Network and Internet Forensics (6G6Z1113_1920_9Z6) 1CWK25

Karan Nihalani - 17023122

Contents

Abstract & Introduction

A ‘synthetic analysis’, is to be carried out, encompassing more than one perspective within this investigation, given the evidence provided, including the additional set of evidence created for the investigation itself. Thorough analysis will be performed from the beginning, until the end of the investigation, allowing a variety of questions to be answered.

It is a necessary practice needed for forensic investigators employed at institutions, which require the application of in-depth examinations for certain cybercrimes that take place in the professional world. This document will, as mentioned briefly above, demonstrate the process taken through almost every stage in a digital forensics’ investigation, similar to a real-world situation. Including the ‘identification’ of the purpose of the investigation and ‘preservation’ of metadata, we’ll be able to navigate through the ‘analysis’ process, where “evidence should be extracted by interpreting the acquired information” and validated tools would be utilised to “conduct special actions and help retrieve additional information, such as deleted files” (R. Fahey, InfoSec Institute, 2019), whereas the ‘documentation’ is meant to be highlighting all these key areas of said investigation.

Throughout the report, the appropriate ACPO Guidelines are integrated into all aspects of the examination. For the collection and preservation of data, we can mention that ACPO Principle 1 will be applied, where “No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court” (ACPO, 2012). This will prevent the examiner from accessing and altering original data and will instead be forced to examine a copy of the data. The second ACPO Principle would be applied to both the analysis process and even the analysis results, as “In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions”(ACPO, 2012), highlighting the need to document and inform an external audience the reasons for accessing the data and the methodologies used to extract certain data from the copy of the original set of evidence. ACPO Principle 3 suggests that “An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result” (ACPO, 2012). This document reflects the third ACPO Principle’s purpose in allowing a third-party to view the process taken in analysing the evidence provided, along with clear techniques, with the final objective of a third-party achieving the same results. The final and fourth ACPO Principle, “The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to” (ACPO, 2012), is centred on the entire examination process, from start to finish and even more, around the forensic examiner himself/herself, emphasizing the idea that it is our responsibility that these guidelines have been followed responsibly.

Collection and Preservation

USB drive containing 3 evidence sets of Apache Logs ('Evidence_Set_1_Apache_Logs'), Chrome browser data ('Evidence_Set_2_Chrome') and Android navigation or activity metadata ('Evidence_Set_3_Android') are presented to us for the entire investigation.

Utilising a Linux machine, it's necessary extract the 3 sets of evidence into a directory. In the Chrome evidence, it is beneficial to combine the three '.zip' files provided, to save space and time, browsing through files. It allows us to create a copy of the evidence provided, preventing violating ACPO Guideline 1, avoiding working on the original data. Once located in the relevant directory, the `cat` command is used and the names of the '.zip' files are listed after, establishing the files to be combined, `cat NaIF-Coursework-Chrome.zip.001 NaIF-Coursework-Chrome.zip.002 NaIF-Coursework-Chrome.zip.003 > naif_combined_coursework-chrome.zip`, where the string right after, `> naif_combined_coursework-chrome.zip`, highlights the name of the newly created '.zip' file, consisting of three compiled files. After, files are extracted from the newly combined '.zip' file, 'naif_combined_coursework-chrome.zip', leading to the representation of three subfolders, 'Local', 'LocalLow' and 'Roaming'. To ensure the integrity of the '.zip' file, a SHA256 hash algorithm is performed, `sha256sum naif_combined_coursework-chrome.zip > naif_combined_coursework-chrome.zip.sha256`. Performing these hashes and comparing them will be able to "make it possible to detect changes in files that would cause errors" (Ubuntu, 2015). This process is carried out the exact same way for the other two sets of evidence. For the Android combination, `cat android_evidence.zip > naif_combined_coursework-android_evidence.zip`, resulting in the sub-folder called, 'data' and the hash, `sha256sum naif_combined_coursework-android.zip > naif_combined_coursework-android.zip.sha256`. For the Apache Logs, `cat apache.zip web_contents.zip > naif_combine_coursework-apache_logs.zip` and when extracted, outputs a 'var' folder, with 'html' data found inside. Another cat command had to be made use of before proceeding, `cat apache.zip > naif_combine_coursework-apache.zip`, because when attempting to combine both the 'apache.zip' and 'web_contents.zip' files, the access logs and error logs from the 'apache.zip' file are not combined into the newly created '.zip' file. This outputs the access and error logs and are then inserted into a newly manually created folder, called 'apache'. The hash is carried out similarly as done previously, `sha256sum naif_combined_coursework-apache_logs.zip > naif_combined_coursework-apache_logs.zip.sha256`, resulting in the SHA file 'naif_combined_coursework-apache_logs.zip.sha56' being made.

Generated on a Firefox browser is the additional evidence. Firstly, a folder, 'Coursework-Evidence-Firefox' is created, where the resulting forensic data is stored. Using '7Zip File Manager', and navigating to the 'AppData' folder, where three subfolders are located, 'Local', 'LocalLow' and 'Roaming'. Within these, there is a folder, named 'Mozilla'. An archive for each is created. The 'Local' folder is entered and on 'Mozilla', the 'Add' option is selected, allowing the user to change the location to the 'Coursework-Evidence-Firefox' folder. The name of the folder is re-named to 'MozillaLocal'. Every other folder is left as default and the same steps are repeated for the other two subfolders, outputting, 'MozillaLocal.7z', 'MozillaLocalLow.7z' and 'MozillaRoaming.7z'. The hashing of these is carried out where the option 'CRC-SHA' is selected, when right-clicked and then, hash SHA-256 is selected. This is then saved in three different text files, 'MozillaLocal.7z.sha256.txt', 'MozillaLocalLow.7z.sha256.txt' and 'MozillaRoaming.7z.sha256.txt'.

Analysis Process

Analysis is begun with Chrome data. Within the evidence, '.sql' files are provided. A program, 'DB Browser for SQLite' allows the analysis of '.sql' files, while searching for data and queries within these files.

Through 'Local', 'LocalLow' and 'Roaming', 'LocalLow' and 'Roaming' folders are found empty. 'Local' contains information about the activity the suspect carried out and it's revealed that it contains many different folders and files. The 'Default' folder contains most browser metadata, and some files containing important information are, 'History' and 'Login Data'. As Chrome does not display file extensions when looking into browser data, the command, `file *`, is input at the terminal when in the 'Default' folder directory, allowing us to have knowledge of all extensions of every file. Out of all files, most of them, are determined as SQL files. Another precaution is that Chrome hides some files, that can be crucial, leading to data being ignored, causing gaps within results. To manage this, there is an icon with three lines, displaying a menu with options. One of the options, 'Show Hidden Files' is made sure to be selected.

The file 'History.sql'. Within this '.sql' file, the table 'urls' is selected. It contains URLs of the websites visited, 'title', which is the description of what was searched, 'visit_count', highlighting the amount of times the site was visited and the 'time' field, representing the date and time the websites were searched and accessed. The 'time' is not represented as "dd/mm/yy" format, but instead, it is shown as the number of microseconds since the 1st of January 1601, therefore an SQL statement is input, `SELECT id, url, title, datetime (last_visit_time / 1000000 +(strftime ('%s', '1601-01-01')), 'unixepoch') FROM urls`. The statement outputs a table with the fields, 'id', 'url', 'title' and the 'last_visit_time' with the recognisable date and time. It is indicated that all of the searches were performed on the same day, on 23rd September 2018, At first, there are 5 different websites visited for "chicken recipes", whereas for the rest of the searches, the curiosity for the discovery of IP Addresses and the functionality of VPNs are investigated, provoking suspicion for malicious intent. Further searches include creations of a Gmail account, various locations explored on google maps, such as Costa Coffee places, communication with another person via Gmail itself and even searches for "manchester gloves" on amazon UK.

Analysing Apache Logs, at the terminal, the commands, `cat access_log | grep 200` and `cat access_log | grep 404` are used to separate successful connections from failed connections. The successful ones demonstrate a connection to an Amazon server and the '404' connections displayed the IP address 107.178.59.37, traced (using an online IP locator) to Kansas, USA and the address, 170.105.23.36, traced to Ontario, Canada. For the 'error_log' file, the commands, `cat error_log | grep 200` and `cat error_log | grep 404` are used, where the '200' connections are represented as "internal dummy connections" and the failed '404' connections demonstrate the IP, 107.178.59.37, belonging to clients in Miami, USA, highlighting the fact of a possible use of a VPN at the time.

Analysing the Firefox data is simpler, due to have Chrome data analysed previously. Opened in the same program, the file, 'places.sqlite' is opened from the directory where the 'Coursework-Firefox-Evidence' is contained and within it, the table, 'moz_places', displays the data needed to be analysed. As done before, a similar SQL statement to calculate the date is executed, `SELECT id, url, title, datetime ((last_visit_time / 1000000), 'unixepoch', 'localtime') FROM urls`, as Unix time is calculated from 1st January 1970, instead. The statement outputs the table with fields, 'id', 'url', 'title', and the readable 'last_visit_time'. All the searches are reportedly done on 23rd December 2019 and out of the evidence, it is made out that the suspect performed a straightforward search, firstly, looking up the city of Barcelona and locations in the city centre, such as "La Rambla". Further on, it is observed that the suspect is being suspicious, due to the search, "pipe bomb" and "pipe bomb design". More searches performed by the suspect

included the attempt in reserving flights from Manchester to Barcelona, a hostel room booking, the search for online bitcoin wallets and using the same technique of pasting google maps addresses online, it’s discovered that the suspect has planned trajectories in the city of Barcelona researched.

Analysis Results

Taking the server logs into account, the data seems to be coming from cities in the USA, emphasizing the idea of the use of a VPN, hence the intent to avoid police tracking their location when searching for terms online. It is less likely that the activity is not entirely innocent, as the searches demonstrate a pattern, almost like a schedule and not random curiosities, although it is slightly possible that it might be. The activity also showed caution in being caught by police and their avoidance too, while seeming to target the Costa Coffee in 263 Great Ancoat St., M4 7DB, Manchester as an attack location. The attack seems to have a goal to retrieve money, where the searches for "luxury destinations" make sense. The suspect even went as far as investigating the interior of this Costa Coffee and performing research into CCTVs and alarm systems, for the purpose of studying their functionalities. The overall consensus appears to be that the suspect was to attack the Costa Coffee when crowded, with the intent of receiving money. Then, escaping in his/her second-hand car, escaping the police arrive at the location, hence their search of "police response time in Manchester."

The additional evidence is determined to be much simpler, as the searches carried out on the browser indicate that they are all sequential, where the suspect is searching highly suspicious terms, such as, "homemade pipe bombs." The overall consensus that can be said is that the suspect plans to travel to Barcelona and stay at the 'Rambla One' hostel, very close to the centre and then proceed to carry out an attack at 'La Rambla' in Barcelona, at the most crowded time of day, with a home-made pipe bomb.

Reflection and Broader Implications

Progressing through the entire investigation, along with the evidence handed and the additional evidence, has helped to recognize the amount of caution and consideration needed to prevent the ignorance and neglection of underlying present data, which would ultimately cause a disruption and plot hole in the results. Furthermore, the need to preserve the authenticity and integrity of the original data handed, along with the preservation of manufactured data is prioritized over other aspects to abide to the ACPO Principles set for carrying out a successful investigation. It can be said that a sense of balance is needed, as well, in terms of analysing data, where a lot of data has to be inspected thoroughly, but with the precaution of not overanalysing data too much, as in the professional world, this can be viewed as a waste of time and insufficient precise data. Challenges presented in this investigation that can be applied to the real world, would be the problem of accusing a suspect because of a lack of innocence, as a suspect would be able to use a “malware defence” to reason with being accused.

To conclude, personal development was made in being more thorough in various aspects in the search and retrieval of evidence, leading to the influence of a sense of organization and order to be followed when examining it. This will prove to aid me in the work environment when being confronted with forensic challenges.

References

Ryan Fahey, InfoSec Institute (2019) 'Computer Forensics: Forensic Analysis and Examination Planning' [Online] [Accessed on 20th December 2019] https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/forensic-science/forensic-analysis-and-examination-planning/

ACPO (Association of Chief Police Officers) (2012) 'ACPO Good Practice Guide for Digital Evidence' [Online] [Accessed on 20th December 2019] https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Ubuntu (2015) 'HowToSHA256SUM' [Online] [Accessed on 22nd December 2019] https://help.ubuntu.com/community/HowToSHA256SUM

NRAO (National Radio Astronomy Observatory) (2019) '7-Zip File Manager — NRAO Information' [Online] [Accessed on 23rd December 2019] https://info.nrao.edu/computing/guide/file-access-and-archiving/7zip