National Gallery Incident-Forensic Investigation

Name

Institutional Affiliation

National Gallery Incident-Forensic Investigation

**Overview of the Scenario**

Based on the 2012 Nationally Gallery DC Scenario, which revolves around an employee of the National Gallery DC Art Gallery. Tracy who works as supervisor at National Gallery is an acquaintance of Carry. In the process there is money transfer between Carry and Terry, which becomes suspicious, especially on the issue of items transferred, though not outright illegal The whole scenario depict the criminal plans for both theft and despoilment, and this attracts performing investigation

**Introduction**

Forensic extraction and evidence examination on the mobile device may differ on each mobile device. Nevertheless, with a consistent examination process to be followed will be critical in assisting the examiner and ensuring the evidence extracted from each phone is well documented and that the outcomes are repeatable and defendable. Ideally, there is no well-established standards process that is meant for mobile forensics (Phillips et al., 2013). Nevertheless, mobile phone evidence extraction process can follow various defined steps, which include intake, identification, preparation, isolation, processing, verification, documentation/ reporting, presentation, and archiving. All methods applied in the data extraction from the mobile devices should be properly validated as well as documented. In this assignment, it aims at extracting evidence from Carry’s Phone through a forensic image of the Samsung GSM GT-I9020a Nexus S (Android) that was collected on 13th January, 2016.

Based on the evidence intake phase this involves request forms and paperwork in documenting ownership information and the kind of incident that mobile device was involved in, and outlining the type of data the requester is looking for. . Additionally, developing specific objectives of the preliminary evidence extracted from Carry’s phone must take place. Such details that are part of the incidences revolves around Samsung mobile phone, which is Nexus 5, which uses Android 2.3.4. In the identification phase forensic examiner should focus on identifying the following details of examination of the mobile device, which include: the legal authority-in this case the forensic expert, examination goals, removal and external storage, and other potential evidence sources.

**Forensic Methodology**

The forensic investigation adopted digital forensic analysis methodology. Digital forensic analysis methodology is an approach that apply scientifically derived and proven approaches in the preservation, collection, validation, identifying, analyzing, documenting, and presenting digital evidence deduced from the digital sources with the aim of furthering the reconstruction of events found to be crime-related. Understandably, digital forensic analysis methodology is based on various key elements, which include the use of scientific methods, collection and preservation of data and digital evidence, validation, identification, analysis and interpretation, and documentation and presentation (Delp et al., 2009). Based on this methodology, its process overview comprises of various steps, which include obtaining and imaging forensic data, forensic investigation, preparation/ extraction, identification, analysis, forensic reporting, and case level analysis. Based on the case under consideration, the investigator and forensic examiner must decide how much of the process is to be completed in every stage. Ideally, the whole process is iterative in nature hence the investigator and examiner must put this into consideration and decide how many times to repeat this process.

**Types of Evidences Files Provided**

Generally, in mobile forensics process steps that are important in obtaining different types of evidence. Based on the scenario in hand, the three main steps that are highly important include seizure; in this case, digital. Forensics operates on the principle that the evidence should be adequately preserved, processed and admissible (Catanese et al., 2013). Regarding the types of mobile forensics to be considered in this scenario, the following parameters will be used:

* Assessing the type of the phone (Make, Model, and Manufacture)
* Analyzing the operating system of the mobile device
* Assessing the encryption level of the device
* Assessing the availability of passcode/ pin code/ pattern

Based on the manual way of starting off with the forensic, the device must be browsed manually by forensic expert. The data on the phone can be directly seen or retrieved. This is a quick method since the examiner is well aware on the type of data to browse (Curran et al., 2012). Another approach is known as logical approach, which is a quick way of evidence extraction from the user files. In this case, data is extracted from flash memory. Other types of evidence that can be extracted can be derived from the file system of operating system-Android. Since it is the operating system that stores information relating to deleted files within the file system, the application of Digital forensic tool such as Autospy can be helpful in this case.

**Description of the Analysis of Each Type of file**

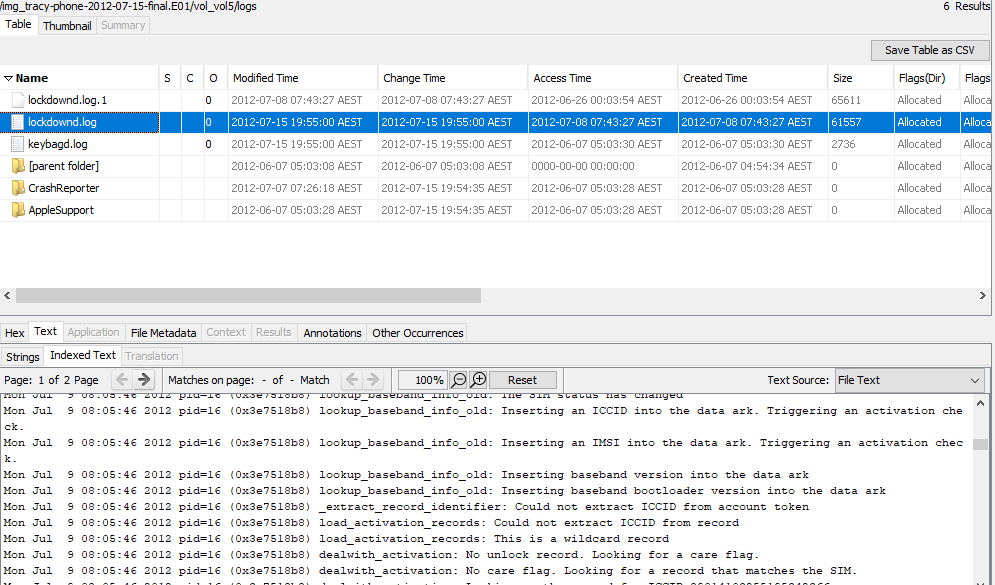
This assignment involves analysis of different fines that could provide evidence on the criminal liability of the suspects, who are Alex, Carry, and Terry. Additionally the analysis involves assessing image files for the Samsung GSM GT-I9020a. Some of the files assessed include email file with email conversation, images files, network traffic file, and various log files. Below is a PCAP log file which provides packet over the network.

Figure 1.

The above file has been captured using Autospy application and it searches for record identifies and data packets

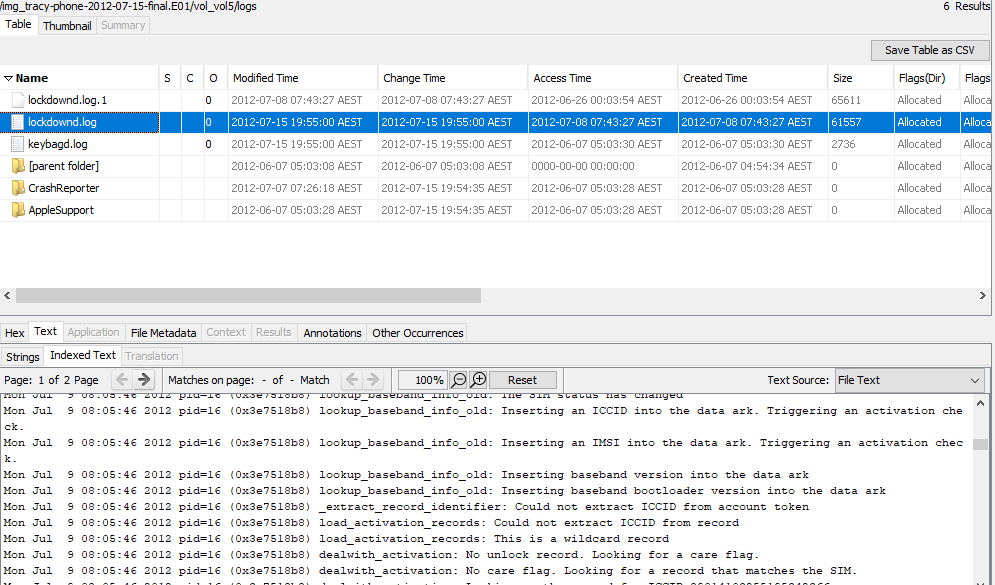
Below is additional PCAP file that analyze packet, which indeed is meant to show communication between different devices. As per now there is no evidence presented of any criminal operations or communication between Terry, Alex, Carry, among others

Figure 2

**Email Addresses and Associated Passwords**

In assessing email addresses used to do any communication between different participants, log files and email conversation must be assessed. This is critical in assessing email used in any communication. Assessing email log files play a critical role in analyzing any conversation between any parties. This section will be analyzed using both Autospy and Wireshark.

**Tracy Phone Analysis**

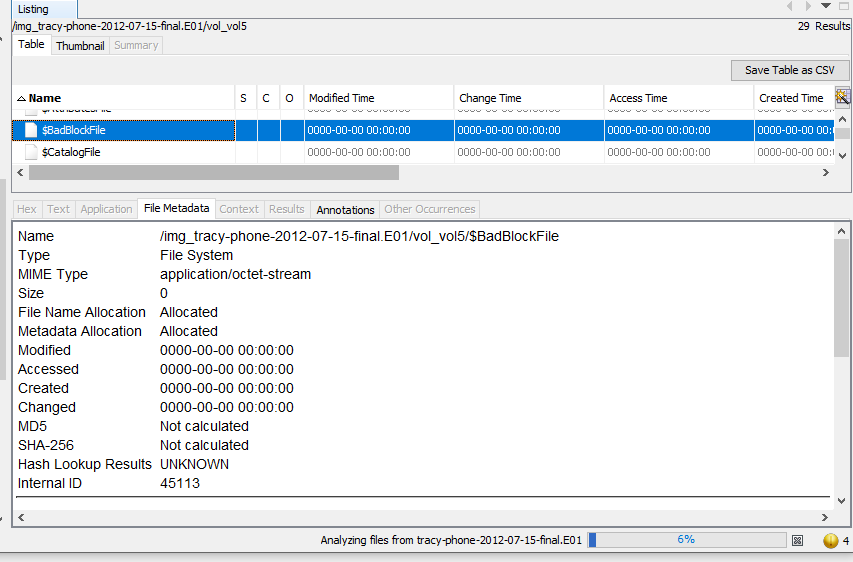
****The analysis below based on the file system of Android operating system of the Samsung phone. This file is ran for investigation purposes and check on the status and type of file system. The screenshot below provides an overview on the same

Figure 3

**User Pat**

Pat is Tracy’s bother based on the description given, and he is subject in this investigation. Even though he is not considered as an outright criminal, the details provided affirm that he walks the line so closely. Based on this analysis, the kind of information regarding Pat as retrieved via Autospy does not show any criminal liability. This can be affirmed through the files retrieved such as ***Noise\_Impact\_Assessment\_Spreadsheet.xls, BusinessPro.xls,*** among others. The diagram below present the analysis carried out.

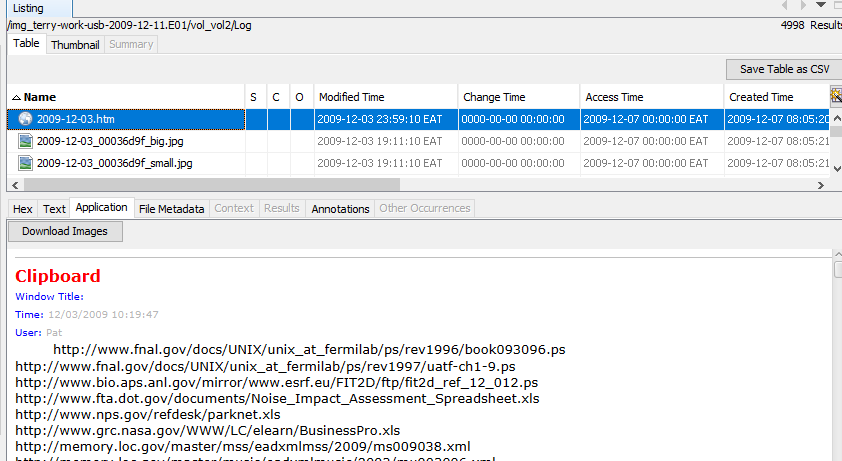


Figure 4

**Email Addresses and Passwords Used All the Participants**

Email has emerged to be an important tool for communication over the internet. Based on the email architecture, email system comprises of an integration of several software and hardware components, services as well as protocols which offer interoperability between the users. In email communication, it is a mandatory to use email address and password when logging in. In such operations which must be conducted over the internet, email system used must have a logging mechanism to keep track of all the operations taking in via the web server. Ideally, in digital forensic a full packet capture is paramount during the investigation of what is happening over the network based on a particular point in time. This provide an evidence on who was involved in an online activity, using which password, and IP address. However, following the TCP stream based on simultaneous application of SMTP and specific IP address can be used in identifying the address from email header tag. Supporting evidence during forensic analysis can be collected efficiently from the stored packets. If the password of the suspect was encoded using Base64, it means it easier to encode using UTF-8 show the actual password used while logging in. In this analysis, use of Wireshark has been used to provide analysis of email and password used in the incident of National Gallery DC.

**Email and Password as Used By Tracy In a Conversation with Joel**

The screenshot below has been captured from Wireshark, which is part of forensic analysis. This captures the email communication between Tracy who is company systems administrator and Joel who is father of terry. This screenshot captures the source email address, password, as well as the password used during the communication between the two. As shown on the screenshot, the email belonging to the sender (Tracy) is [root@Tracys-MacBook-Air.local](mailto:root@Tracys-MacBook-Air.local) and password used as per the analysis done via WireShark is ***K@6yteec***.

Following email logs on the same, it appears this email was sent by SMTP server, where the server username tracysumtwelve logged in on 28th June, 2012 at 15:42:13 as described on the code except below. Notably, the email client application used by Tracy to send this email is Thunderbird as shown below.

***![LogKext Daemon starting up : Thu Jun 28 15:41:39 2012]***

***![User 'tracysumtwelve' has logged in : Thu Jun 28 15:42:13 2012] legalBee otou<del><del><del>utlothunderbird.com***

***<cmd>wya<del><del>hotmail.com***

***coralblue22<del><del><del>two<del><del><del><del>e<del>***[***uetwo@hotmail.com<tab>legalBee<cntrl>tthunderbir***](mailto:uetwo@hotmail.com%3ctab%3elegalBee%3ccntrl%3etthunderbir)

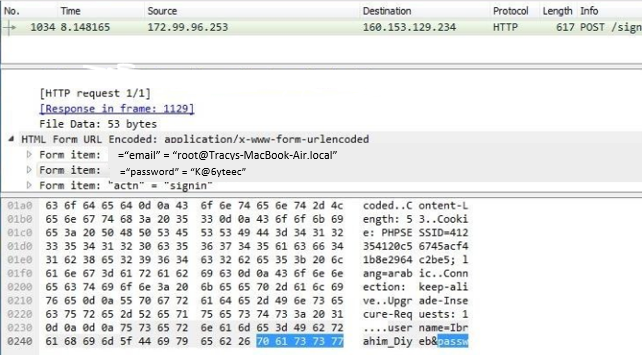


Figure 5

In analyzing the second email sent by Tracy to Joel there is something suspicious between in the conversation between Tracy and Joel. Tracy tells Joel to be careful not to lose the jobs. Something weird seems to be happening within Tracy and Joel. See the screenshot below

![User 'tracysumtwelve' has logged in : Fri Jun 29 10:33:25 2012] 9<del>legalBee <del><del><del><del>

Be careful! We have enough problems as it is, we can't get <del><del><del><del>be getting in trouble or losing our jobs. Nothing special has turned up here, but I am still keeping an eye out. We usually sot<del><del><del>start to host some interesting events this time of the year, I'm sure som

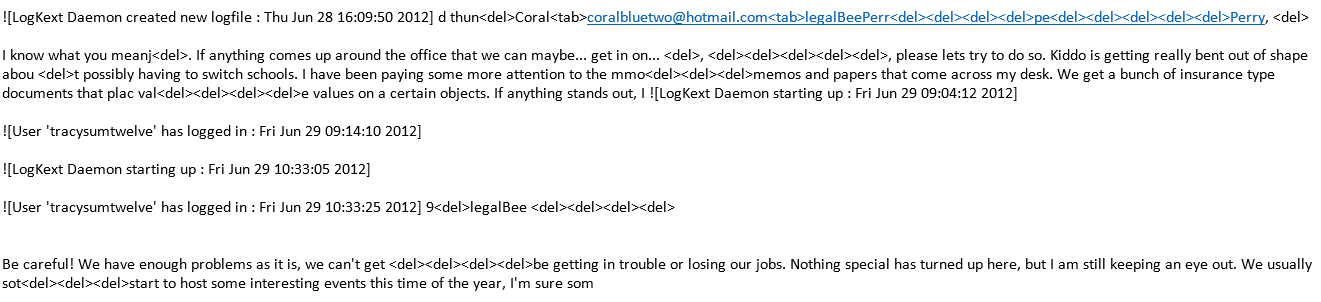
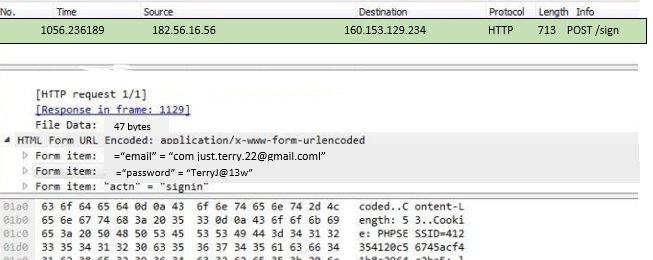
**Terry’s Email and Password**

Figure 6.

**Tracy Conversation with Pat**

Based on the screenshot below for the conversation between Tracy and Pat, the email that pat used has been identified as [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com) and the password has been identified as kUP@t12. However, there is no suspicious conversation between the two, which could lead to prosecution of both. Forensic analysis only show keyword serve of the email, hence no criminal issue to link them with. The screenshot below show a capture based on the forensic analysis and investigation carried out

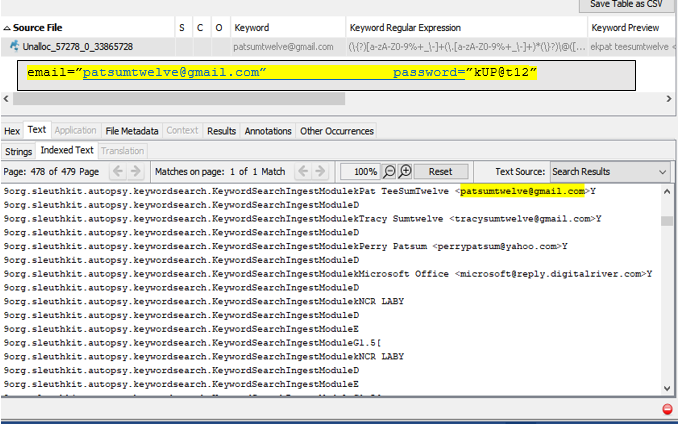


Figure 7

**Timelines of Data Extracted**

In the forensic investigation carried out, the data extracted from the logs show different dates and times where various operations happened especially email conversations and storage of different data files. In this case Tracy is the main suspect, and most of the operations and conversations seems to have been initiated by her. Some of the data extracted include captures from network logs, email logs and conversations between the persons involved, among other things

1. **Network Logs**

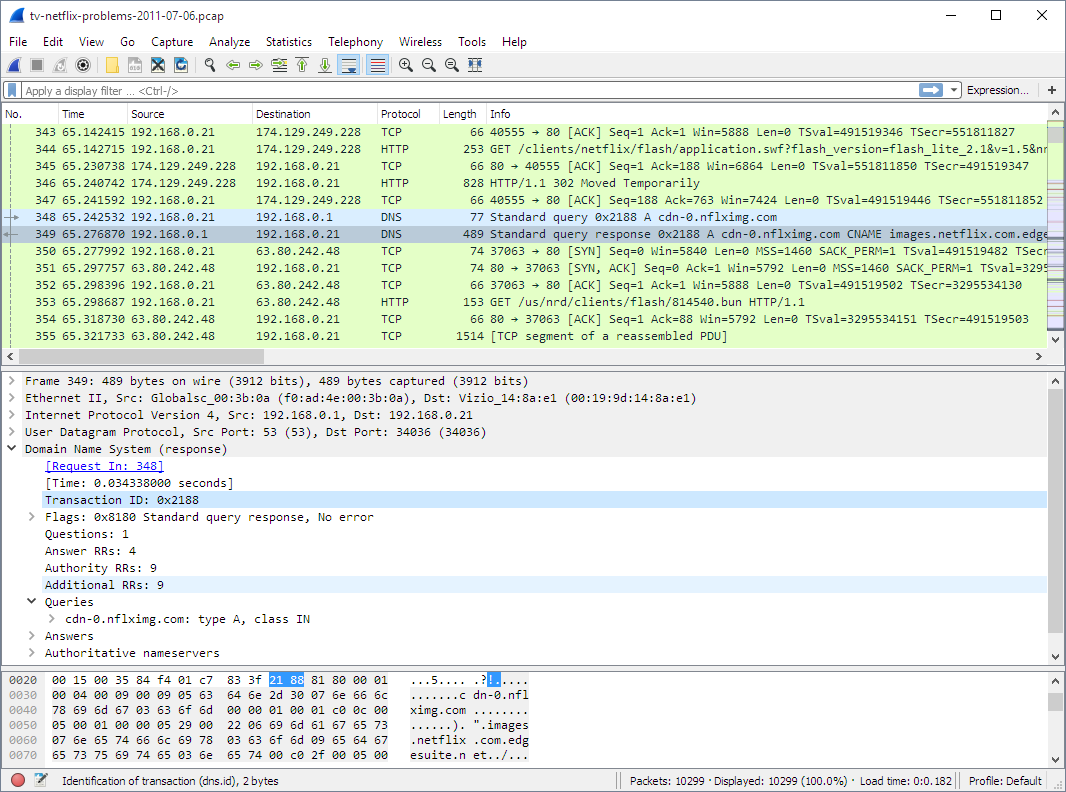
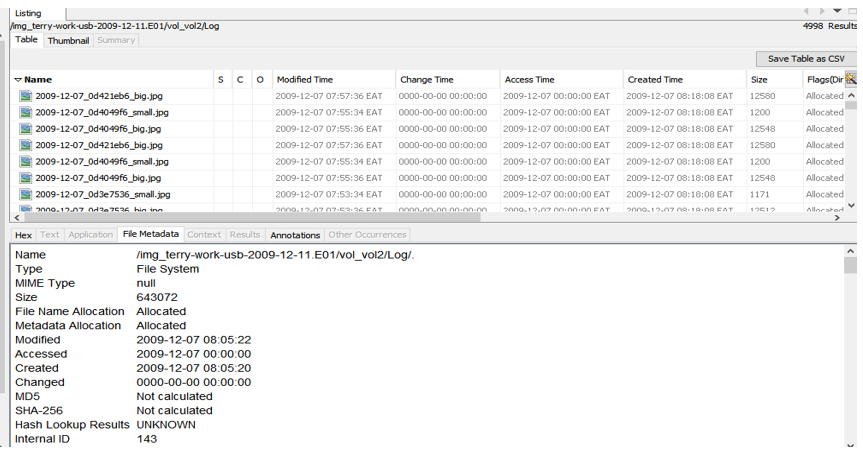
In digital forensics, network logs are used to analyze network traffic and event logs with the aim of investigating network traffic. In the analysis and investigation, it appears there have been there are many network operations that occurred which have been identified via log file showing the date. The screenshots below show some of the network log files

Figure 8:

The above screenshot display a screenshot of the network operations of by Tracy, which shows that she did her operations using Ethernet network and used different IP address when accessing and sending different files via the network

Figure 9

The screenshot above show network logs as captured from terry-work-usb-2009-12-11. This is an image file which was created on 2009-12-07:08:05:22

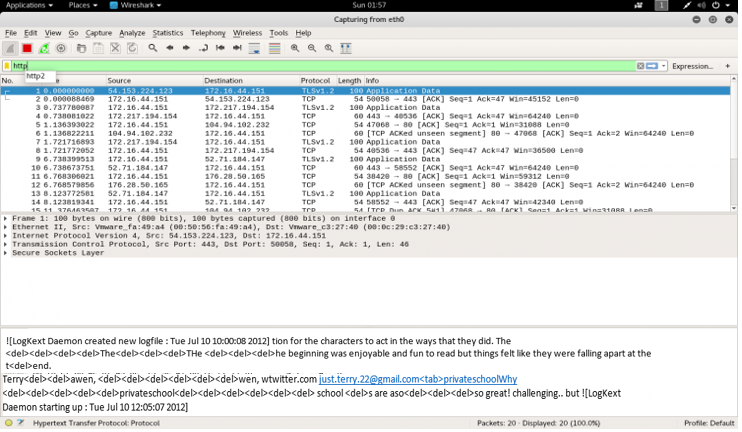
**Email Log by the Keylogger**

Figure 10

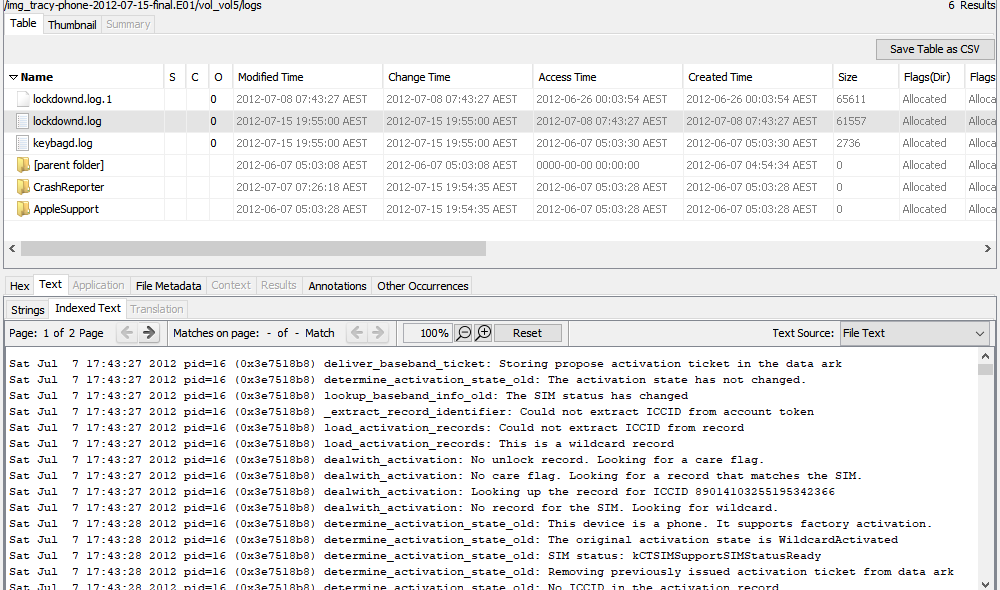
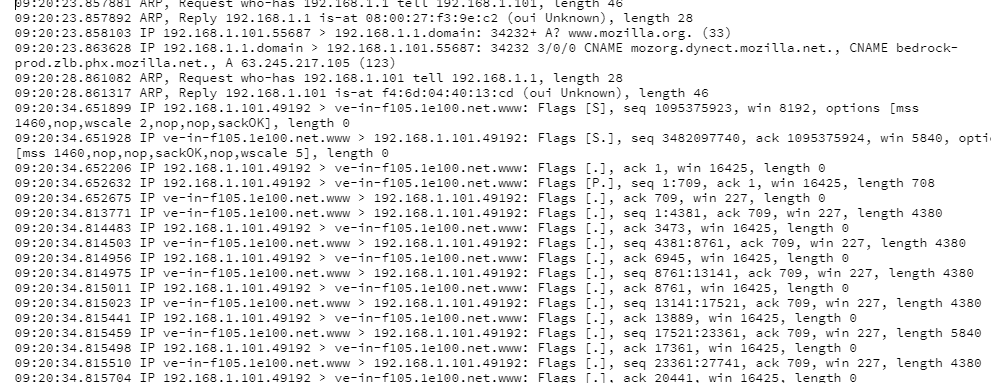
**Tracy’s Iphone Logs**

Figure 11

**Tracy’s Macbook Air Logs**

This log file provides an overview of the operations carried out by Tracy using her Macbook Air Laptop Figure 12

**Carry’s Tablet**

Based on the analysis of Carry’s Tablet, there are many files accessed including video files. The aim of doing this analysis is to asses if there was any criminal involvement by Carry. The files accessed does not show any substantive evidence that Carry was involved in National Gallery Incident. The screenshots below some of the analysis done by the forensic analyst

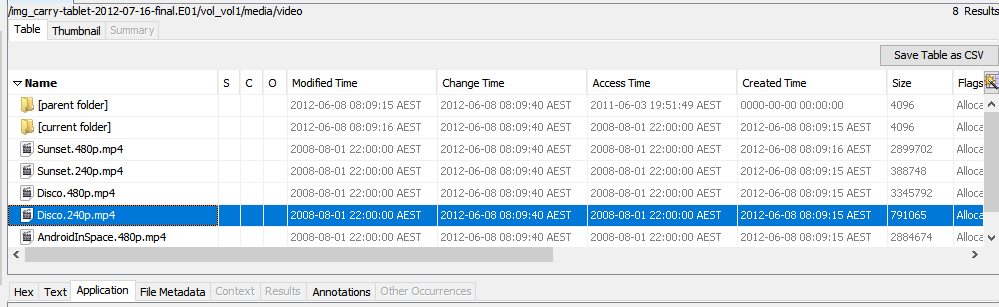
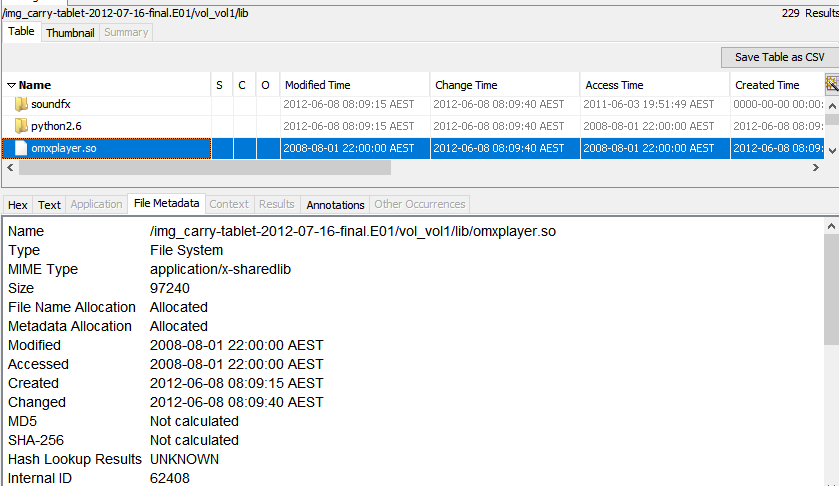


Figure 13

Additionally, Metadata access logs from Carry’s laptop can be described as shown on the screenshot below.



**Conclusion**

In summary, this assignment aimed at undertaking forensic investigation to ascertain whether Carry, Joel, Pat, Terry, and Tracy were involved in criminal activity associated with National Gallery DC Incident. Though there is no substantive evidence of involvement in criminal activity based on the forensic analysis undertaken, email conversant between Tracy and Joel has a suspicious content where Tracy tells Joel to be careful because not lose the job. However, this is not clear on if was a discussion on criminal activity or not hence no prosecution to any of the person.

References

Catanese, S., Ferrara, E., & Fiumara, G. (2013). Forensic analysis of phone call networks. *Social Network Analysis and Mining*, *3*(1), 15-33.

Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2012). Mobile phone forensic analysis. In *Crime Prevention Technologies and Applications for Advancing Criminal Investigation* (pp. 250-262). IGI Global.

Delp, E., Memon, N., & Wu, M. (2009). Digital forensics. *IEEE Signal Processing Magazine*, *26*(2), 14-15.

Phillips, A., Godfrey, R., Steuart, C., & Brown, C. (2013). *E-discovery: an introduction to digital evidence*. Cengage Learning.