Digital Investigation of a Cybercrime: Sextortion as a Case Study

ALJI Mohamed and CHOUGDALI Khalid

Electronics and Telecommunication Systems Research Group, National School of Applied Sciences,
Ibn Tofail University, Kenitra, Morocco
mohamed.alji@uit.ac.ma and chougdali@gmail.com

Abstract. Sextortion is a way of blackmailing a victim for money, or favors, in which a sexual content in a digital format is being used for the extortion. In order to apprehend the criminal and present him to the court of justice, law enforcement agencies need to identify the suspect and link its computer to the happening of the crime. The present article is a case study of a digital investigation on a sextortion crime. The aim is to present a way of solving such a crime based on the digital artifacts that may be found on the suspect computer. We also held an experiment to demonstrate the utility and the reproducibility of our approach and concluded by a discussion on some unique indicators of committing the crime using the suspect computer.

Keywords: Digital investigation, Forensic analysis, Software Forensic artifacts.

1 Introduction

1.1 Cybercrime

The internet can be reached by more than 46% of the world population according to the Internet Live Stats project [1], that's more than 3.9 billion people all over the world that can use internet up to now. Imagine if a small fraction of those people know a malicious way to exploit the endless possibilities of the interconnected devices, that may engender the happening of a lot of digital crimes or a so-called cybercrime.

The term 'cybercrime' is used to express a crime that a computer device is somehow involved in it. That means not only the illegal hacking of an online banking system is considered a cybercrime, the offense of stealing a notebook is also a cybercrime. In fact, according to [2], cybercrime means two things either it is the crime that has migrated from the real world to the cyberspace, for instance : harassment can either be on schools during recreation time or on online blogging platform, or it is the offenses that are specifically designed for the cyberspace, such as distributed denial of service, spam or website defacing.

One of the offenses that migrated from the real world to the cyberspace and got an amplified effect because of the easiness of multimedia sharing content through social networks and online platforms is Sextortion.

1.2 Sextortion

According to the definition available on the official Interpol website[3], sextortion is a blackmail in which a sexual information or images are used to extort sexual favors and/or money from the victim. A sexual content at the disposal of a malicious person can lead to an attempt of a favors extortion from the victim. The question in our context is "how an internet user can commit such

a cybercrime ?". For illustration purposes, we describe one scenario of a typical happening of the crime as follow: the criminal assumes the identity of an attractive woman and uses a suggestive video broadcasted as a live video to an instant messaging application (such as IMO or Skype). The victim believes that the conversation being held is real and instantaneous, thus, answering the suggestive solicitations with similar ones. The criminal takes advantage of the situation and proceed to the recording footage of the victim in the nude or performing a sexual act. After that, the criminal blackmails the victim and threatens to diffuse the recorded video to an online video sharing platform such as Youtube or to share it with the victim's Facebook friends, unless a certain amount of money is paid [4].

1.3 Fight back : Digital forensics efforts

Some victims pay the money taking no guarantee of the none reiteration of the extortion. Other victims choose to deposit a complaint to the police, the investigation yields most of the time to the identity of the suspect. The local police proceed to the seizing of the suspect computer. At that moment, it is up to the computer forensic expert to assert whether the suspect is the searched for extortionist or not, through analyzing the digital forensics artifacts present on the digital evidence device that may link the computer of the suspect to the happening of the crime. Knowing the digital forensics artifacts and how to figure them out for a typical scenario of such cybercrime will easy the computer forensic expert task. The main aim of this article is to bridge such gaps.

The present article is structured as follow: In section 2, we will describe the adopted research methodology and the way the experiment has been designed. In the second section 3, we depict the results of the research. Lastly, in section 4, we discuss those results in details and we conclude.

2 Research Methodology

2.1 Overview of the Computer Forensic Examination Process

Understanding the computer forensic examination process is from two different standpoints: the theory and the practice. At first, the computer forensic examination is the practice of collecting, analyzing and reporting on digital data, as visualized in the following diagram:

The collection part consists of the gathering of the digital evidence following the most current best practices [5]. The analyzing step consists of finding out what happened in the digital environment based on the available digital forensic artifacts. The reporting phase consists of answering the issues raised to solve the case [6].

Fig. 1. The process of computer forensic examination

In practice and in general, the steps of a computer forensic examination proceeded by a law enforcement agency are as follow [7]:

During the collection phase, the police department needs to obtain the authorization from the court of justice to search and seize the digital devices that may contain digital evidence. After that, they should secure the area where the devices are found (the crime scene). From the seizing of the devices, a document of the chain of custody is established to ensure the traceability. The devices are uniquely identified and securely transported to the digital forensic laboratory. In some cases, the digital evidence acquisition is to be done on the scene on a running live system. A forensic image is created from the devices using forensically sound methods and tools.

During the analysis step, and while securing the original material in a safe location, the digital forensic examiner designs a review strategy of the digital evidence including, for instance, a list of keywords and search terms. Then proceed to the examination and the analysis of the forensic images according to that strategy.

During the reporting phase, the digital forensics examiner interprets and draw inferences based on facts gathered from the digital evidence. Then, he writes down in a standardized format report the description of its findings. He may also give testimony under oath in a deposition or in a courtroom as a witness expert.

In what follows, we will simulate an extortionist computer and study its digital forensic artifacts. So we need to have a computer-like running system with a sextortion predefined scenario set-up. We then acquire the forensic image, and we consider the bitstream image as the input. The simulated bitstream image is the forensically sound acquired image from the suspect computer that has been used to commit the cybercrime.

2.2 Setting up the computer suspect Virtual Machine

In order to experiment with the possibility to go back on time, we made the choice of using Virtual Machines. We chose Oracle VM VirtualBox as a Virtual Machines manager on a Linux machine for stability reasons. We downloaded the operating system Windows 10 on ISO format available from the following link [8]. Following the recommendations of the Oracle VM VirtualBox official manual [9], we created a Virtual Machine. We installed the guest OS (Windows 10) on the Virtual Machine after configuring the virtual disk as dynamically allocated and relatively small starting size. We installed the VirtualBox Guest Additions on the guest os. Finally, We executed the steps of the predefined scenario of sextortion as described in the following paragraphs. As stated before, we are supposed to create a suspect machine with the cybercrime already committed using it. One way of committing a sextortion is visualized on figure 2.

10.11228/dpsc.01.01.005

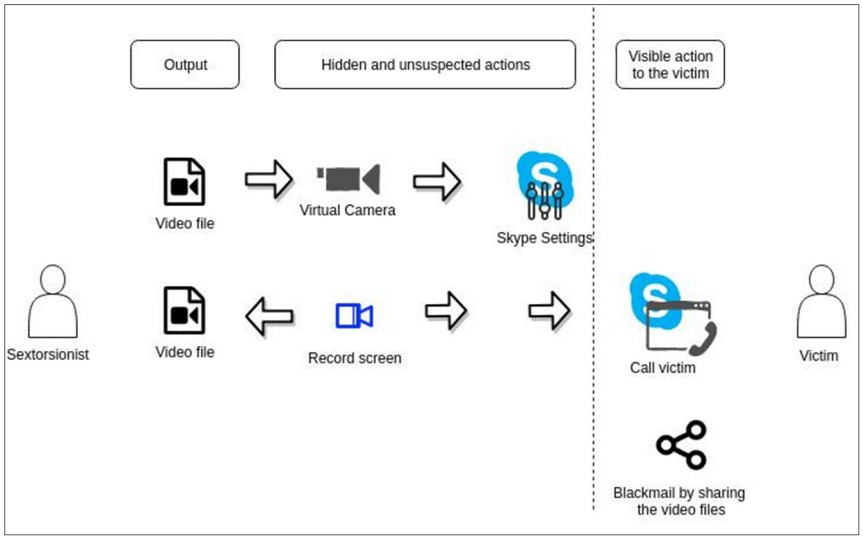

Fig.2. A simplified illustration of a way of commiting a sextortion crime

We describe the steps to make the virtual machine of the suspect computer commit the sextortion crime as the following predefined scenario :

1 We installed the instant messaging software (Skype) and video camera effects manipulator (SplitCam) and configured them in a way to set in Skype settings the SplitCam Virtual Camera as a default camera for Skype video conversation.

2 We created one account for the suspect (Sarah-suspect) and one account for the victim (victim-one) on Skype. We made a text conversation and a call to the victim account.

3 We recorded the footage using one of the available screen recorder and save the recording result to a file.

4 We shared the recorded file on a private channel on Youtube, and then proceeded to the extortion discussion through Skype.

5 We finally uninstalled the video camera effects manipulator (SplitCam).

2.3 Acquisition of forensic images for analysis

From the VirtualBox manager on the Linux machine, we proceed to the snapshots needed while performing the steps of the previously predefined scenario. For instance, a snapshot is done after the installation of the instant messaging software and the video camera effects manipulator. Then, we create a clone of the virtual disk using the following command:

```
VBoxManage clonemedium snapshot_i.vdi snapshot_i.raw --format RAW
```

The i corresponds to each snapshot required. Then, we are performing a bitstream copy and a conversion from the virtual disk format (.vdi) to a RAW format because the digital forensic analysis platform (Autopsy) does not support a data source in .vdi format.

The acquired images are forensic images according to [10] and will be useful for any postmortem analysis. The following flowchart 3 details the design of the experiment retained to establish the necessary forensic images for further analysis.

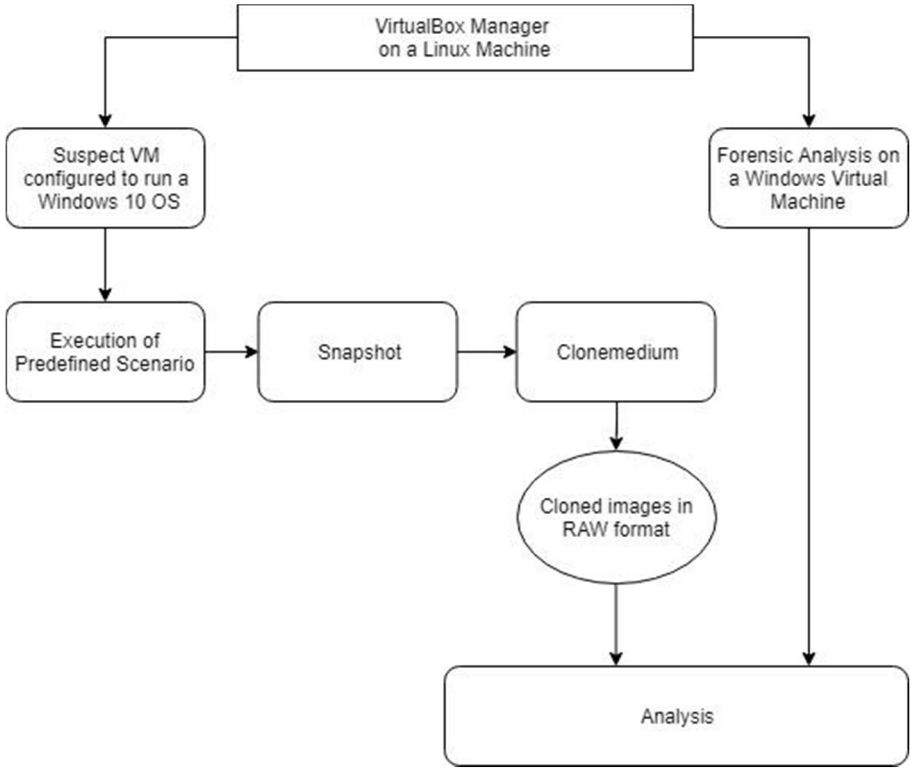

Fig.3. Experiment design flowchart for the acquisition of forensic images

2.4 Tools used for the Analysis of the suspect virtual machine

Since we are playing with a simulated version of a suspect machine, we can use multiple tools to analyze multiple aspects of digital forensics artifacts. We will do a postmortem analysis of the content of the filesystem using the digital forensic analysis platform: Autopsy. The registry content will be frozen before and after each step and a comparison is established using: RegShot. Registry Viewer will allow to view the registry content and parse some registry values. The hexadecimal viewer: HxD will allow the representation of a hexadecimal data and a search within unstructured values. The file recovery: Photorec will allow the recovery of deleted or lost files independently from the filesystem.

Oracle VM VirtualBox v5.2.18	create forensic images
Autopsy v4.8.0 on Windows os	parse the file system content
RegShot v1.9.0	save state of the registry for analysis
Registry Viewer v2.0.0	view registry keys and hives
RegLookup v1.0.1	recover registry keys
HxD v1.7.7 on Windows oS	search unstructred data & view hexadecimal values
PhotoRec 7.0 on linux	recovery program of lost files

Table 1. A list of used tools

3 Results Analysis

3.1 The recovery of SplitCam log file

The video camera effects manipulator SplitCam is installed on the following directory %ProgramFiles(x86)%\SplitCam knowing of course that it is provided only as a 32-bit program. Some data specific to SplitCam are store don the following directory C:\Users\%USERPROFILE%\AppData\Roaming\SplitCam. An interesting text file named "SplitCam.log" is created in this directory after the first run of the application. The log file has an important forensic value since it records all the uses of SplitCam with their timestamps. For instance, we can observe the line "> Source ". It tells the source of content used at a specific time for SplitCam. It may be a Camera, a file or a folder of a list of multimedia content. Other digital artifacts are a desktop shortcut that points to splitcam.exe, a quick launch shortcut, and a start menu folder. The main objective of using the file recovery PhotoRec is to recover the SplitCam log file as a remnant digital forensic artifact. In order to narrow the process, we limited the recovery to txt and tx? files format. And for further optimization, we used our own custom signature for the SplitCam log file which corresponds to:

extension name : log

offset of the signature : 0

signature or magic value :"==== ["

footer: 0d-0a 0d 0a hex

We managed to figure it out as described in following documentation web page [11]. But before doing so, we checked successfully that PhotoRec can recover the SplitCam log by using the beta version of PhotoRec online checker. The recovered log file contains a line that starts > Source: that indicates the source of the broadcasted video content. In our case, we found a video file in Windows Media Video format (WMV) entitled "Wildlife.wmv".

3.2 Recovery of meaningful registry subkeys

Windows registry keys and subkeys left by software can contain a valuable forensic information [12]. In our case, the main registry key artifact left by Splitcam can be found on the following location: HKEY_CURRENT_USER\Software\ SplitCam\SplitCam.Onthefilesystem,thefile"NTUSER.dat"comprisesthose pieces of information is located in the user main directory "Documents and Settings". In the previously mentioned registry key path, there are some registry subkeys, named "LastDevice" and "LastVideo", that have a forensic value. "LastDevice" indicates which device was lastly used by SplitCam as a source of content. For instance, if the subkey contains the value "SuperVision HD". That meansthelastdeviceusedonSplitCamthataddedeffectstoitsaninstantaneous stream is the suspect machine camera "SuperVision HD". After uninstalling SplitCam, such registry key may disappear. Recovering from windows registry using reglookup-recover tool [13] & [14] will allow to uncover the value of the registry subkeys "LastVideo" and "LastDevice". If this recovery does not succeed, an approximate search of the unstructured data within the file "NTUSER.DAT" using a hexadecimal viewer such as HxD, yields its values.

3.3 Exploring the content in Windows filesystem

There is another artifact, that allows as to check whether the suspect had set the SplitCam virtual video camera as a default source camera for the instant messaging application Skype. We found that the settings file "settings.dat" located at %USERPROFILE%\AppData\Local\Packages\Microsoft.SkypeApp_ID\Settings contains a parameter that shows "SplitCam Video Camera" set as prefered camera. The digital forensic analysis platform Autopsy allows the parsing of the filesystem content. So that, a simple search for some files based on their types will allow the finding of Videos and Images that may have been used to commit the cybercrime. A search for the video file that was set as a source in SplitCam log can ease the task. In addition, reading and parsing the skype discussions content logged in the suspect machine may reveal the extortionist discussion. While this part will not be detailed since Skype forensic artifacts are widely explored by the digital forensic research community. Sometimes, the parsing of the suspect’s browser history can disclose the presence of links to an online video sharing platform such as Youtube. And those pointed out videos may have been removed from the platform because of their sexual content.

4 Discussion

The main objective of the digital investigation is the findings of unique incriminating indicators of the happening of the cybercrime (Sextortion). In our case, the presence of digital forensics artifacts of the typical following software such as a Camera Effects Manipulator, an Instant Messaging Application and even a Screen Recorder can indicate that the suspect may have used this trio of software to commit the sextortion crime. But that is still insufficient, since the suspect may have used that software for other common reasons. Setting a virtual camera from a video effect manipulator that points to a suggestive video file as a default source video for Skype will reveal the criminal intention of a suspect. In addition, the recovered registry keys may have disclosed that the registry key "Last Video" points to a suggestive video file. The presence of incriminating content of files such as video files that may be used to lure, like

suggestive videos of girls or the screen recorded scenes of unknown people will help the judge decision. Further more, the extraction of artifacts of Instant Messaging such as the blackmail discussion and the log of made calls to the victim can assert the happening of the sextortion. Any further extracted web history of the accessed links and shared links of uploaded videos related to the matter will help incriminate the suspect.

5 Conclusion

In this paper, we described a typical way to solve a Sextortion cybercrime and we performed an experiment to assess the reproducibility of the results. We used virtualization capabilities to simulate a suspect machine. We examined some digital forensics artifacts that lead to the incriminating of the suspect. Still, there are much more ways to commit the Sextortion crime. Indeed, the sextortionists can innovate and use other instant messaging applications rather then Skype. They can record the screen in so many ways, for instance using a lightweight standalone application, or an installed one, they can use old version of the tools. They can run the portable version from a USB thumb. It is difficult to size all the malintentioned possibilities. In a future work, we will try to size those cases in order to provide a more integrated way to deal with such a crime while aiming at assisting the justice.

References

1. InternetLiveStats.com. Real time statistics project. internet live statistics. 2016. [Online; accessed 28-July-2018].
2. SusanW.Brenner. Cybercrime:Re-thinkingcrimecontrolstrategies. Crimeonline, pages 12–28, 2007.
3. Interpol. Online Safety. https://www.interpol.int/Crimeareas/Cybercrime/Online-safety/Sextortion, 2018. [Online; accessed 07-Avril2018].
4. Michael Joyce. Video chat extortion and sexual abuse. 2012.
5. Tom Killalea and Dominique Brezinski. Guidelines for evidence collection and archiving, 2002.
6. J. Kävrestad. Guide to Digital Forensics. Springer Briefs in Computer Science, 2017.
7. Reynaldo Anzaldua Linda Volonino. Steps to take in a computer forensics investigation. http://www.dummies.com/computers/pcs/computer-security/steps-to-takein-a-computer-forensics-investigation/, 2008. [Online; accessed 15-Juin-2018].
8. Microsoft Corporation. https://www.microsoft.com/fr-fr/softwaredownload/windows10ISO, 2018. [Online; accessed 20-Avril-2018].
9. Oracle Corporation. Oracle vm virtualbox manual. https://www.virtualbox.org/manual/, 2004-2018. [Online; accessed 13-Sept2018].
10. Manish Hirwani, Yin Pan, Bill Stackpole, and Daryl Johnson. Forensic acquisition and analysis of vmware virtual hard disks. The 2012 International Conference on Security and Management, 2012.
11. CGSecurity. Add your own extension to photorec. https://www.cgsecurity.org/wiki/Add_your_own_extension_to_PhotoRec, 2016. [Online; last accessed 14-Sept-2018].
12. Harlan Carvey. The windows registry as a forensic resource. Digital Investigation, 2005.
13. Timothy Morgan. Reglookup. http://projects.sentinelchicken.org/reglookup/, 2011. [Online; last accessed 14-Sept-2018].
14. Timothy Morgan. Recovering deleted data from the windows registry. The Digital Forensic Research Conference, 2008.