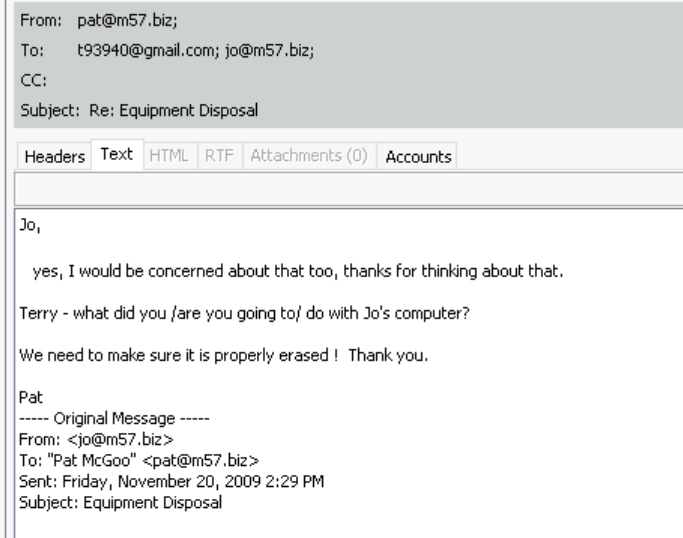
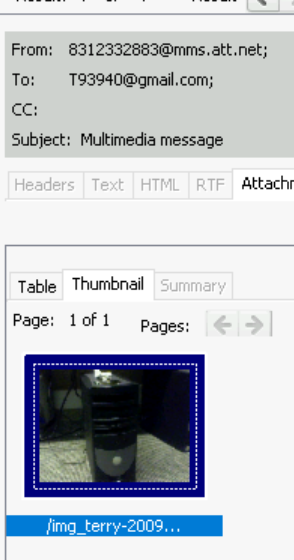
* Finally, there was Jo, who was in contact with [js9999sj@yahoo.com](mailto:js9999sj@yahoo.com), to whom they were sending HR patents. 

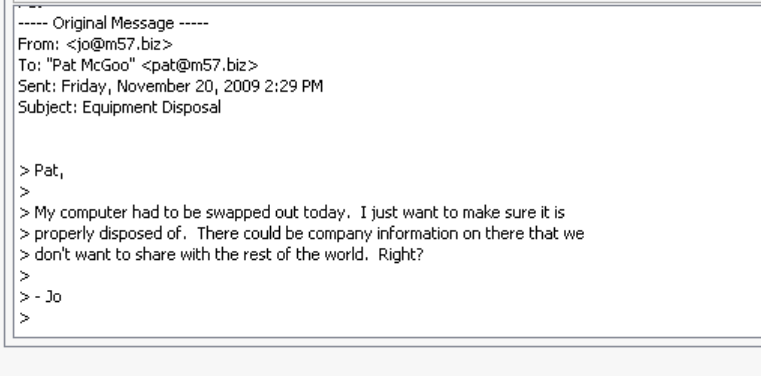
Part 2:

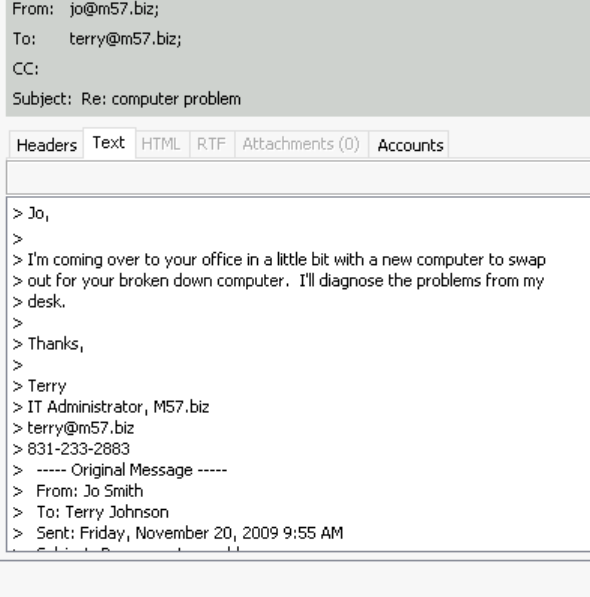
Yes Jo is the owner of the files, the evidence is shown below of the images of HR patents stored on Jo’s device:



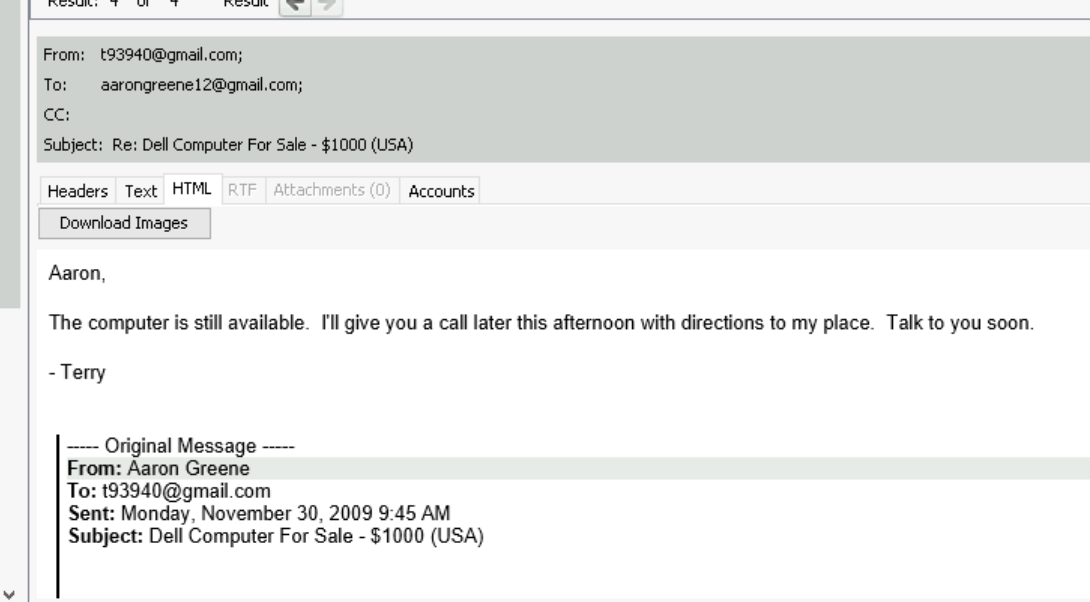
The computer ended up being sold on the seconday market by the IT guy, Terry. He retrieved the computer from Jo to troubleshoot it being slow, instead he took the computer, and listed it on craigslist to be sold. This is an image of Jo’s computer that Terry emailed to himself. There is also emails showing Terry retrieved Jo’s computer for troubleshooting. Terry had let Pat and Jo know that he would wipe the computer clean, however he failed to do so. As Aaron.Greene, the buyer of the computer would turn the computer in to law enforcement.

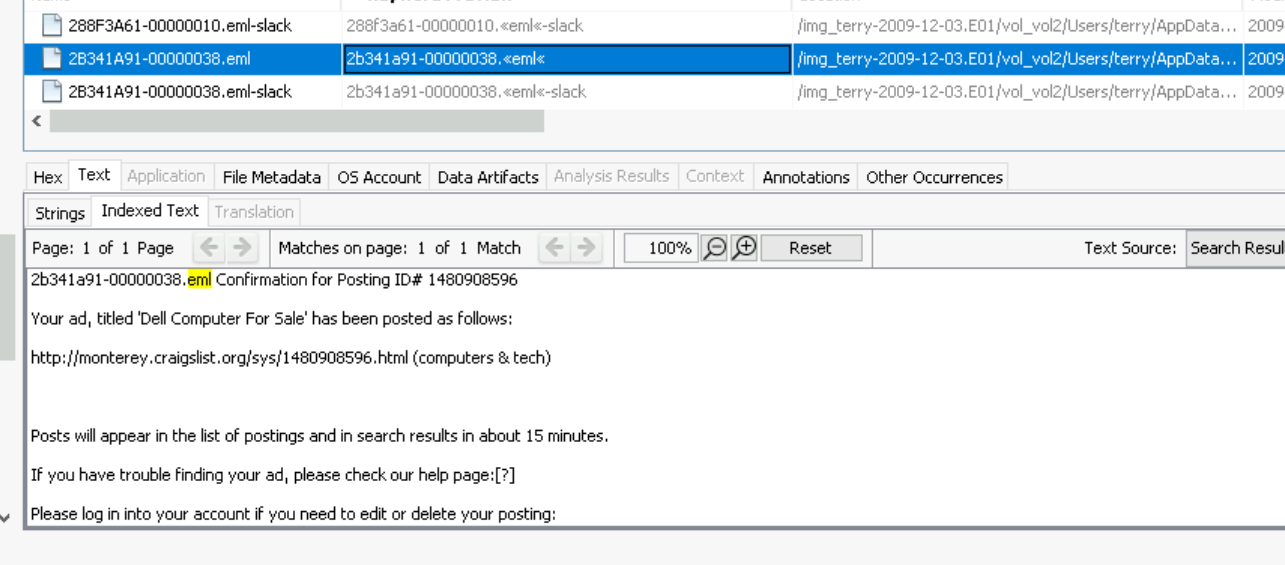




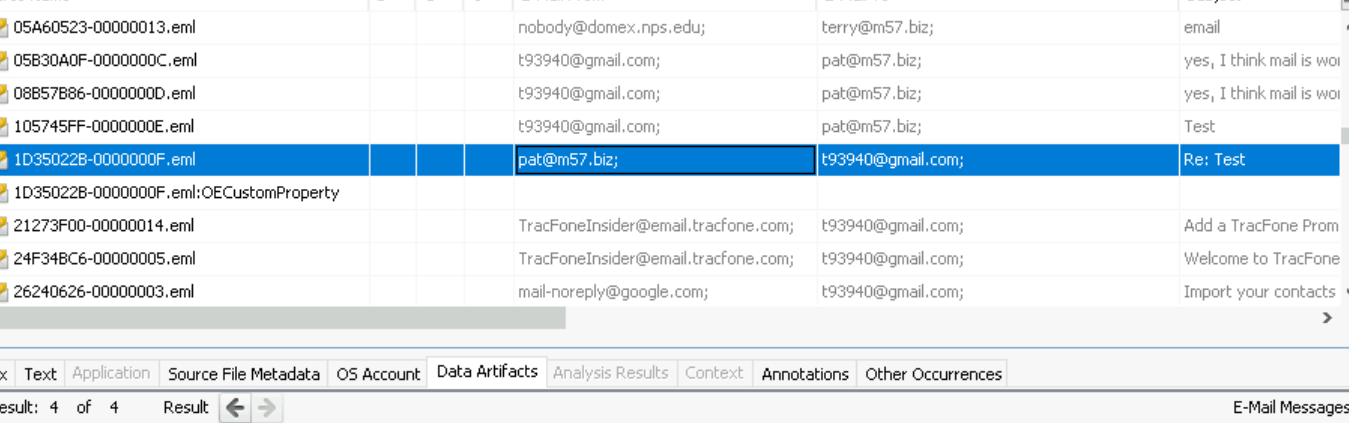


Below is evidence of Terry listing the same Dell computer shown in the image above, for sale on craigslist:

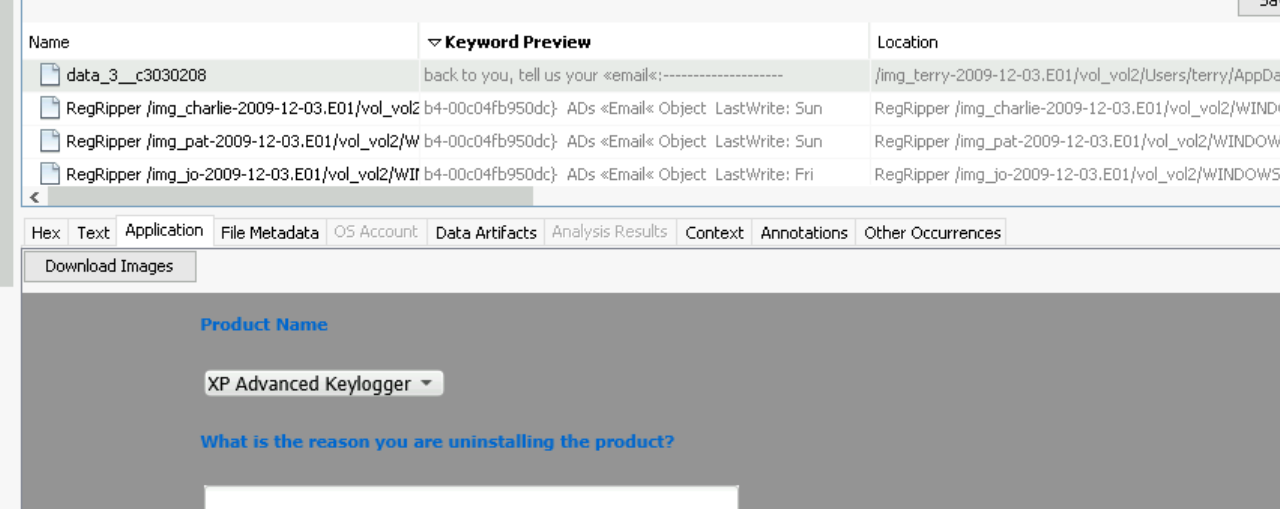


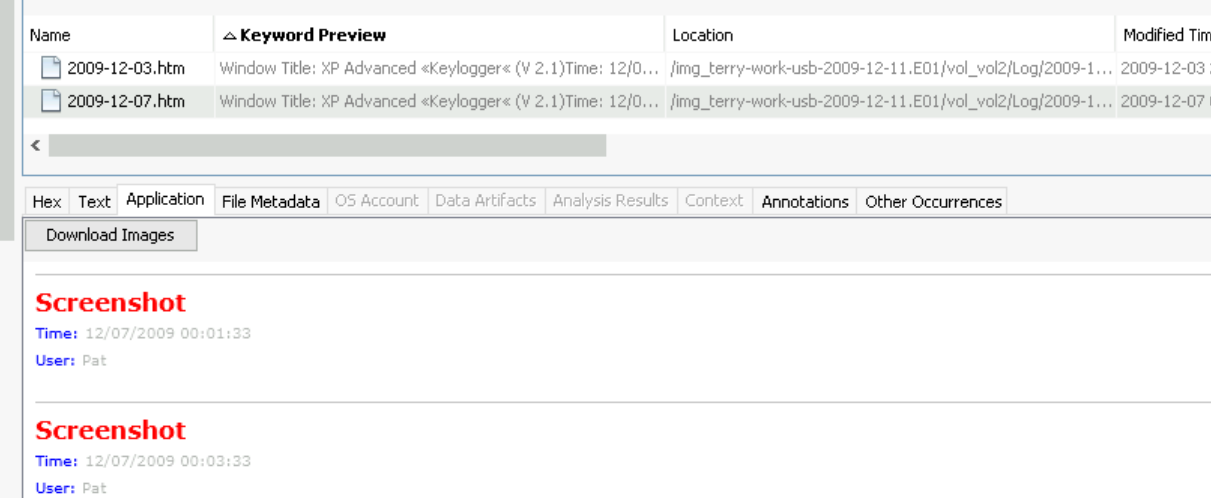


The email, [t93940@gmail.com](mailto:t93940@gmail.com) is Terry, we know this because he sent emails to his boss Pat from that same gmail account:



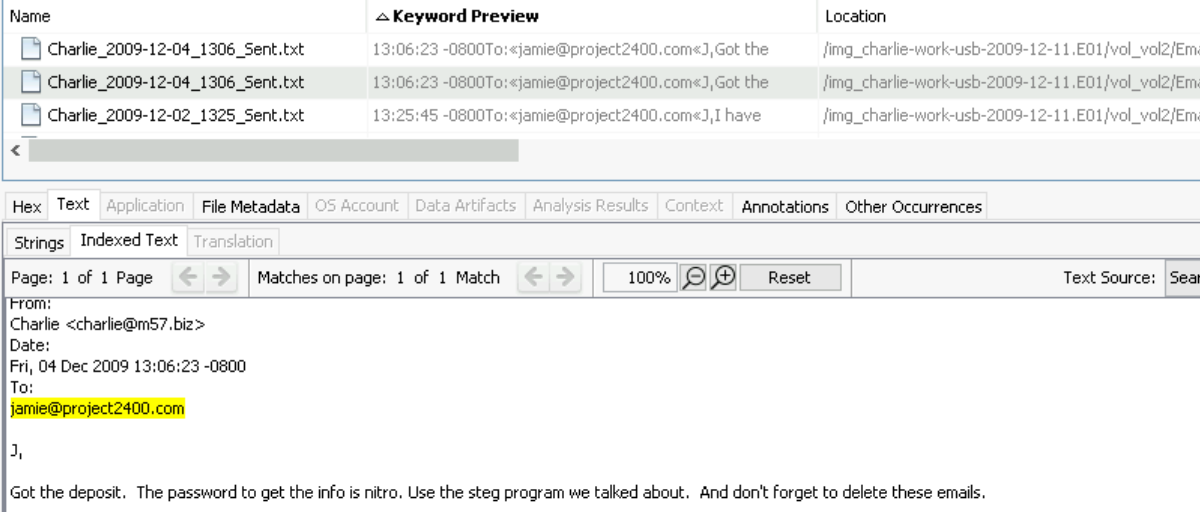
Terry is the primary suspect in this situation. Terry also installed a keylogger on his boss’s computer:

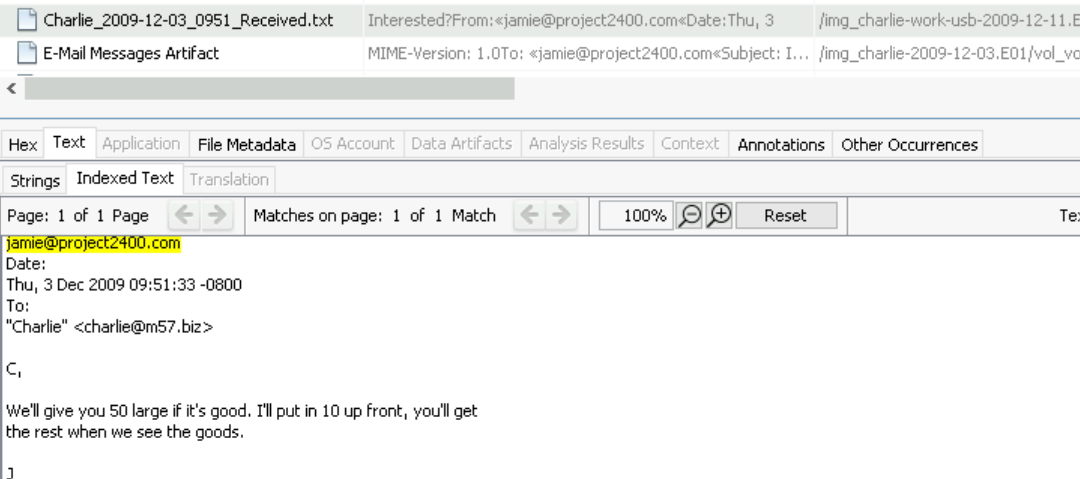


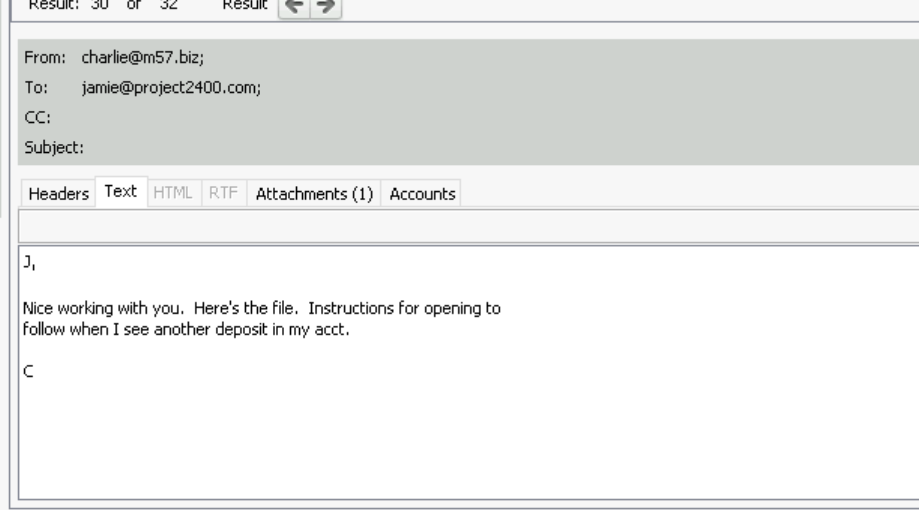


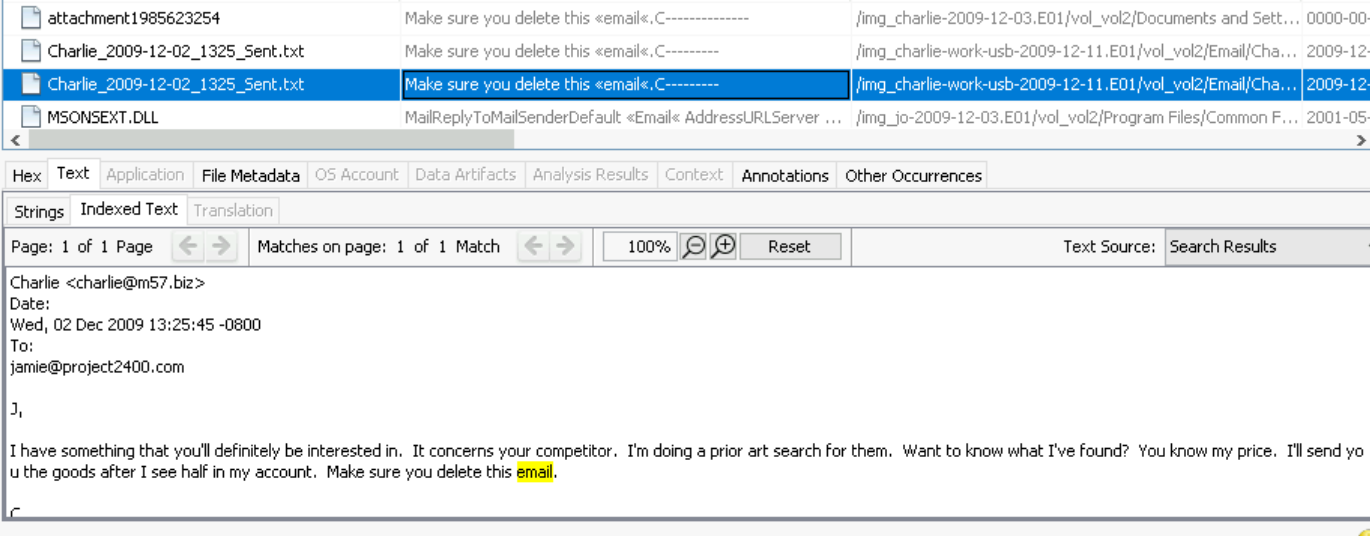
Part 3:

Data exfiltration seems to be done by a people in the organization. Charlie and Jo both had their instances. Charlie was selling details regarding their prior art research to another company’s employee:

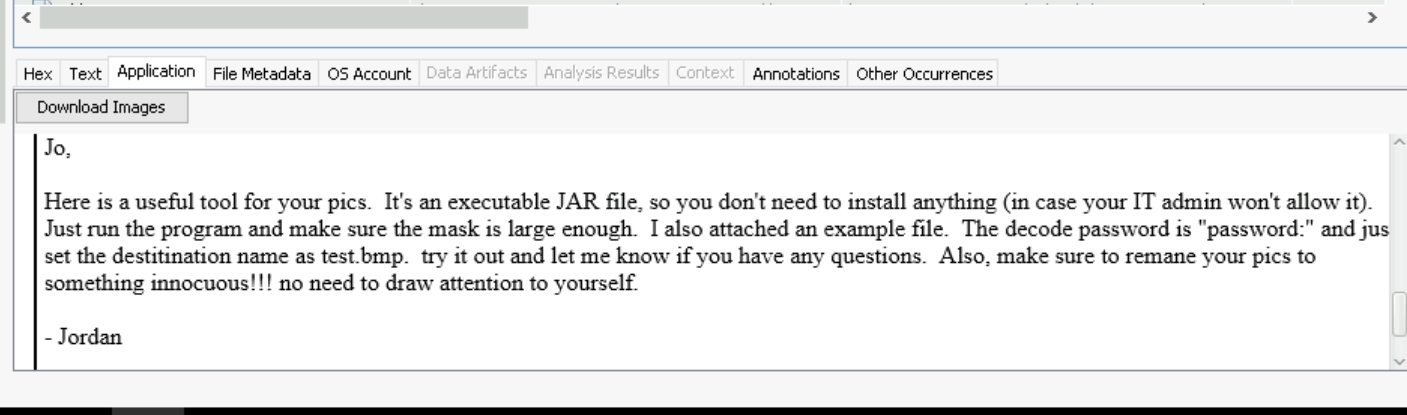


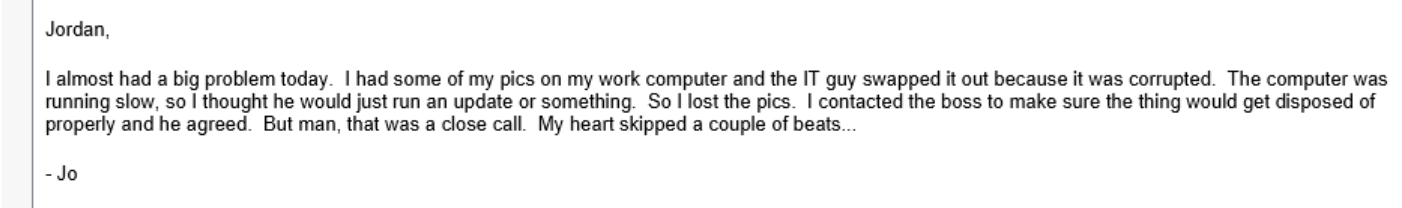


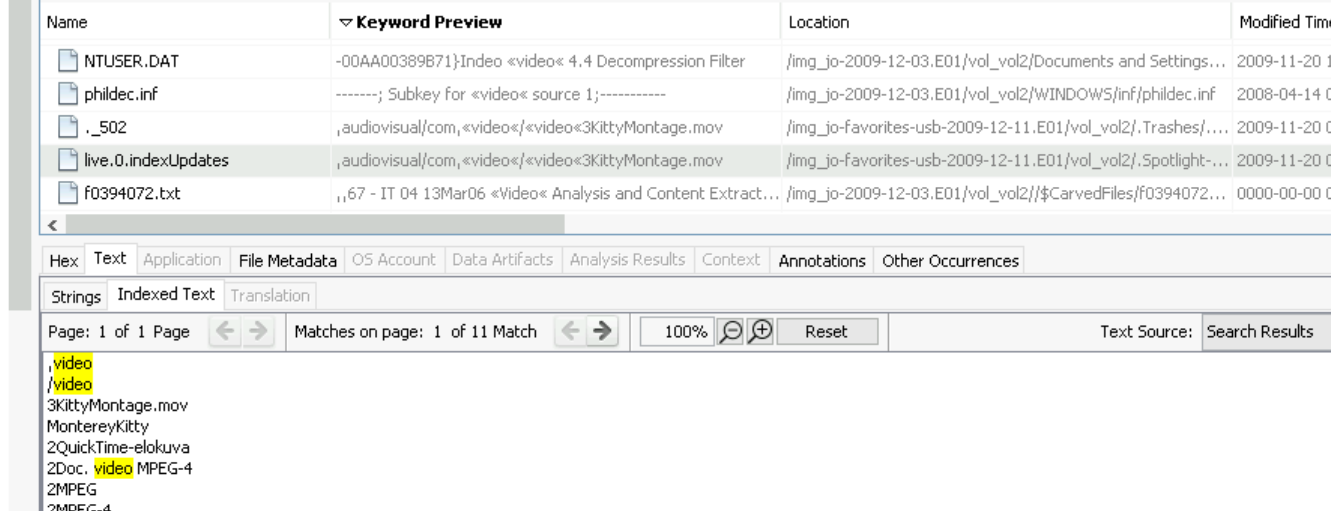


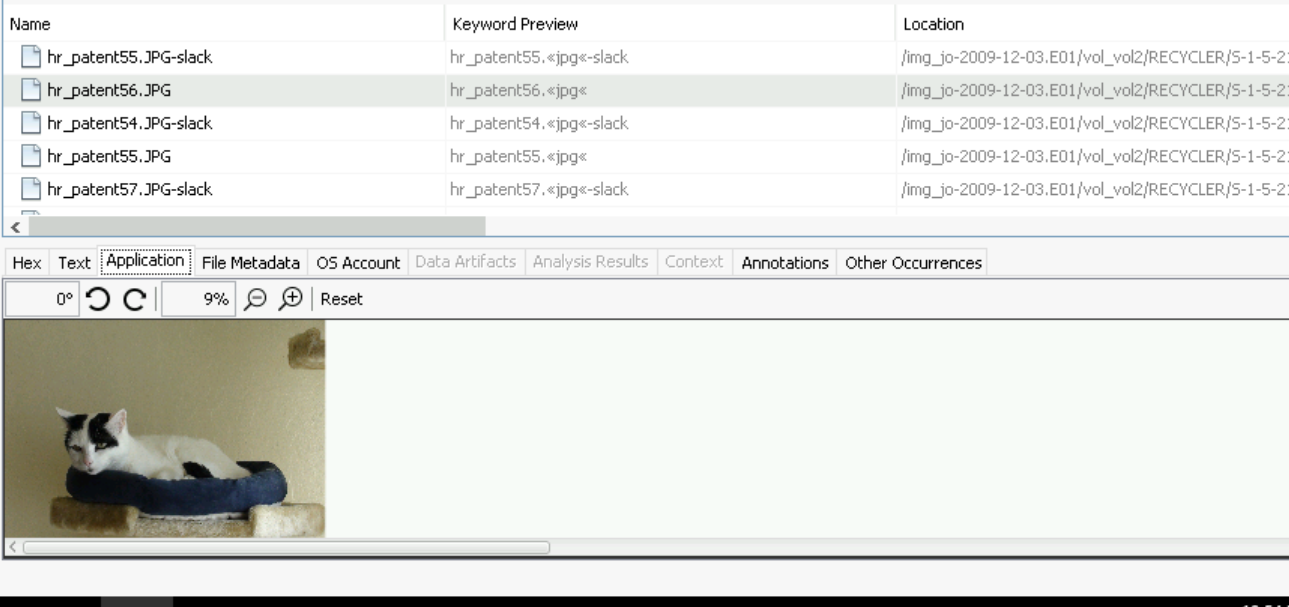


Jo on the other hand, was sending patents to an external user as was listed above <mailto:js9999sj@yahoo.com.> Jo also sent an email to Jordan regarding the fact that their computer was swapped by Terry and they almost were compromised. Jo was then instructed to hide the files and obfuscate them by changing file names.









This person most definitely can be charged, releasing company data and exfiltrating it to an external source is a crime. It is considered theft of company property.