Digital Forensics (DIFO)
Stockholm University
Department of Computer and Systems Sciences

Lab Assignment II: Advanced Windows Forensics

Prof. Oliver Popov &
Alaa Altorbaq &
Jesper Bergman

Version 1.0
Autumn 2017

1 Introduction

Counterfeit and fraud are suspected to have been committed by Evgeny Gachev, alias lucky12345, one of the most wanted cybercriminals according to TSSCP[1]. In order for the court of law to determine whether Mr Gachev is guilty of the suspected crimes or not, you have been called in as expert forensic examiner to analyse the image of his computer hard drive. The hard drive was acquired by the technology savvy field officer in charge of the house search. The evidence hard drive was acquired in raw format using an Image MASSter Solo 4. The raw data file of the hard drive was transferred to a USB to your virtual machines. Hash sums from the Image MASSter Solo4 were verified to be the same as the hash sums from the image files put onto the virtual machines available to you.

After reading through chapter 5 in Casey's book, and watching the Windows Forensics lectures, you should now try to use that obtained knowledge in order to examine the Windows 7 system in the lab 2 file in EnCase. The acquisition of the original hard drive was done as described above. The evidence hard drive was imaged using a dedicated imaging device (Image Master Solo4). For those of you who are doing this lab in the CS2Lab.You can find the raw evidence file (.raw) inside the DIFO folder under the Lab Files on the Desktop. You can also download the files, from the FTP by opening an explorer window in Windows and typing in the following links in the browser:

http://ftp.cs2lab.dsv.su.se/DIFO/evgeny_40GB_2.raw

http://ftp.cs2lab.dsv.su.se/DIFO/DIFO_hashsums.txt

You are free to use any forensic tools that you would like for this assignment, we encourage you to be creative in your analysis and examination, and use different tools to cross reference with, but to also learn the differences, strengths and weaknesses of various tools. Frankly, everything that could in some way be related to cybercrime is interesting for the court of law to assess. You will learn more about the following basic forensic tools and concepts during this lab.The files needed for doing this lab are available on each group's machine. Some of the exercises can be done on a basic Windows/Linux system after downloading the files from there, though that is on your own responsibility.

1.1 Purpose

This lab is designed to further develop your knowledge and skill in the area of digital forensics.This assignment is worth 1.5 ECTS - that is equivalent to one week of full time studies per person[2]. We expect you to spend that time on this exercise, and it is required to be completed within that time frame.

[1] The Super Secret Police

[2] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/hogskoleforordning-1993100_sfs-1993-10

1.2 Marking Grading

This assignment is worth 1.5 ECTS (i.e. one week of full time studies) and is graded Pass or Fail. In order to pass this assignment, you will be graded based on the depth of your analysis and reflection (30%), The correctness of your answers (40%) and how well you report the forensic examination (30%).

1.3 Useful Tools

The following tools might be useful in your investigation. Feel free to use any other tool that you find sufficient. All tools are available for free on the net. Operating system under which the tool works is specified in parenthesis: The following tools will be useful for this lab, but feel free to install any additional software that you need on the lab computers.

- HexEdit - A binary file editor
- The Sleuth Kit and Autopsy
- DCode - Time-stamp interpreter
- TriD - File identification tool
- SQLiteBrowser - An SQL database viewer
- EnCase - Industry standard forensic tool
- FTK - Industry standard forensic tool
- PRTK - Password recovery tool
- Hashcat - Password recovery tool

Nota Bene:
You are advised to read the literature and information found on the iLearn2 page of DiFo 2017 and also make use of the references in this document for additional material that could be very handy while trying to solve this case. Please be aware that the lab staff will not give you any correct answers to the questions.

2 Questions

2.1 System Related Questions

- What is the disk image hash? Is the forensic image's integrity verifiable?
- How many sectors did the disk contain? What was the size of each sector? What was the size of the entire disk in bytes?
- How many partitions did the disk contain? What file system(s) has been used and how many sectors per cluster did it contain and of which size? How many bytes were allocated and how many unallocated?
- Examine the operating system version/ boot options that were used on the computer. What other information can you extract regarding the installation and configuration of the operating system? Can you find any indication if the system was a physical or a virtual system?

2.2 Case Specific Question

- Can you find any user accounts of the system; if so, which accounts, and when were they first created and used - when were they last used?
- What programs were installed on the computer?
- Is there any email correspondence that might indicate criminal activity related to counterfeit goods or fraud of any kind? If so, which aliases were involved? What was the content of the correspondence?
- Have any anonymisation tools or techniques been used to hide the user's identity? If so, can you see how many times they have been run?
- What domain has the computer been connected to?
- Are there any indication of remote connection to servers via FTP, SSH, Telnet, or any other network service protocol except HTTP/HTTPS?
- Assessing the registries and registry entries - can you find any useful information about remote connections, program settings, IP addresses etcetera that might be of interest?
- Can you find any failed or successful event logs of software installation attempts?
- Examine the prefetched folder. Can you find any program that has never executed?
- Which programs have been executed? How many times have they been executed?

- Examine the web browsing artefacts of the system. Can you find any interesting searches or websites visited?
- Examine any communication software and artefacts that you can find. What kind of communication has taken place? How has it taken place; between which parties?

3 Reporting

Your report will be sent to your boss who also is a senior forensics investigator as well as a police officer. A critical aspect of succeeding with the task is not to just find the relevant artefacts (if any) but also to communicate your findings in a scientific and neutral way. Therefore you should be very precise when reporting how your examination was performed and you shall clearly present where and what artefacts you have investigated (even if no artefacts of evidential value are found you should present where and why you looked for the potential evidence). You are required to use ReportTemplate (available in iLearn2) for this assignment. Please note that this template is a modified version of the "Case brief 1 report" in the NIST documentation Forensic Examination of Digital Evidence: A Guide for Law Enforcement[3]. Under the section "Examination" you should present the steps taken in the examination, for example:

[PATH] was investigated in order to find potential evidence belonging to information of [TYPE]. No data of evidential value was recovered OR Data of evidential was recovered by [METHOD].

If you would like to read example reports we recommend you to read the NIST documentation (pp. 23-38) available under Resources in iLearn2. For your report you are expected to use your newly gained knowledge from the DiFo course and document the procedure, perform an appropriate analysis on the key points and draw some conclusions on why this is necessary. You should be very precise when reporting how your examination was performed and you shall clearly present where and what artefacts you have investigated and also reason about the evidential value of the artefacts in an objective and scientific manner. Another aspect is to document how you proceeded i a way that allows your investigation to be reattempted and provide the same results. Even if no artefacts of evidential value are found you should present where and why you looked for the potential evidence. The following points are recommended to include in the report:

1. Description of the cases handled,
2. Description of the evidence and the chain of custody,

[3] https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

3. Method and tools used for answering the questions,
4. An explanation of what you found, how you found it and where you found it.
5. Conclusions
6. Your views on the proceedings

3.1 Plagiarism

Please do regard the term project as any other examination process. Plagiarism is not tolerated and the occurrence of plagiarism of any kind (including self-plagiarism) will face disciplinary actions in accordance with Stockholm University's code of honour. All hand-ins will be checked for plagiarism using the plagiarism checking tool Urkund. See DSV's code of honour and regulations regarding examinations for more information: http://dsv.su.se/en/education/study-information/regulations