J103563

by ABDELRAHMAN ABDELWAHAB

Submission date: 08-May-2023 05:23PM (UTC+0100)
Submission ID: 205187979
File name: J103563_963454_105755146.docx (2.25M)
Word count: 3811
Character count: 20388

Digital forensics report for Thornton Software House (TSH)

Table of Contents

1. An overview

1.1 Introduction:

Following the post intrusion request of TSH company to investigate for a possible data breach that may have occurred. TSH company has provided a detailed information on the infrastructure of the company and by analysing these data it can be suggested that there are possible vulnerabilities in the infrastructure. However, all the possible scenarios were taken into consideration and will be discussed in the following lines.

1.2 Possible scenarios of the infiltration:

1.2.1 SSH

The use of secure shell client should be based on a safety criterion, for example, the criteria mentioned by Miller (2022), it is suggested to use public and private keys so the service can be immune to some extent to brute forcing attacks. However, according to Turner (2023), employees might not be cautious enough in the way they handle the keys by leaving them exposed. Additionally, if an employee left the company, he would still have either the keys or the passwords, so they must be changed periodically. In addition to the number of employees and the devices the company has, there will be variety of keys stored in central database which can be difficult to maintain. The criteria also suggest against allowing remote root privileges which might be one of the scenarios to consider since the intruder can gain access to the password and shadow files.

1.2.2 DNS poisoning and VPN

DNS poisoning can be a possible scenario by misleading the users into browsing fake websites instead of what they are they are used to browse in daily basis (Ec-Council, 2016). The company also uses VPN which is according to the National Cyber Security Centre (2019), have various vulnerabilities especially the service provided by Pao Alto, Fortinet and Pulse Secure. For example, allowing the intruder access to files containing the login credentials which can be used to gain access to the internal devices.

1.2.3 Centralized login

Centralized login is used to store logs in one file, and to enhance the way the system performs (Ec-Council, 2016). However, one of the possible scenarios and according to Ec-Council (2016), the server must be only used in executing the loggings by ensuring that there are no other services undergoing beside it. In addition, if the logs are not analysed in real time a threat might be warning to take over the system without realizing that for a long time and this is what has happened in this case.

1.2.4 Miscellaneous scenarios

Scenarios can also extend to virus attacks by changing how a device can behave, it can also be trojan horse attacks for capturing sensitive data (Ec-Council, 2016). Moreover, the attacker might rely on social engineering, for instance, using emails containing malicious malwares (Ec-Council, 2016). However, managing 35 devices working remotely is challenging and might be taken as an advantage, so the attack might be from an insider.

1.3 Information and resources to be requested from the company.

The allowed down time in the future steps if there was an eminent danger on the company will be requested from the company. Moreover, the email addresses and contact information will be requested as well. Accordingly, the VPN provider name will be requested to check if it is included in the vulnerable list mentioned previously in section 1.2.2. Likewise, it is

essential as mentioned by National Institute of Standards and Technology (NIST) (2006), to follow the company digital forensics policy which states the scope of investigation and the allowed tools to use because some tools might record sensitive information, for example using keystrokes.

1.4 Digital forensics process

After analysing the infrastructure of the company, digital forensics process will be implemented as demonstrated in Figure 1. Ken Zatyko process according to Sammons (2014), begins by taking the legal regulations into consideration and agreeing on the legal terms. However, since the devices belong to the company, then the contract signed by the employees should be checked to ensure if it states that the devices may be checked for security purposes. Additionally, while analysing the logs of router, firewall and network, if there is a need to request logs from the internet service provider it will require a warrant (NIST, 2006). In the second step, a chain of custody will be setup because as mentioned by NIST (2006), and Sammons (2014), this step is crucial to maintain the integrity of the evidence since its capture till being delivered to the court. Likewise, in each step of custody the evidence shall be labelled by a date, location, and the person in charge. Similarly, Ec-Council (2016), describes this step as proof against any alteration in the logs since data collection.

In the third step the two devices in question will undergo imaging and this copy will be used during investigations while the original copy of the data will be kept aside and secured to be handed to the court. According to NIST (2006), and Sammons (2014), the data must be imaged not just copied to include non-publicly accessible files, in addition to hashing the copied and the original versions and comparing them to ensure the integrity of the data. In the following step, the tools that might be used are illustrated in Table 1. In illustration, since the company uses centralized logs so it can be analysed using parsing tools for example Windows Event Viewer, besides analysing the suspicious traffic that went in between. Accordingly, imaging tools and malware analysis tools will be used. Based on the outcomes of these tools, a recommendation report will be built including the findings, and documentation will be made to ensure the credibility of the final evidence.

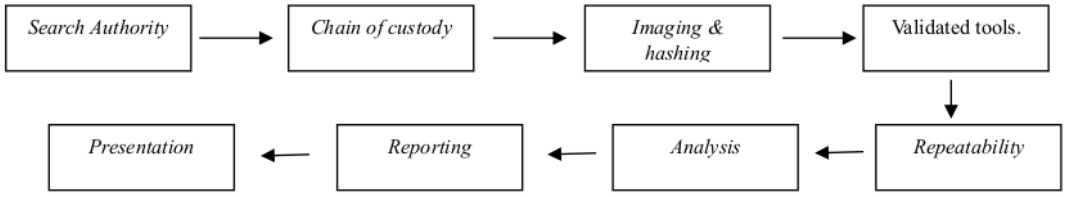

Figure 1. *Digital forensics process based on Ken Zatyko steps* (Sammons, 2014)

1.5 Tools to be used.

As shown in Table 1, all the tools that will be used in the following steps are included.

Tool	***Use***
Dumpit	*Memory imaging*
Autopsy and Volatility	*Analysing the image taken by DumpIT*
FTK Imager	*Disk imaging*
Detect it easy	*Static analysis*
IDA	*Disassembling tool*
dot Peek	*Decompiling tool*
Process hacker	*Debugging tool*

Table 1. *The tools which are going to be used in the following steps.*

1.6 Impact on the business

The impact on the business will depend on the severity of the intrusion and the burden will increase by moving forward to further analysis. For instance, any down time for now is not expected by the company, but it is suggested to isolate the two devices which had traffic in between. Additionally, there is a possibility of spreading malware properties in which the case will be to isolate all the devices in the network. However, the tests should be confidential to secure both the company reputation and the customers worries about their sensitive data.

2. Imaging Windows 10 device

After commencing on the digital forensics process and agreeing on all the terms, the scans began, and it was discovered that some of the security logs were not viewed in Windows event viewer. Accordingly, imaging of Windows 10 device will be done, which focuses on imaging the secondary and volatile data storages, alongside securing the original items (Hassan, 2019).

2.1 Memory Imaging

The company has indicated that neither the windows 10 nor the windows server 2019 were rebooted since the accident. Accordingly, as mentioned by Hassan (2019), if the device is still running, then the RAM can be imaged since it requires power to keep information. Additionally, Hassan (2019), states that there are two ways of doing it; the first way is to shut down the devices then starting to image the RAM, and the second way is to image it while the device is still powered on, which is more favorable, and which will be demonstrated in the following lines.

2.1.1 Benefits of memory imaging:

The RAM image contains information about the used applications, the internet browser history and sessions, instant messages, and passwords; that is why it is crucial to take the RAM image when the suspicious device is still running (Hassan, 2019). Moreover, RAM imaging can also help in identifying malicious processes or any unauthorized activities, so it is crucial to take the image as soon as possible.

2.1.2 Using DumpIt:

For imaging RAM, one of the quickest tools to do that is Dump It, as demonstrated in Figure 2, Dump It was used on Windows 10 device to take an image of the RAM, and by inputting (y) the acquisition has started. The process will take about 3-5 minutes to be done, and it will result in a 6 GB file which is the exact size of the RAM installed on the device.

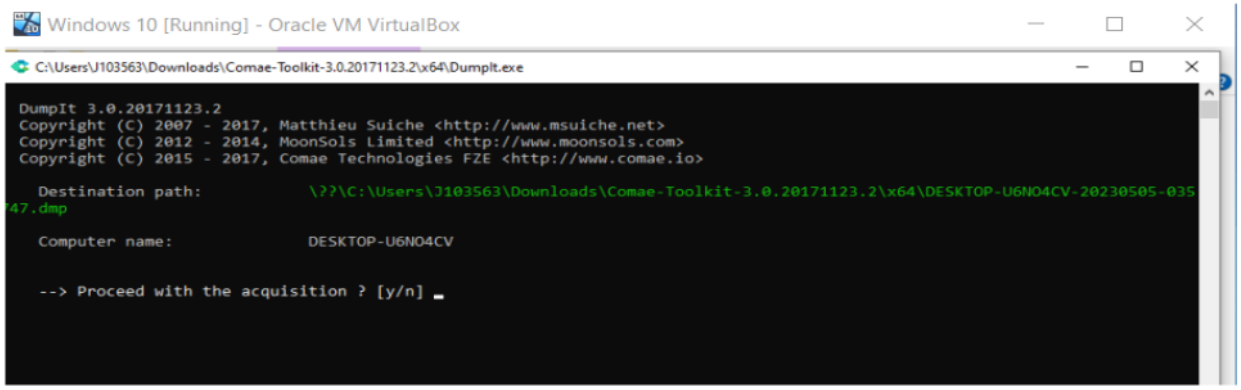

Figure 2. *Acquisition of the RAM*

2.1.3 Using Autopsy and Volatility:

The image of the RAM was then added to Autopsy to be analyzed and as shown in Figure 3, the hex view on the bottom shows that the user has browsed amazon website searching for a book, maybe this was an intent of finding countermeasure to secure the infiltration action.

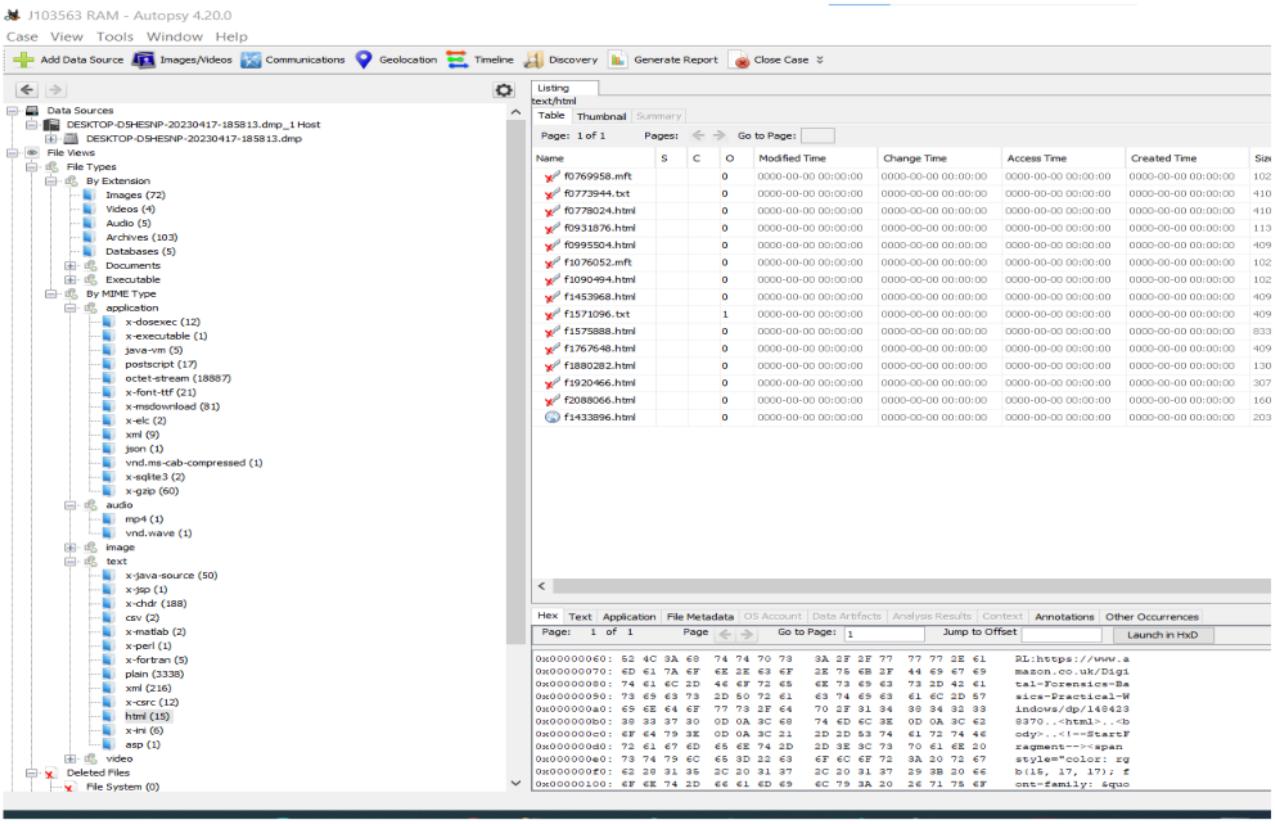

Figure 3. *The browsing history of the user.*

Additionally, in the application interface an email context can be viewed clearly as shown in Figure 4.

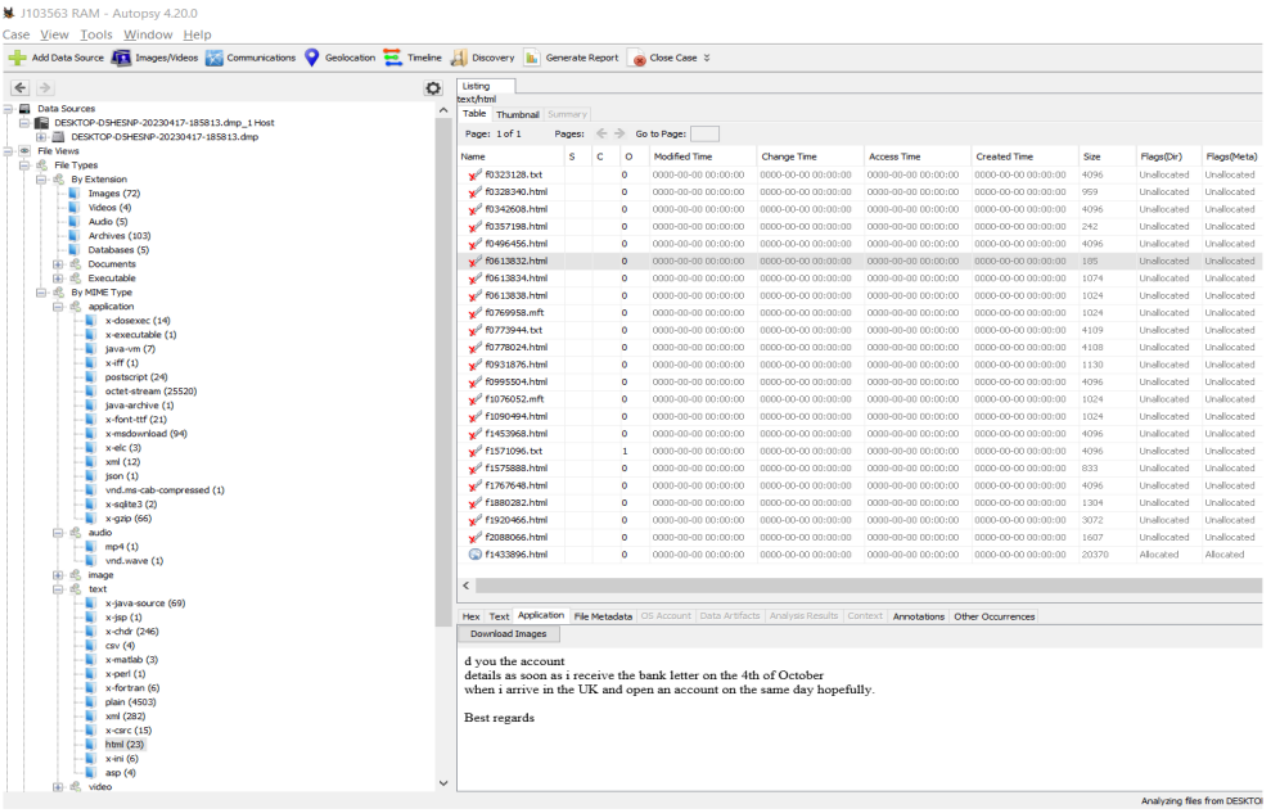

Figure 4. *The context of an email address.*

Moreover, according to Chetry et al. (2019), Volatility tool can also be used for the RAM analysis and extracting evidence using variety of commands as shown in Table 2.

Command	**Function**
Imageinfo	Shows information about the operating system
Psscan	Search for invisible processes
Pslist	Shows the running process on the image
Netscan	Shows network related information
Filescan	Shows files used recently or in the past

Table 2. *Commands and functions of Volatility.*

2.2 Disk Imaging:

2.2.1 Benefits of disk imaging:

As mentioned by Hassan (2019), the hard disks have a slack space in which there are deleted files that could be recovered for analysis. Additionally, as described by JL2977 (2018), the image of the hard disk will also contain file type system and boot sectors, besides data essential for restoring data in case of hard drive data corruption. Likewise, imaging hard disk can maintain the unallocated space and critical files (Kirvan, 2023).

2.2.2 Using FTK Imager:

By analyzing a hard disk image, a deleted image was discovered, and this is one of the reasons why the hard disk should not be copied, but it should be imaged to find deleted files as shown in Figure 5.

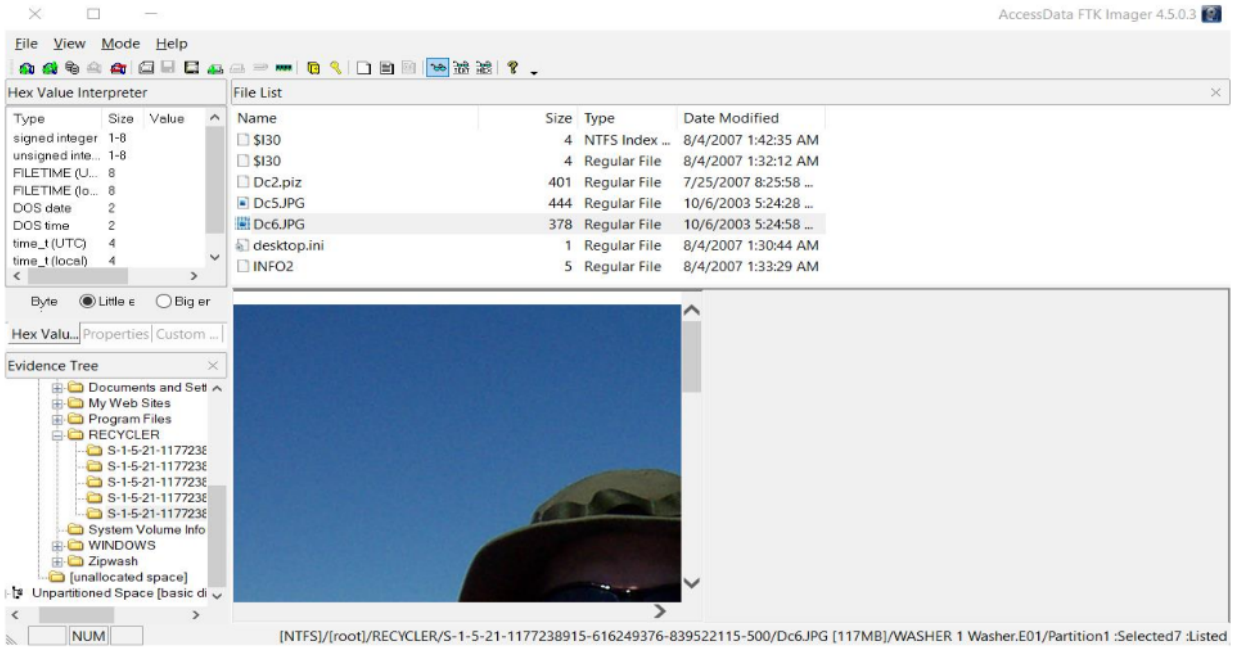

Figure 5. *Discovering a deleted image.*

Likewise, another importance of imaging is having access to hidden files, as shown in Figure 6, a hidden file was found including the date of its creation, and as the image analysis goes on there might be a discovery of a hidden malware.

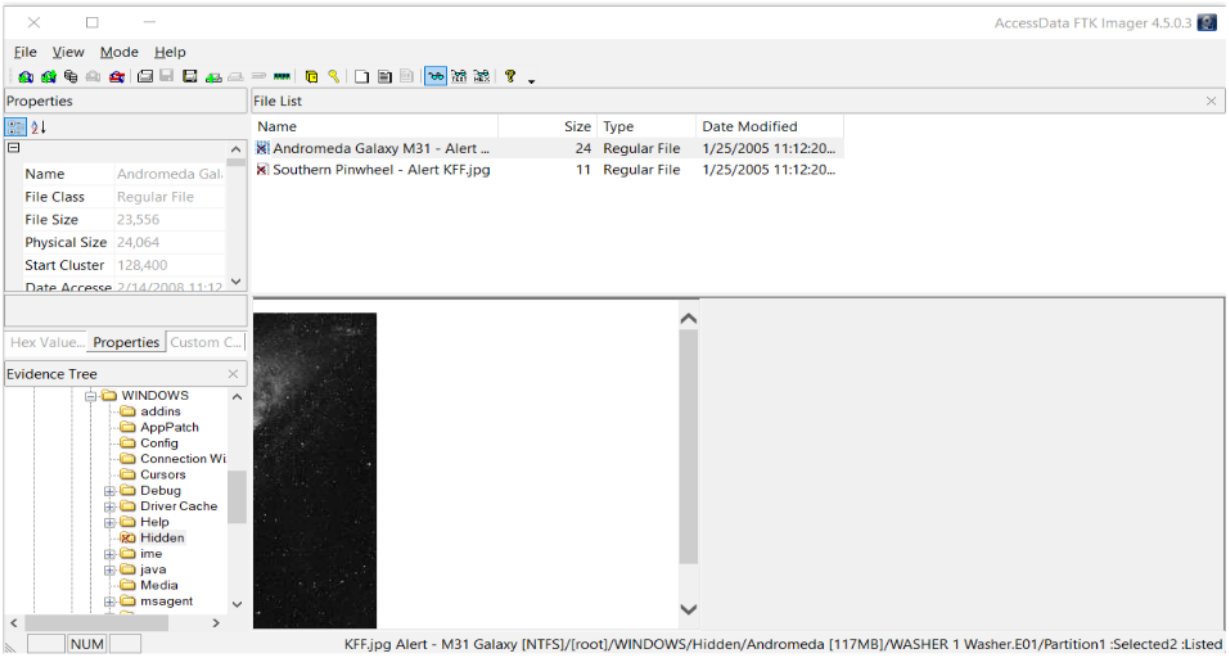

Figure 6. *Discovering a hidden file.*

2.3 Precautions for imaging process:

There are some precautions to consider, firstly ensuring that the tool used is compatible on the device infected, for instance, Dump It and Autopsy are compatible with Windows 10, as mentioned by Hassan (2019). Secondly, according to Sammons (2014), the validity of the tool is crucial since the results must be relied on since it will end up in the court. Thirdly, using variety of tools is important to collaborate the results (Sammons, 2014), that's why taking a second RAM image by FTK Imager would be beneficial. Another precaution is the file system the tool supports, as mentioned by Ec-Council (2016), FTK Imager supports NTFS, besides each file system stores files in a different way (Hassan, 2019). For instance, it will cover the devices in question, while on the other side it would not cover the Mac devices if they were discovered to be attacked.

As indicated by NIST (2006), volatile data should be prioritised over non-volatile in terms of copying it first since it can be lost if any power supply problem occurs, and because it takes less time to be gathered. However, as described by Hassan (2019), when comparing HDD and SSD hard drives, SSD is sometimes unattainable in restoring deleted files. Additionally, as described by Kirvan (2023), using write blocking device should be taken into consideration in order to terminate any possible modifications to the original copy, for instance using USB write blocking device. Perhaps, the image will be taken on external storage device, and the file type of the external storage should match the infected device.

Moreover, there are variety of extensions of the images, for instance, a raw format was used for RAM which is ".dmp", the reason behind this is the ability to obtain an identical copy, besides bypassing any possible reading errors while copying (Hassan, 2019). On the other side, "E01" is beneficial in splitting and compressing files (Altheide et al., 2011), and this was the extension of the large size hard disk image used because it enables dividing the disk into chunks (Hassan, 2019)

3. Malware analysis

3.1 Static Analysis:

Static analysis is concerned with seeking metadata of the malware, for example, file type, file size, strings, and hashes responsible for the algorithms, by other means it focuses on collecting information without launching the malware (Roberts et al., 2017; Sikorski et al., 2012). However, it does not show the complete desire of the malware and its' type without subsequently using dynamic analysis (Talukder et al., 2020). As a result, a variety of tools will be used, but if the malware was packed or compressed by the attacker, so unpacking process using UPX tool should be started first (Sikorski, 2012).

3.1.1 Detect it easy:

Using Windows 10 virtual machine as shown in Figure 7, and by uploading an example of a malware into Detect it easy, it has shown that the malware was built using C programming language, besides being an unpacked malware, which means it is the original state of the malware.

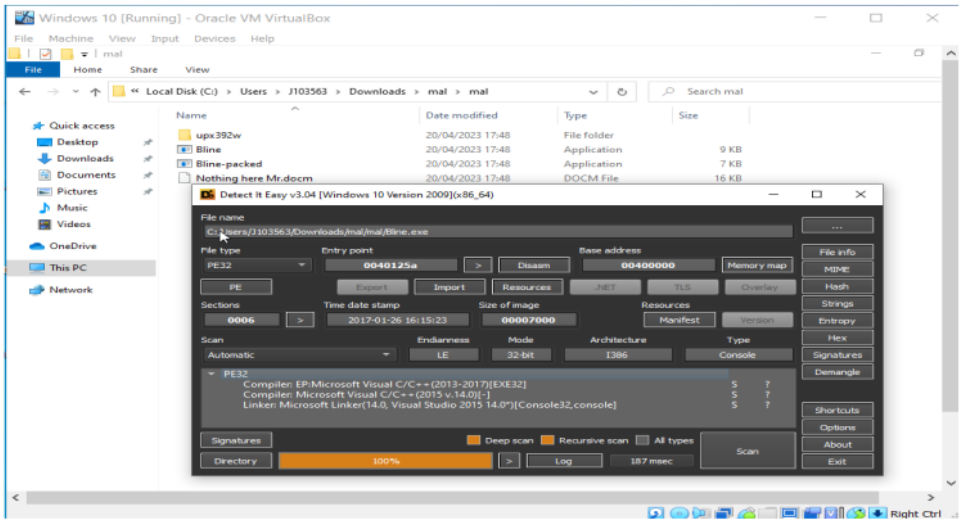

Figure 7. *Detecting the programming language of a malware.*

Additionally, by doing string analysis it has revealed the functionalities of the malware which is that it creates a text file and adds the word "echo" in that file, besides only pinging the local machine as shown in Figure 8.

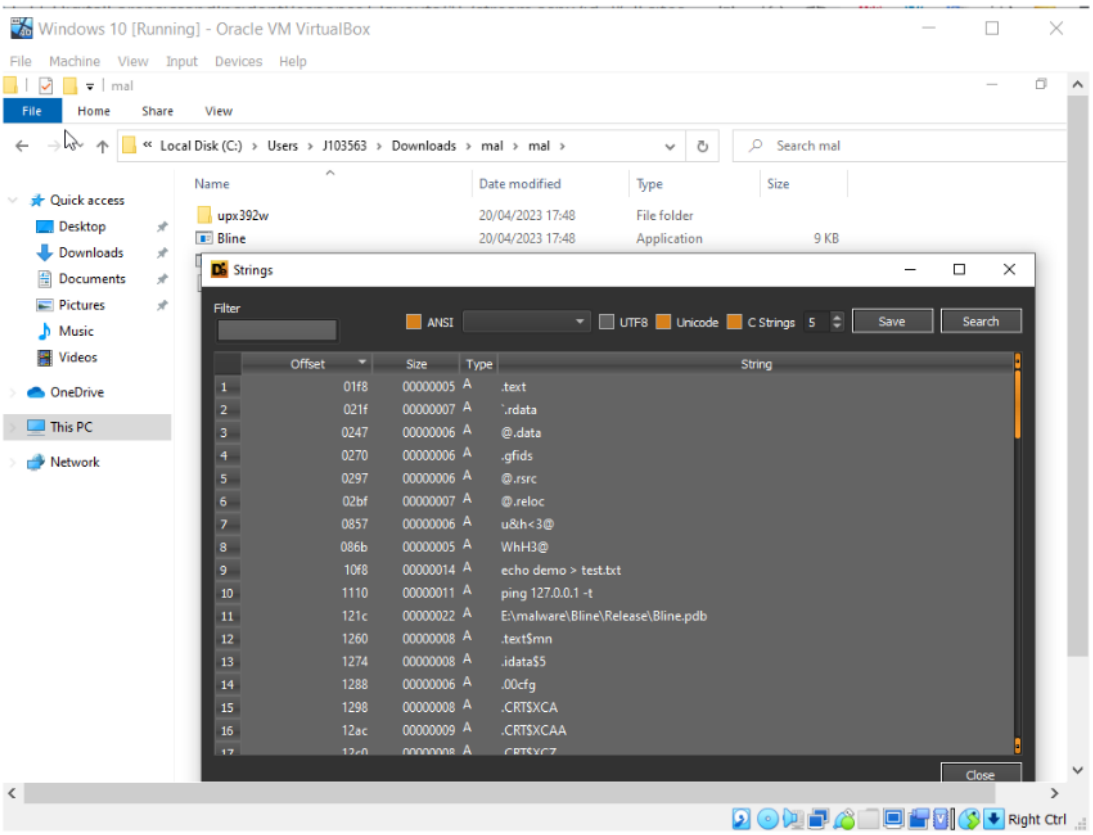

Figure 8. *String analysis.*

3.1.2 Disassembling process, and its advantages and disadvantages:

It rebuilds the malware written code in assembly language instead of binary to be readable by analysts (Kumar et al., 2015; Main et al., 2003; S et al., 2015). Additionally, by seeing the translated written instructions this could reveal the tasks of the malware that might not be observed during dynamically analyzing the malware (Roberts et al., 2017). Moreover, it gathers information about how the malware was written and what is the desired outcome (Sikorski et al., 2012). For instance, it identifies the functions of the written code. On the other hand, as mentioned by Madoš et al. (2014), some malware might be large and will take time to process it, besides the required time to read the code and understand its desired outcome.

3.1.3 IDA disassembling tool

As shown in Figure 9, the IDA tool was used on a malware file, it has changed the binary code into assembly, and as shown on the right side it seems that the malware is targeting the username of the device.

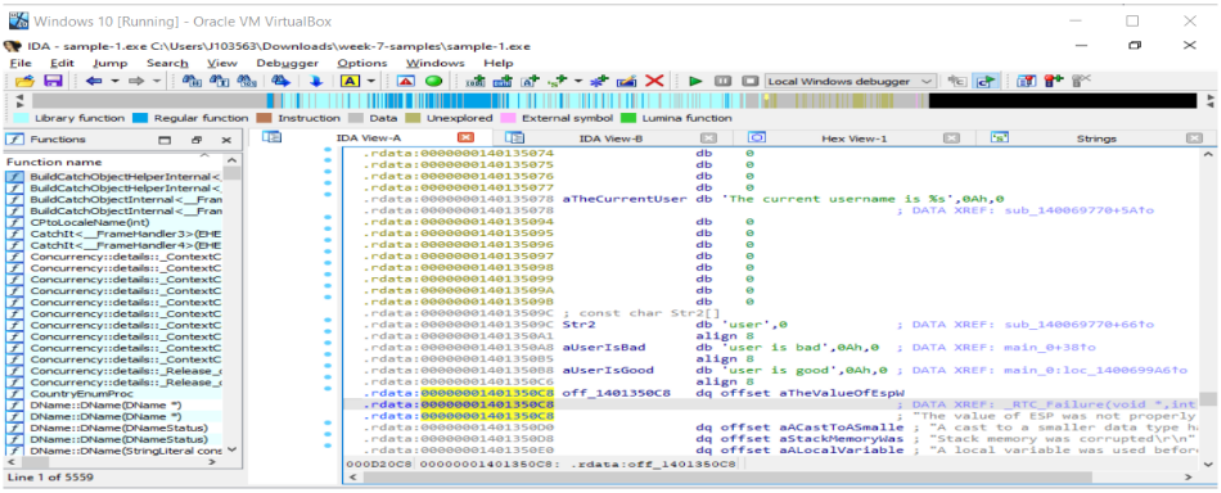

Figure 9. *Using IDA to convert binary code into assembly.*

3.1.4 Decompiling process, and its advantages and disadvantages:

Afterwards, decompiling process has occurred by converting the code to a higher programming language for example C++, which will be matching the originally created code to some extent (Kumar et al., 2015). On the other side, according to Li et al., (2012), the obtained high-level code will make the understanding of the code easier, but the converted code does not match the original one, and there might be technical errors in decompiling leading to the miss of some code lines.

3.1.5 dot Peek decompiling tool:

By opening another malware file inside dotPeek, it has shown in Figure 10, that this malware might be a keylogger, and collects data typed by the user and sends them to an email address. However, this can be confirmed by dynamic analysis in the following section.

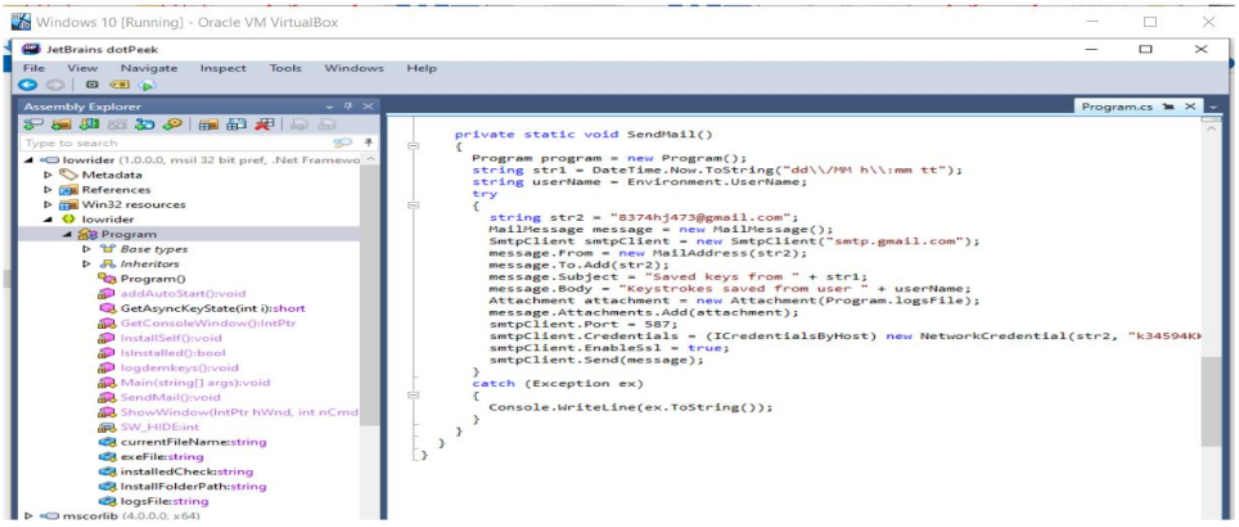

Figure 10. *Using dotPeek to decompile malware.*

3.2 Dynamic analysis

Dynamic analysis is concerned with launching the malware and observing the changes done to the system (Roberts et al., 2017). Perhaps it is beneficial in endorsing the predictable outcomes collected by statically analyzing the malware (Sikorski et al., 2012). However, it is crucial to take all safety precautions while doing it, for example, running the malware on a virtual machine (Roberts et al., 2017). Additionally, according to Sikorski et al (2012), internet connection should be turned off until enough analysis was performed to predict how the malware would act in case the malware does not require internet connection to be analyzed.

3.2.1 Debugging process, and its advantages and disadvantages:

Debugging tools are used to execute malware and observe what it does (Sikorski et al., 2012). It can adjust a break point to stop the execution of the program at a certain programming line (Kumar, 2015). On the other hand, worms might transfer to all the network devices if it has spreading properties (Sikorski et al., 2012). According to Sikorski et al (2012), some malwares have the property of detecting that they are being launched in a virtual machine and this might lead to a different action than the predicted one. Likewise, as described by Talukder et al. (2020), some malware requires a specific date to be launched at.

3.2.2 Process Hacker tool:

As shown in Figure 11, Process Hacker tool was launched on the right side before launching the malware file, then on the left side the activity of the malware was observed. The collaboration between the tools was beneficial because in the previous step by using dotPeek there was a preformed guess that the malware might be a key logger. As a result, by attempting to use a notepad and writing a couple of letters, it was observed that the peak and the activity of the malware on the left side was increasing in terms of writing data. Likewise, these written data were sent to the previously identified email address using dotPeek.

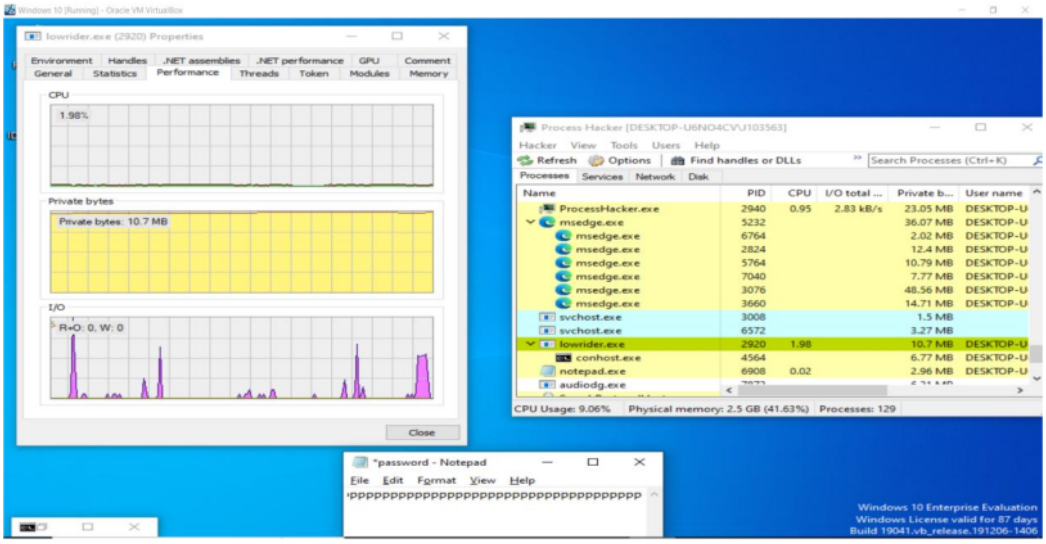

Figure 11. *Executing the code.*

4. Recommendations:

After performing all the previous steps, the security posture of the company requires adjustments to mend the vulnerable points. It is recommended that the company take certain measures especially because it took them a long time to discover the infiltration. The first measure is implementing security information and event management SIEM which is described by Granadillo et al., (2021), as a mean of collecting data from the firewall, antiviruses, and intrusion systems, then it can collaborate these findings and warn the security team about any possible threats. Another measure which can be implemented is Security Orchestration, Automation, and Response (SOAR), which is responsible for the automation of the processes, however SOAR and SIEM can work together to achieve a highly pro-active security system in terms of automation and quicker responses (Granadillo et al., 2021).

Thirdly, the use of VPN is acceptable if the company does not use the vulnerable list of providers mentioned previously in section 1.2.2. On the other hand, the use of SSH for remote access can be adjusted in the short term to depend on public and private keys which can be continuously changed until finding alternatives, besides prohibit remote root privileges, on the long term if the continuous change of credentials was unattainable. It is also recommended to keep these services up to date, besides providing training against social engineering attacks for the employees.

5. References

Altheide, C., & Carvey , H. (2011). *Digital Forensics with Open Source Tools.* Syngress.

Chetry, A., & Sharma, U. (2019). Memory Forensics Analysis for Investigation of Online Crime - A Review. *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*. https://ieeexplore.ieee.org/document/8991425

Ec-Council. (2016). *Computer Forensics Investigating Network Intrusions & Cyber Crime.* Cengage Learning Ptr.

Granadillo, G. G., Zarzosa, S. G., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis,Trends, and Usage in Critical Infrastructures. *Sensors. 21(14)*. https://doi.org/10.3390/s21144759

Hassan, N. A. (2019). *Digital Forensics Basics A Practical Guide Using Windows OS.* Apress.

JL2977. (2018). The benefits of disk imaging for students. *The Yale Tribune.* https://campuspress-test.yale.edu/tribune/the-benefits-of-disk-imaging-for-students/

Kirvan, P. (2023). What is a Forensics Image? *TechTarget*. https://www.techtarget.com/whatis/definition/forensic-image#:~:text=Creating%20forensic%20images%20and%20backing,of%20critical%20files%20in%20general.

Kumar, K., & Kaur, P. (2015). A Generalized Process of Reverse Engineering in Software Protection & Security. *International Journal of Computer Science and Mobile Computing, 4(5), 534-544*. https://www.ijcsmc.com/docs/papers/May2015/V4I5201571.pdf

Li, J., Gu, D., & Luo, Y. (2012). Android Malware Forensics: Reconstruction of Malicious Events. *32nd International Conference on Distributed Computing Systems Workshops, 552-558*. https://doi.org/10.1109/ICDCSW.2012.33

Madoš, B., Čajkovsky, M., Hurtuk, J., & Morvacik, K. (2014). Analysis of the Software Behaviour Using Forensic Methods for Computer Security Purposes. *Acta Electrotechnica et Informatica 14(2), 36-40*. https://doi.org/10.15546/aeei-2014-0015

Main, A., & Oorschot, P. v. (2003). Software Protection and Application Security: Understanding the Battleground.

Microsoft. (2023). GetUserNameA function (winbase.h). *Microsoft*. https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-getusernamea

Miller, M. (2022). SSH Key Management Overview & 10 Best Practices. *Beyond Trust*. https://www.beyondtrust.com/blog/entry/ssh-key-management-overview-6-best-practices.

National Cyber Security Centre. (2019). Vulnerabilities exploited in VPN products used worldwide. https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

National Institute of Standards and Technology. (2006). *Guide to Integrating Forensic Techniques into Incident Response: NiST SP 800-86.* CreateSpace Independent Publishing Platform .

Roberts , S., & Brown, R. (2017). *Intelligence–Driven Incident Response: Outwitting the Adversary.* O'Reilly.

S, S. Y., Prayudi, Y., & Riadi, I. (2015). Implementation of Malware Analysis using Static and Dynamic Analysis Method. *International Journal of Computer Applications, 117(6)*. https:doi.org/10.5120/20557-2943

Sammons, J. (2014). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics (2nd.ed).* Syngress.

Sikorski, M., & Honig, A. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software.* No Starch Press.

Talukder, S., & Talukder, Z. (2020). A SURVEY ON MALWARE DETECTION AND ANALYSIS TOOLS. *International Journal of Network Security & Its Applications (IJNSA), 12(2)*. https://aircconline.com/ijnsa/V12N2/12220ijnsa03.pdf

Turner, P. (2023). What Are Your SSH Security Risks? Best Practices for Securing SSH. *Venafi*. https://venafi.com/blog/best-practices-ssh-key-management-what-are-your-ssh-security-risks/

J103563

GRADEMARK REPORT

FINAL GRADE

80/100

GENERAL COMMENTS

Instructor

Task 1:

Good Introduction. Detailed explanation of the Digital Forensics Process. The approach to the investigation is solid. All the relevant tools are identified. Well done!

Issues: Important information about the breach is in the centralized log server. Centralized log management analysis should have more focus.

29/35

Task 2:

Good attempt. All the screenshots are provided with detailed information about the memory and disk imaging. You have explained all the precautions. Well done!.

Issues: There is no mention of the recommended external storage size in the precautions. Some details of Volatility would have earned more marks.

21/25

Task 3:

Good attempt. All the screenshots are provided with detailed information about the static and dynamic analysis process.

Issues:

You have not discussed precautions of the malware analysis process. For instance, analysis in a virtualized environment and taking snapshots of the VM at regular intervals is also important along with several other precautions.

17/25

Task 4:

Excellent recommendations. You have not mentioned the importance of having an operational Incident Response policy

13/15

PAGE 1

PAGE 2

PAGE 3

PAGE 4

Comment 1

What about the built-in tools?

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9