CYBERSECURITY

Assessment 2

M57-BIZ

ILLEGAL DIGITAL MATERIALS

CAT PICTURES

HARIN RAMJI-21521277

CINIL CHERUKARA JOSE-23547150

SAPNA-22535954

EXECUTIVE SUMMARY

A functioning workstation purchased on the secondary market was found to contain illegal digital images and videos. The computer was originally owned by M57.biz, and it was used by an employee named Jo as a work machine. The police have taken possession of the computer and provided disk images from all the computers and USB devices found onsite at M57, including a USB thumb drive belonging to Jo. Students need to determine whether Jo is the owner of the illegal files, how the computer ended up on the secondary market, and if any attempts were made to hide these activities.

The objective of the investigation was to find out who the culprit was and also gather some evidence.

We as a group took all the files and scanned them via the autopsy app. We have found answers to all questions but not definitive enough to convict someone. The police need to investigate further upon our conclusions.

DIGITAL EVIDENCE EXAMINATION

We were handed 7 files listed below

Hard drive images from all workstations in the office:

charlie-2009-12-11.E01, jo-2009-12-11-002.E01, pat-2009-12-11.E01, terry-2009-12-11-002.E01

(Optional) RAM dumps from the machines taken during the police visit (mdd or windd images):

charlie-2009-12-11.mddramimage.zip, jo-2009-12-11.mddramimage.zip, pat-2009-12-11.mddramimage.zip, terry-2009-12-11.mddramimage.zip

Three company USB drives found on-premises and one personal USB drive seized from Jo:

charlie-work-usb-2009-12-11.E01, jo-work-usb-2009-12-11.E01, terry-work-usb-2009-12-11.E01 jo-favorites-usb-2009-12-11.E01

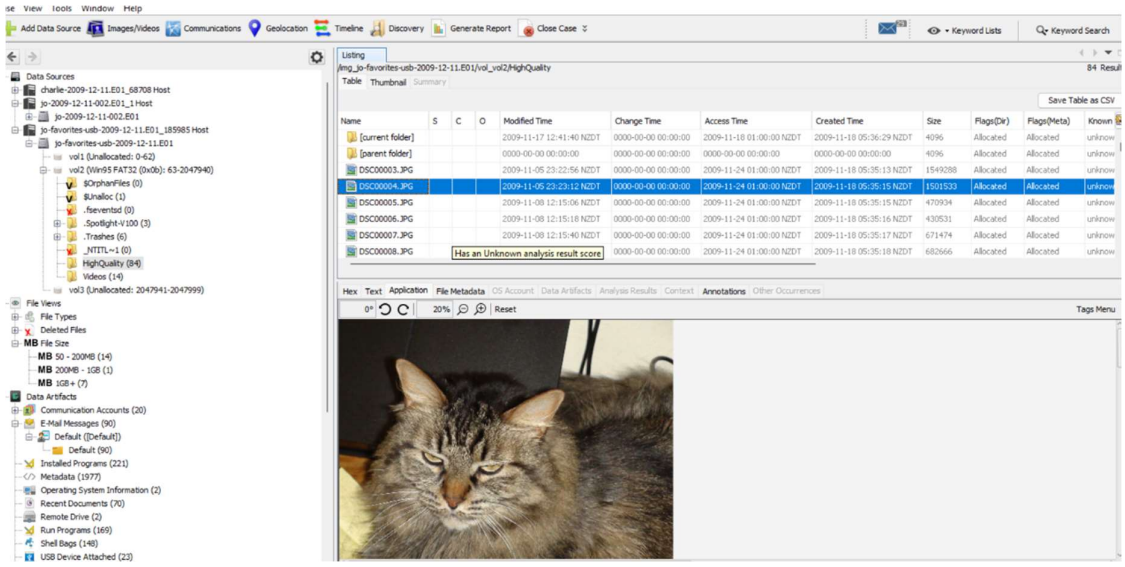
We used as a group Autopsy version 4.19.0

(https://www.autopsy.com/download/)

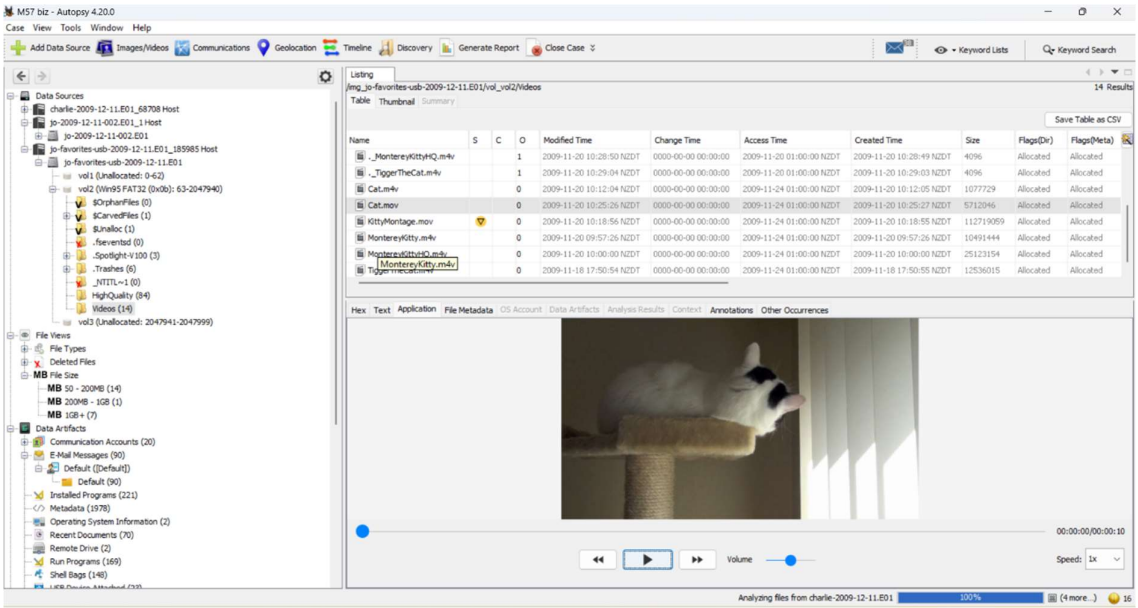
Which is an open-source forensics software. The advantages of using this software is that it brings all the data together in one solution and organizes is in a proper manner that helps forensics experts comb through evidence with ease but with precision. There is very low chance the software misses something however there is always a chance the human working with the software misses something.

ANALYSIS AND FINDINGS

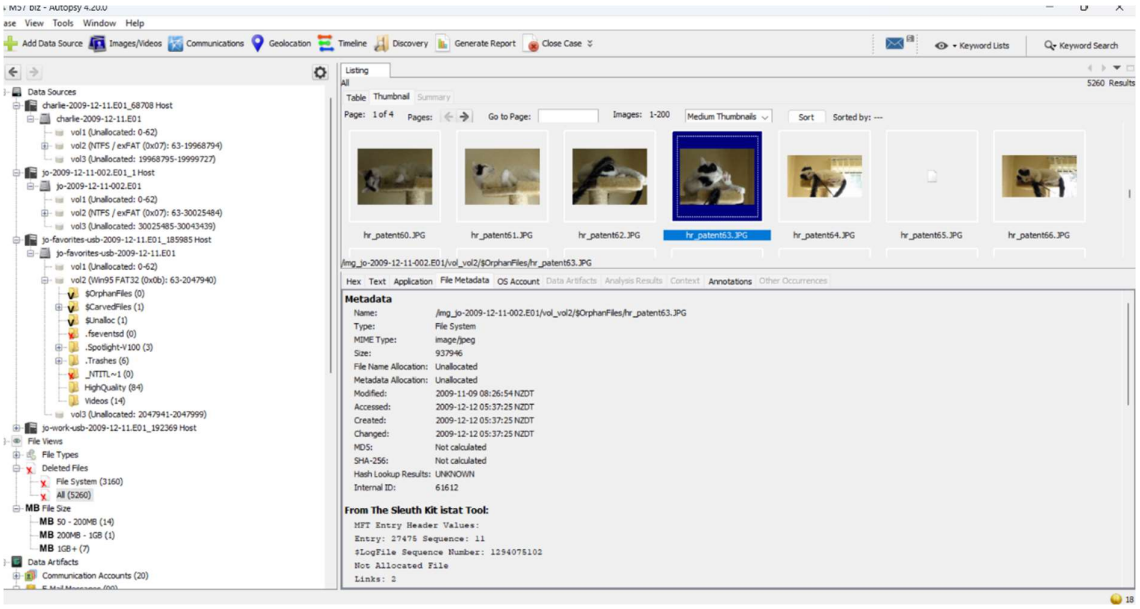
Below are some of the screenshots that provide some evidence. Below each screenshot would be a brief description of what it means and what we would like the police to do ahead.



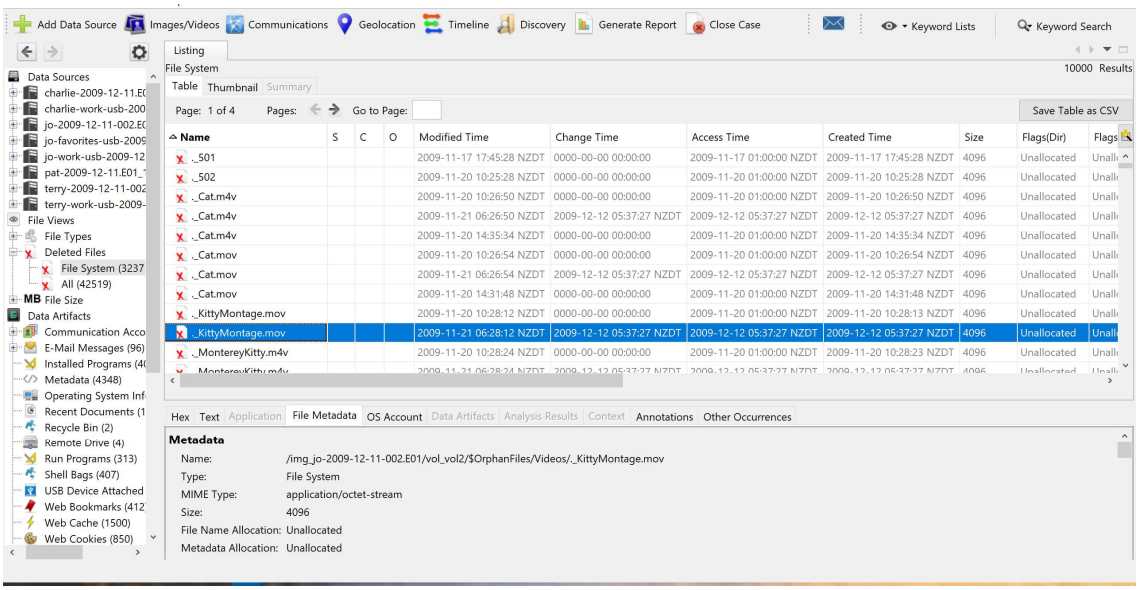
This is evidence we found on Jo's USB containing the illegal materials. As you can see it was created on 18th of November 2009 and was also accessed/opened on 24th November 2009.



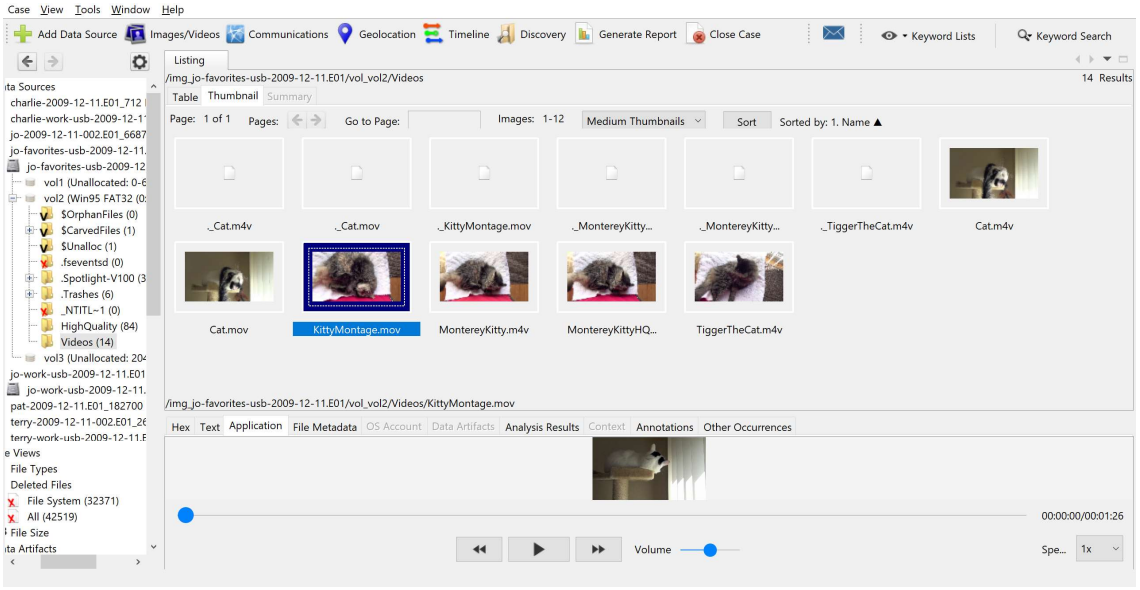
Another piece of evidence showing the illegal materials in jo's USB.



Further evidence pointing the finger at Jo.



This is evidence that an illegal file was in Jo’s computer and she deleted it. However, the software picked it up as it was not deleted properly. Find evidence below of us knowing that the mentioned video file is an illegal video file that now exists in the USB.

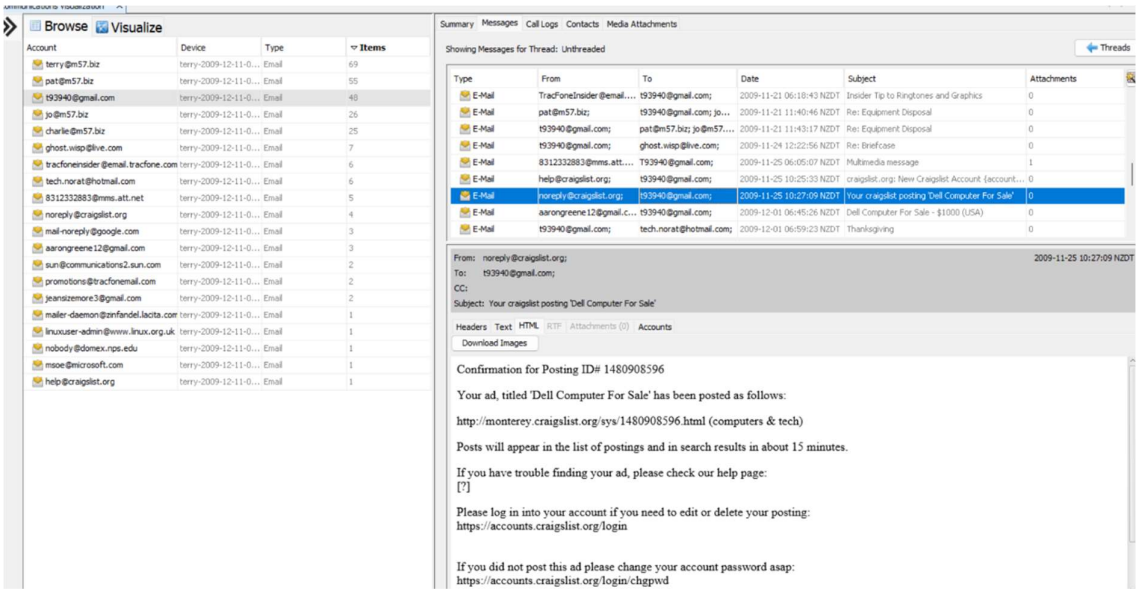


CONCLUSION

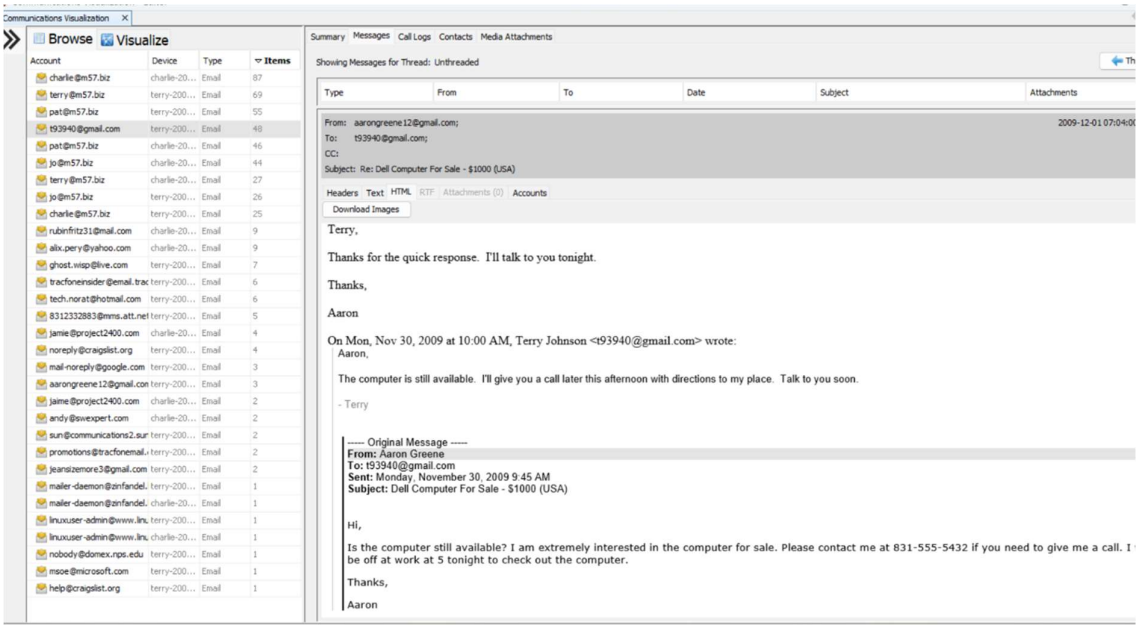
1. ***<u>Is Jo the owner of the illegal files found on the purchased machine? What evidence supports this conclusion?</u>*** **YES**

OTHER FINDINGS

2. ***<u>How did the computer come to be sold on the secondary market? Are there any indications of theft or unauthorised sale?</u>***

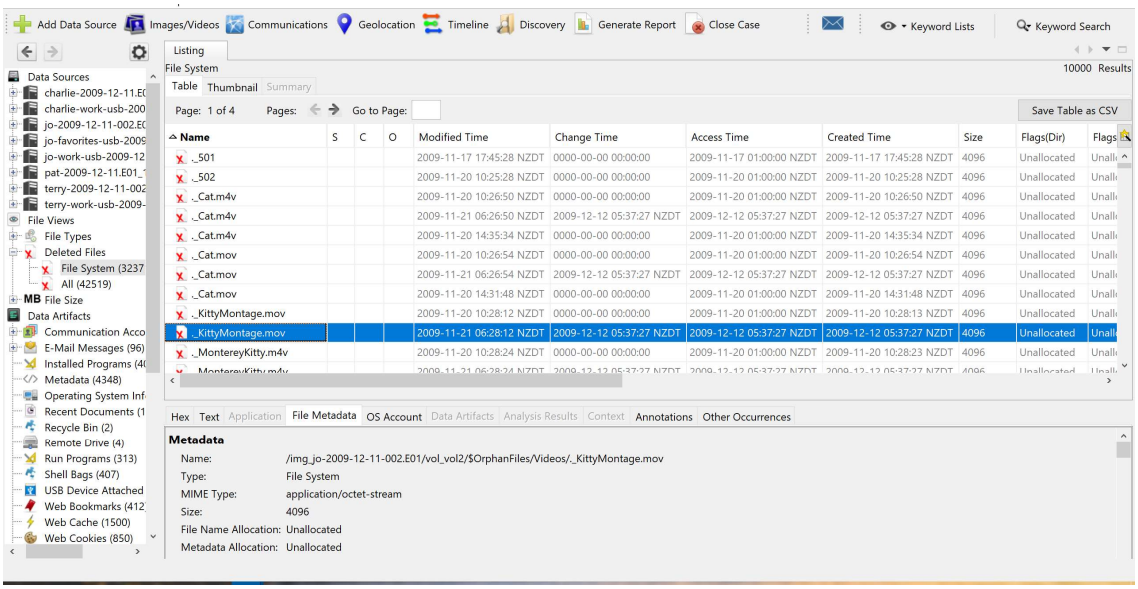


Terry's personal mail was the one used to create the listing of the pc on craigslist.



Above is also communication between Aaron(PC buyer who called the cops) and terry showing communication about an exchange of a PC. This shows that terry sold the computer on craigslist. However, we do not know whether it was approved by the CEO(Pat) or not. We would suggest the detective to question Pat whether he approved the sale or not.

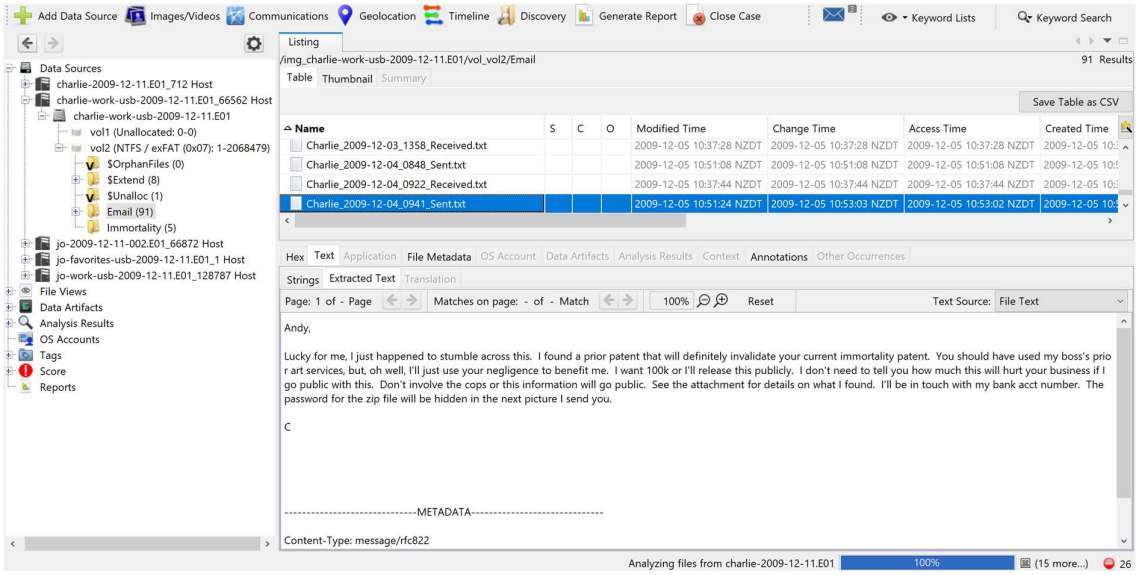
Were any attempts made to hide the presence of the illegal activities on the computer? If so, what techniques or tools were used?



This shows that jo actively tried deleting the illegal materials items from his work device.

Are there any other suspicious activities or files discovered during the forensic investigation of the disk images and USB drives?

We also found communications between Charli and the company competitor where charlie was trying to sell off information to the competition.



This image is evidence of an email from Charlie to the competitor (jamie@project2400)

A number of professional contacts and outside persons (friends of the employees) appear in this scenario. Who are they? Are they involved in any of the activities uncovered?

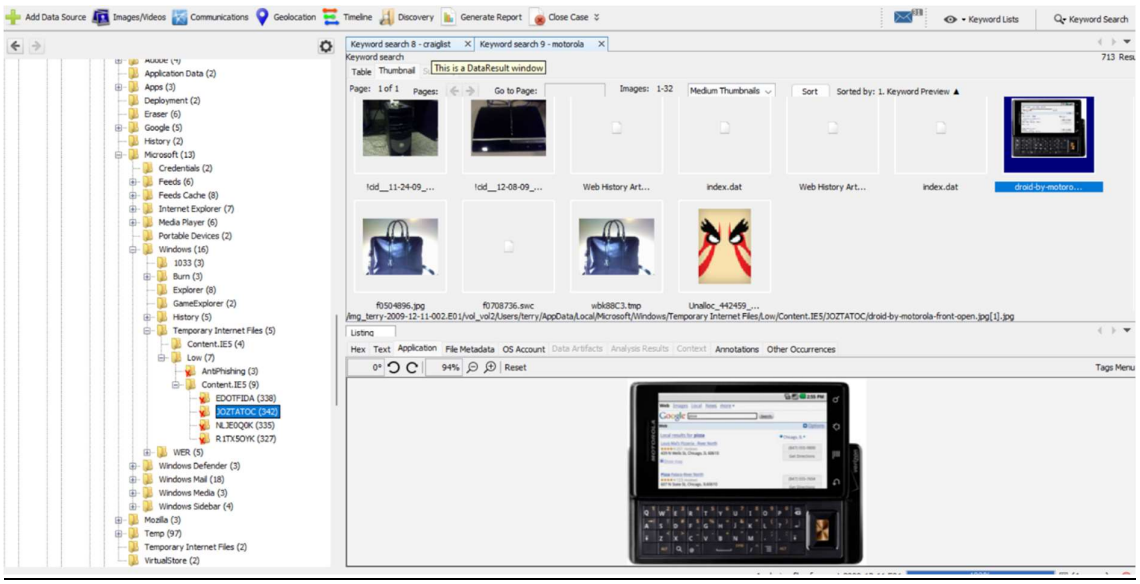
We have Alix Perry who seems to be Charlie's partner/friend and we have some communication between them.

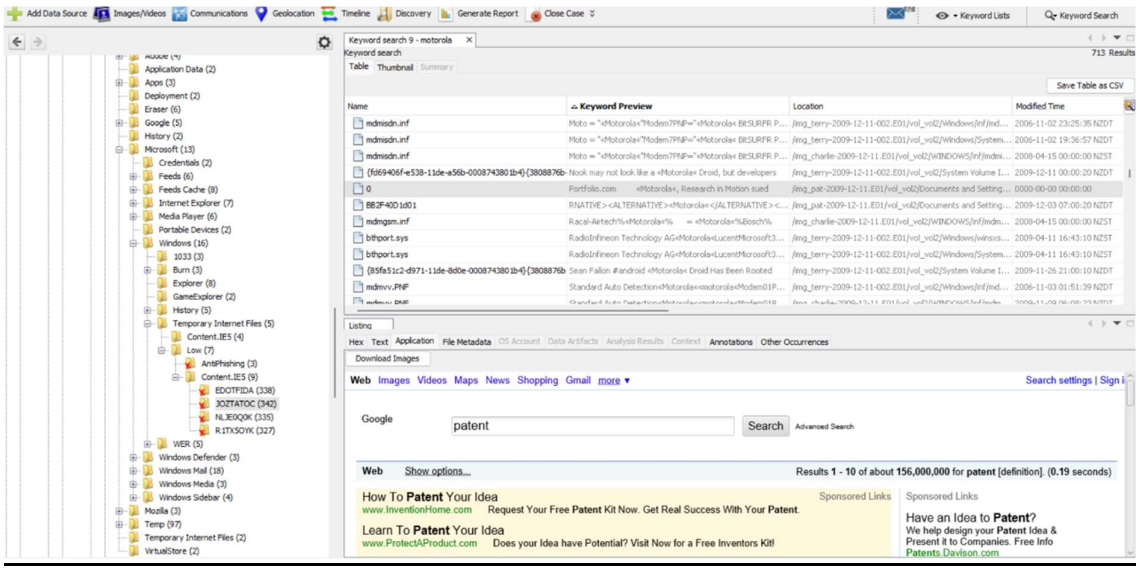
We have Jamie from project2400 which is a competitor and we have Charlie communicating with him trying to sell valuable info for 100,000 dollars. (Investigate further)

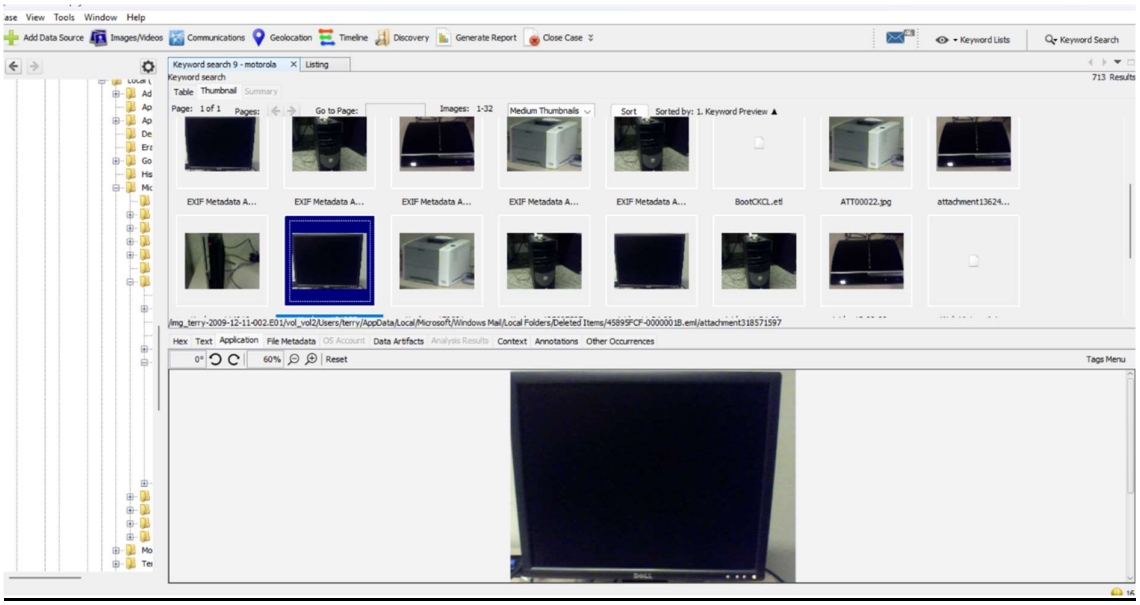
We have Andy who seems to be a client and we have some back-and-forth communication between Andy and Charlie although it's nothing serious.

Rubin fritz seems to be a friend of Alix and Charlie and there is some communication between all three

Note: Terry's phone is not available in the corpus. However, several files that originated from the phone exist somewhere in the corpus. Can you find them? Are they related to the case?







Terry’s mobile is a Motorola device that was used to take pictures for the online listing. This device also contains terry personal email. It does not help in jo’s case but it could be used as evidence when pursuing theft of company property (If PC was sold without Pat’s approval).

CONCLUSION

We as a team have looked through all of the evidence and can confidently conclude that the owner of the illegal digital materials is Jo. We also found evidence of other potentially illegal activities as highlighted above. As per stated above we need the detective to investigate further and check whether Pat had given permission to Terry to sell the computer or not. If permission was not given then it could be considered theft. We also found evidence of corporate espionage which could be investigated further.