ANALYSIS OF RANSOMWARE THROUGH THEIR BEHAVIOUR

ELYNA NAJIHA BINTI MOKHTAR

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS*

JUDUL: ANALYSIS OF RANSOMWARE THROUGH THEIR BEHAVIOUR

SESI PENGAJIAN: 2016/2017

Saya: ELYNA NAJIHA BINTI MOKHTAR
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat Salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

________ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

________ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

✓ TIDAK TERHAD

(ELYNA NAJIHA BINTI MOKHTAR)

(EN. MOHD ZAKI BIN MAS'UD)

ALAMAT TETAP: NO.8, JALAN
ADENIUM 2A/1, BUKIT
BERUNTUNG,48300 RAWANG,
SELANGOR

Tarikh: 18/08/2017

Tarikh: 18/08/2017

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

ANALYSIS OF RANSOMWARE THROUGH THEIR BEHAVIOUR

ELYNA NAJIHA BINTI MOKHTAR

This report submitted in partial fulfilment of the requirements for the Bachelor of Computer Science (Computer Security)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DECLARATION

I hereby that this project report entitled

ANALYSIS OF RANSOMWARE THROUGH THEIR BEHAVIOR

is written by me and is my own effort and that no part has been plagiarized without citations.

Student: ______________________ (ELYNA NAJIHA BINTI MOKHTAR) Date: 18/08/2017

Supervisor: ______________________ (EN. MOHD ZAKI BIN MAS'UD) Date: 18/08/2017

DEDICATION

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education

To my supportive friends, my supervisor and all lectures, thank you so much for assist and help.

ACKNOWLEDGEMENTS

I would like to show my gratitude and appreciation to my supervisor, En.Mohd Zaki Bin Mas’ud for all the advices in guiding me throughout the project.

I would also like to thank my beloved parents who have given me the greatest support in all sorts of materials throughout my years of studying in this university.

Finally, I would like to thanks to all my friends and course mates for their kindness in sharing knowledge and resources.

Thanks a lot.

.

ABSTRACT

A new threat in the cyberspace nowadays are known as ransomware and the threat are increasing in alarming rate. Ransomware is computer malware that installs covertly on a victim’s computer and have the ability to encrypt the whole file in the machine. Once encrypted the owner of the ransomware will demand an amount of money to decrypt the file. In order to get a better understanding on ransomware, this final year project use dynamic analysis approach to analyze this type of malware. This project objectives are including to identify ransomware traces through network traffic and program process as well as identify ransomware behavior through it malicious activities. This preliminary study of ransomware is the initial step in getting a depth knowledge on ransomware especially in identifying the parameter and traces of ransomware behavior during its execution

ABSTRAK

Ancaman yang baru di ruang siber pada masa kini dikenali sebagai ransomware dan ancaman ini semakin meningkat dalam kadar yang membimbangkan. Ransomware adalah malware komputer yang memasang secara terselindung pada komputer mangsa dan mempunyai keupayaan untuk menyulitkan keseluruhan fail di dalam mesin. Sekali disulitkan, pemilik ransomware akan menuntut sejumlah wang untuk menyahsulit fail tersebut. Dalam usaha untuk mendapatkan pemahaman yang lebih baik mengenai ransomware, projek tahun akhir ni meggunakan pendekatan analisis dinamik ini untuk menganalisis jenis malware ini. Antara objektif projek termasuklah untuk mengenalpasti kesan ransomware melalui lalu lintas rangkaian dan proses program serta mengenal pasti tingkah laku ransomware melaluinya aktiviti berniat jahat. Kajian awal ransomware adalah langkah awal dalam mendapatkan pengetahuan mendalam mengenai ransomware terutama dalam mengenal pasti parameter dan kesan tingkah laku ransomware semasa pelaksanaannya.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Introduction

This chapter will describe about the introduction of the project. This chapter are consisting of the problem statement, project question, project objective project scope, project contribution, report organization and the summary. The purpose of the project is to analyze a malware known as Ransomware that caused the increasing number of attack to target individuals, corporate entities and public-sector organizations by infects a computer. The content of this report including the definition of the malware itself, how ransomware works, the examples of ransomware, their latest form of attack, and the step by step of the method used to analyses the malware.

1.2 Problem Statement

Nowadays, malware can be easily infecting user's computer and widespread rapidly within a second in the network if the computers have many vulnerabilities. The computers nowadays are exposed and widely vulnerable to malware where it can widespread rapidly within a second in the network easily. The safety must be maintained and the security should be improved due to the huge growing use of internet, cyber-attacks are often to happen. Recently one of the threat is been come into existence known as Ransomware attacks which targets at any system files of the computer user. Ransomware has become one of the most widespread and damaging attacks that internet users face. Most of the internet users have less understanding about which parameter will use to study the behavior of ransomware. The problem statement is summarized as in Table 1.1.

Table 1.1: Summary of Problem Statement

PS	Problem Statement
PS_1	Insufficient information on the parameter use to explore the behavior of ransomware.

1.3 Project Question (PQ)

Several questions are issued based on this project Problem Statement. These questions are done to help develop the objective of this project. The questions are mainly on the behavior of the malware, its attack pattern, and the procedure of retrieving the attack pattern of the ransomware to enable it to be analyses through dynamic analysis. The project questions are summarized as in Table 1.2.

Table 1.2: Summary of Project Question

PS	PQ	Project Question
PS_1	PQ_1	What is the parameter uses to study the behavior of ransomware?
	PQ_2	What is the clear evidence on the behavior of ransomware?
	PQ_3	How the ransomware activity affects the parameter?

1.4 Project Objective (PO)

The project objectives are based on the problem statement and project question that has been highlighted in Table 1.1 and Table 1.2. Each project question consists of one project objective as to understanding about which parameter will use to the behavior of ransomware, to gains clear evidence on the behavior of ransomware, and to get knowledge on how the ransomware will affect the parameter. The project objectives are summarized as in Table 1.3.

Table 1.3: Summary of Project Objective

PS	PQ	PO	Project Objective
PS_1	PQ_1	PO_1	To understand about the parameter, use to study the behavior of ransomware.
	PQ_2	PO_2	To investigate the behavior of ransomware.
	PQ_3	PO_3	To link the ransomware behavior with the parameter.

1.5 Project Scope

The scope of this project is to analyze the behavior of a malware known as Ransomware to specific parameter or application and what the effect after the infection occurs. By using dynamic analysis approach to see the behavior of ransomware through virtual machine software (VMware) and through monitoring software as example by using *Wireshark* and process monitors. The malware installed into the virtual OS or application and then the behavior will be observed and recorded. The behavior of the application before and after the malware infection also analyzed to generate attack flow.

1.6 Project Contribution

The research contributions of the project help determine what the project will produce besides its objective. This project will help to determine the parameter that is used to analyze the behavior of ransomware. In addition, it also helps to determine the behavior of ransomware based on clear evidence and determine on how ransomware will affect the parameter. The project objectives are summarized as in Table 1.4.

Table 1.4: Summary of Project Contribution

PS	PQ	PO	PC	Project Contribution
PS_1	PQ_1	PO_1	PC_1	Determined the parameter use to study the behavior of ransomware.
	PQ_2	PO_2	PC_2	Determine the behavior of ransomware based on the investigation.
	PQ_3	PO_3	PC_3	Determine the link of ransomware behavior with the parameter.

1.7 Report Organization

To ensure this project is going on smoothly and successfully, report organization is constructed in order to arrange chapter by chapter respectively. The summarization and description of each chapter stated as below:

Chapter 1: Introduction

This chapter discuss about the introduction and the background of this project but in brief. There is problem statement, project question, project objective, project scope, project contribution and summary for this chapter.

Chapter 2: Literature Review

This chapter shows the preview to the literature review of this project. As example, the discussion about the software and hardware that being used in other research which is related to this project.

Chapter 3: Project Methodology

In this chapter, project methodology discussed according to activities, step taken and stages followed in order to make sure this project going smoothly in sequence and priority.

Chapter 4: Design

This chapter defines the results of the analysis of the preliminary design and the result of the detailed design. There is network system architecture, logical and physical design, possible scenarios, security requirement, metric measurement and the conclusion for this chapter.

Chapter 5: Implementation

This chapter will briefly describe about the activity involved in the implementation phase and what is the expected output after this phase is complete. Outline diagram also provided for this chapter.

Chapter 6: Testing and Analysis

In this testing and analysis chapter, the actual result of this project will be documented. This chapter also will briefly describe about the activity involved in the implementation phase of this project.

Chapter 7: Project Conclusion

This final chapter will be the project conclusion that will review on the limitation and the contribution for this project and the future works that can be done through this analysis.

1.8 Conclusion

This chapter explains the introduction of this project that defines malware and the analysis, also explains about the problem statement that describe of problems that directly influence the motives of the project, project question is arise from the problem statement and need to be answered in this project, while project objectives describe the things that this project need to achieve. The Project scope describes every scope involved and their reasons. The project contribution describes who or what may benefit from the project and lastly report organization that give a summary of each chapter presented in this report.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

This chapter presents the related works or previous works related to analyzing ransomware, critical review of current problem and justification where it explains about the methodologies, techniques, parameter, software and hardware that being used in other research. It also covers the proposed solution based on the previous research. The comparison has been made to highlight the differences.

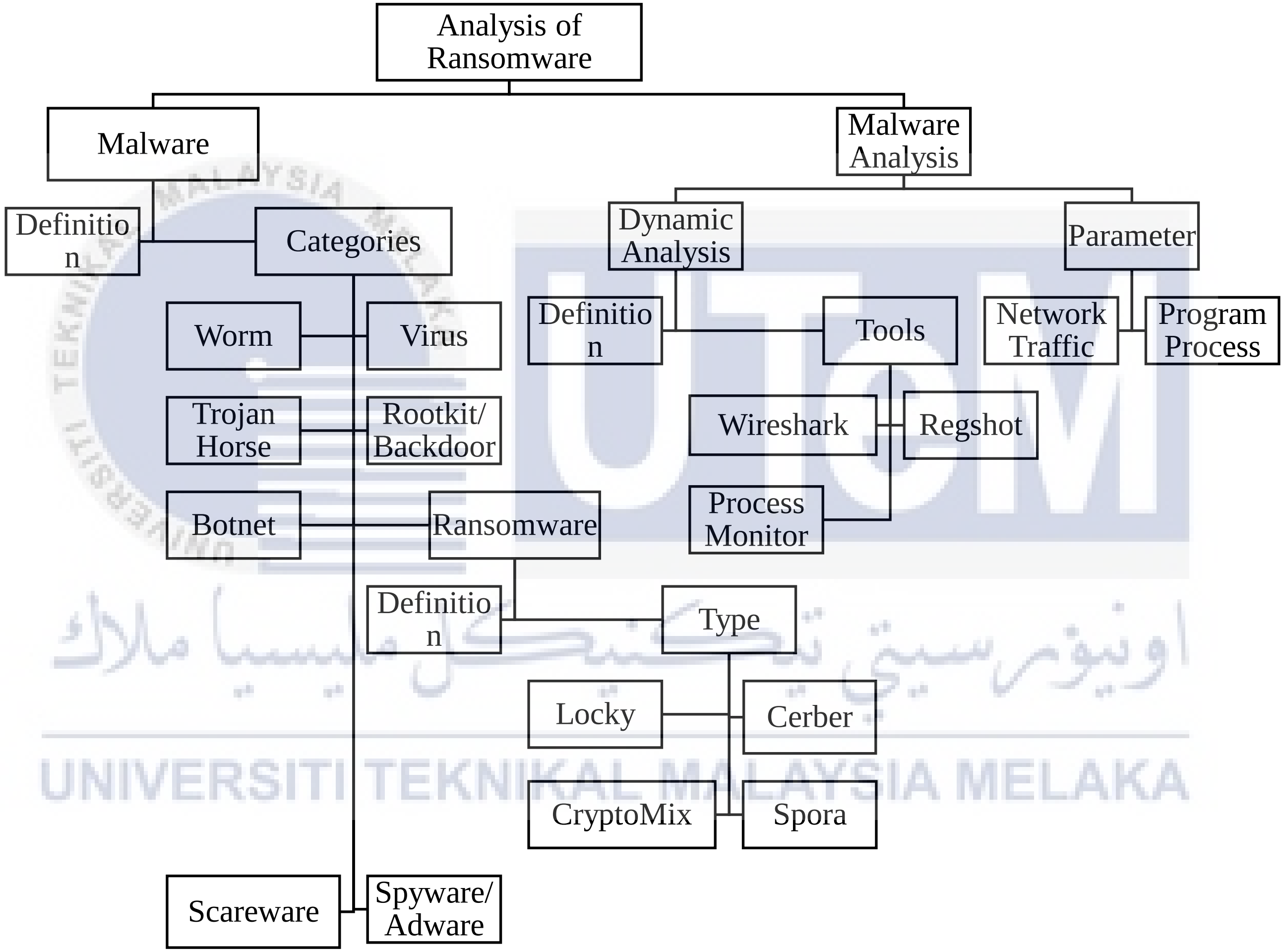


Figure 2.1 Taxonomy of Malware Analysis

2.2 Critical review of current problem and justification

2.2.1 Malware

Malicious software, or malware, is used by cybercriminals, hacktivists and nation states to disrupt computer operations, steal personal or professional data, bypass access controls and other wise cause harm to the host system. Appearing in the form of executable code, scripts, active content or other software variants, there are many different classes of malware which possess varying means of infecting machines and propagating themselves.

2.2.1.1 Worm

A worm is self-replicating software designed to spread through the network. Typically, exploit security flaws in widely used services can cause enormous damage. Worm also launch DDOS attacks, install bot network to access sensitive information and cause confusion by corrupting the sensitive information.

2.2.1.2 Virus

Virus is a tiny program that able to exploit and negatively alters the way a computer works. It able to automatically replicate itself, done without user knowledge or intervention but still needs to be activated initially by the user either time based or activity based. Viruses often spread to other computers by attaching themselves to various programs and executing code. This malware can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

2.2.1.3 Trojan Horse

Trojan Horse is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. Trojan Horse give a malicious party remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to steal data (logins, financial data, and even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, etc.), use the computer in botnets, and anonymize internet activity by the attacker.

2.2.1.4 Rootkit/ Backdoor

A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet. Rootkit prevention, detection, and removal can be difficult due to their stealthy operation because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits. As a result, rootkit detection relies on manual methods such as monitoring computer behavior for irregular activity, signature scanning, and storage dump analysis.

2.2.1.5 Botnet

Bots are software programs created to automatically perform specific operations. While some bots are created for relatively harmless purposes (video gaming, internet auctions, online contests, etc.), it is becoming increasingly common to see bots being used maliciously. Bots can be used in botnets (collections of computers to be controlled by third parties) for DDoS attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites. Websites can guard against bots with CAPTCHA tests that verify users as human.

2.2.1.6 Ransomware

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom. This malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove. Ransomware typically spreads like a normal computer worm ending up on a computer via a downloaded file or through some other vulnerability in a network service. Afraidgate, PseudoDarKleech, CryptoMix, Spora are the name of the ransomware that this project analyzes.

2.2.1.7 Scareware

Scareware is a class of malware known as scareware has become popular among cybercriminals. This malware takes advantage of people’s fear of revealing their private information, losing their critical data, or facing irreversible hardware damage.

2.2.1.8 Spyware/ Adware

Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections. Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans. While adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements. Common examples of adware include popup ads on websites and advertisements that are displayed by software. Often time’s software and applications offer “free” versions that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a revenue generating tool.

2.2.2 Malware Analysis

Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. It goals are to determine exactly what happened, and to ensure the location of all the infected machines and files, also to determine exactly what a suspect binary can do, how to detect it on the network, and how to measure and contain its damage. Once identify which files require full analysis, it's time to develop signatures to detect malware infections on the network. It also Known as Reverse Engineering (RE).

2.2.3 Dynamic Analysis

Dynamic analysis by analyzing a program while it executes. The advantage is it can be fast and accurate. The disadvantage, it is "what you see is what you get". Some of the analysis process are process monitoring, registry monitoring, file monitoring and network sniffing using Wireshark. In dynamic analysis, the Regshot used to captures file registry and use Process Monitor Software as tool for capture program activities also.

2.2.4 Parameter

The parameter of this project consists of the by tracing ransomware activities on the network traffic and program process flow. This project also looking at the file system analysis.

2.3 Previous Project

Table 2.1: Summary of Study and Analysis of Previous Works

No.	Author & Years	Aim/ Objective	Technique	Methods	Parameters	Results
1.	(CABAJ, 2015)	To gain actions made by the malware within the infected machine and tracing its activity over the Internet.	Network activity analysis of CryptoWall ransomware.	In this approach, a HoneyPot technology as well as the automatic run-time malware analytical system called Maltester were used.	Dynamic analysis may provide several types of information, so, it is worth to distinguish two kinds of analyses – each require different techniques and have different goals: actions made by the malware within the infected machine and tracing its activity over the	The presented analysis and its results proves the advantages and usefulness of dynamic analysis concept and Maltester environment. Identification

					Internet. In the first case, the scope of damage can identified on the infected host.	
2.	Elekar, (2015)(Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015)	To detect a significant number of ransomware attacks without making any assumptions on how samples attack users' file.	A long-term analysis of ransomware families with a special focus on their destructive functionality.	They also observed that different classes of ransomware attacks with multiple levels of sophistication share very similar characteristics from file system perspective due to the nature of these attacks	Their analysis suggests that implementing practical defense mechanisms is still possible, if effectively monitor the file system activity for example the changes in Master File Table (MFT) or the types of I/O Request Packets (IRP) generated on behalf of processes to access the file system	When looking at the execution traces of the malware programs, they observed that the way malicious processes generate requests to access file system was significantly different from benign processes.

3.	(Scaife, Carter, Traynor, & Butler, 2016)	To limit attackers and reduce the incentive for victims to pay with CryptoDrop, an early-warning system for ransomware attacks.	Their solution targets ransomware by monitoring the victim’s data and detecting the behaviors that ransomware must perform.	They first identify these required operations, classify ransomware into three major classes, and develop indicators that inspect, capture, and alert on ransomware while avoiding benign applications.	• File Type Changes • Similarity Measurement • Shannon Entropy • Secondary Indicators • Union Indication • Indicator Evasion	They find a 100% detection rate with as few as zero victim files lost before detection. They discover that ransomware frequently trips all of these primary indicators, while legitimate applications do not, creating a shortcut to detecting ransomware with fewer files lost.
4.	(Sharma, Zawar, & Patil, 2016)	To look at where and when the Ransomware attacks worked, not just from a geographical point	They collect mix of binary-file-based locker Ransomware		• Analysis of Locker Ransomware Vs Crypto	64% of binary-based Ransomware families observed have been crypto Ransomware while locker

		of view but also from operating system viewpoint.	versus crypto Ransomware in the past 12 months.		Ransomware 2014-2015. • Yearly evolution of Ransomware Attacks based on OS • Percentage of attacked user's over the countries. • Number of users affected worldwide quarterly due to Ransomware. • TOP 10 countries by percentage of attacked users	Ransomware made up the remaining 36%.

2.4 Further Project

This project proposed solution is by looking at the network traffic and program process. This research uses the dynamic analysis approach to see the behavior of ransomware through virtual machine software (VMware). A set of personal computers was setup within the installation of monitoring tools such as Wireshark, Process Monitor, and Regshot. The malware will be installed into the virtual OS or application and then the behavior will be observed and recorded. The behavior of the application before and after the malware infection also will be compared and analyzed.

2.5 Conclusion

This chapter discuss about the related work, critical review of current problem and justification, and proposed solution or further project. The taxonomy also provided in this chapter where it explains about the definition of malware, and types of malware. The details information about ransomware also explained in this chapter such as it general attack pattern, the mechanism and the parameter used to analyze this type of malware.

CHAPTER III

PROJECT METHODOLOGY

3.1 Introduction

This chapter discuss on the methodology that is chosen to prepare for this project. This chapter also reveals the milestone of the project that is done according to the methodology phases. There are four phases on project methodology which is Literature Review, Analysis, Designs and Implementation and the last is Testing and Evaluation. The framework of project methodology described in figures below.

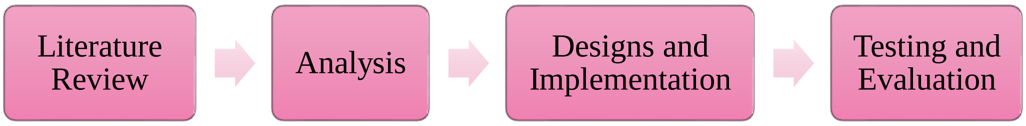


Figure 3.1: Project Methodology

3.2 Methodology

There are four phases for the methodology of analysis of ransomware behavior. Each phases description shows on the below figures.

3.2.1 Phase 1: Literature Review

In this phase, all related study about ransomware including Ransomware, attack pattern and malware analysis where be done in this phase. The process of understanding malware, attack pattern and malware analysis are selected in sequence as illustrated in Figure 3.1.

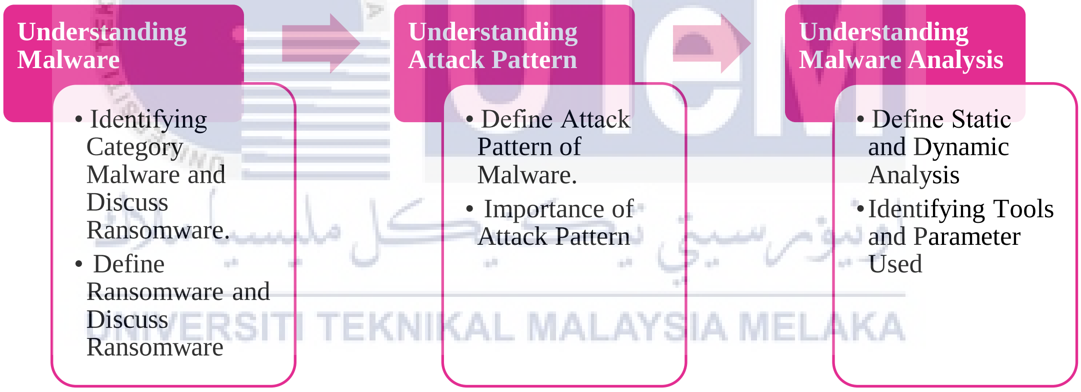

Understanding Malware
• Identifying Category Malware and Discuss Ransomware.
• Define Ransomware and Discuss Ransomware
Understanding Attack Pattern
• Define Attack Pattern of Malware.
• Importance of Attack Pattern
Understanding Malware Analysis
• Define Static and Dynamic Analysis
• Identifying Tools and Parameter Used

Figure 3.2: Literature Review

The result of study is used for next phase which is analysis phase.

3.2.2 Phase 2: Analysis

Dynamic analysis is carried out in this project to observe the ransomware behavior and monitor the changes made by this malware. This analysis focus on the network traffic and the program process. Some samples of ransomware are executed on the Windows 7 operating system in an isolated environment with virtual machine software, Regshot, Wireshark, and Process Monitor. Network monitoring tools such as Wireshark are used for capturing and collecting network activities including for detecting anomalous network traffic between the malware and its remote server. Process Monitor displays and captures all changes made by any process running on a system while the Regshot takes a snapshot of the Windows registry hives. The process of understanding dynamic analysis, analysis collected data and identifying the parameter and behavior of ransomware are selected in the sequence as illustrated in Figure 3.2

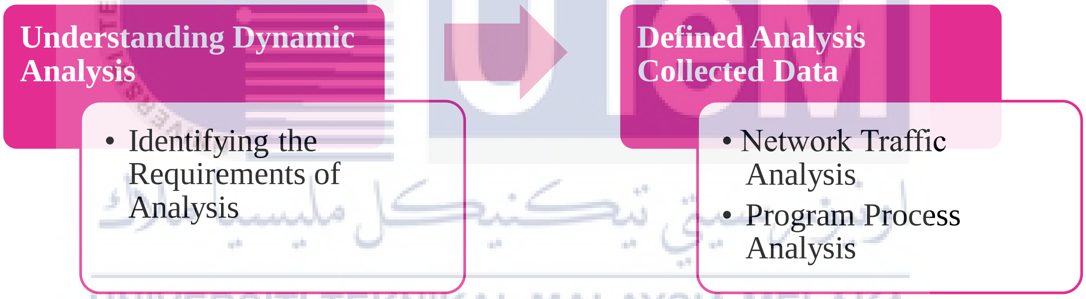

Understanding Dynamic Analysis
• Identifying the Requirements of Analysis
Defined Analysis Collected Data
• Network Traffic Analysis
• Program Process Analysis

Figure 3.3: Analysis

3.2.3 Phase 3: Designs and Implementation.

Regarding Figure 3.4, there are three issues involved in this phase which are malware detection technique, alert correlation technique and alert correlation framework’s module which has been reviewed and discussed previously in Chapter Two.

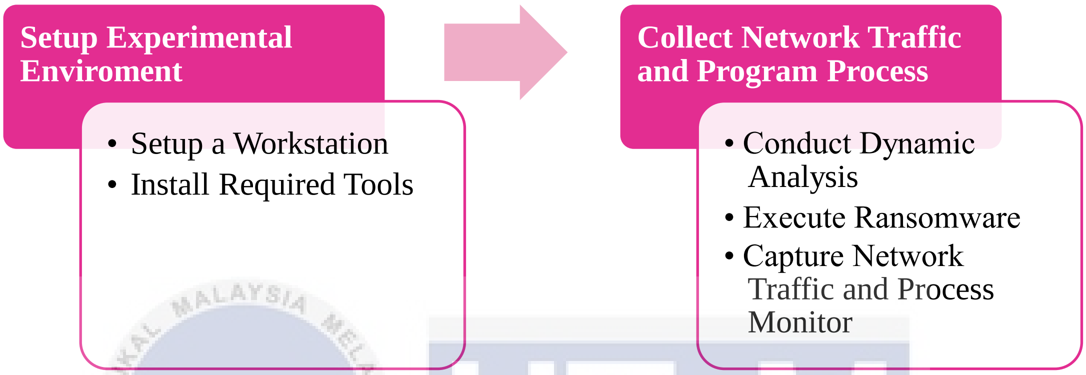

Setup Experimental Enviroment
• Setup a Workstation
• Install Required Tools
Collect Network Traffic and Program Process
• Conduct Dynamic Analysis
• Execute Ransomware
• Capture Network Traffic and Process Monitor

Figure 3.4: Designs and Implementation

3.2.4 Phase 4: Testing and Analysis

Testing and evaluation phase is important to verify whether the selected attributes will generate the right attack pattern or not. Script designing will be used to test on selected sample ransomware to verify the result of attack pattern generated in design and implementation phase. Besides, the testing will be carried out by comparing output results with static analysis on ransomware thus verify the result of attributes and attack patterns getting from dynamic analysis.

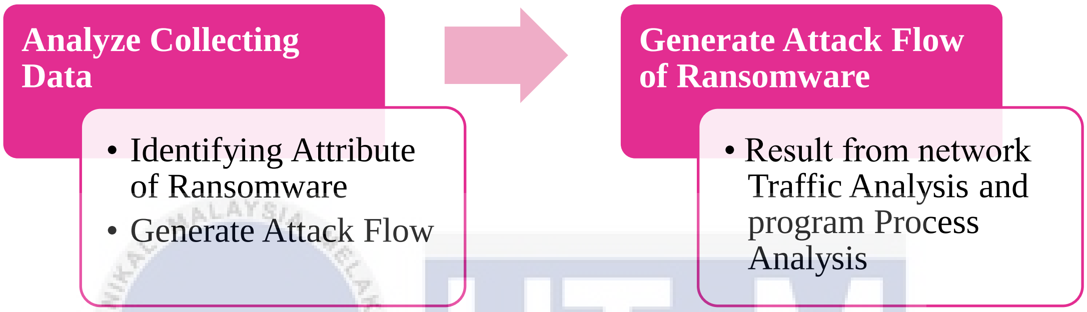

Analyze Collecting Data
• Identifying Attribute of Ransomware
• Generate Attack Flow
Generate Attack Flow of Ransomware
• Result from network Traffic Analysis and program Process Analysis

Figure 3.5: Testing and Analysis

3.3 Project Milestone

The milestone of this project help to keep us in our track to be able to complete this project according to the given time.

Table 3.1: Project Milestones

Week	Activity	Action
1 13 – 17 February 2017	Proposal Submission	Proposal submission Topic research
2 20 – 24 February 2017	Proposal Enhancement	Proposal correction Topic research
3 27 Feb – 3 Mar 2017	Chapter 1	Device application and setup (1 set of personal computers) Topic research
4 6 – 10 Mar 2017	Chapter 2	Formatting device Topic research
5 13 – 17 Mar 2017	Chapter 3	Installation of driver Topic research
6 20 – 24 Mar 2017	Chapter 3	Installation of virtual machine software Topic research
7 27 – 31 Mar 2017	Chapter 4	Installation of operating system in virtual machine Topic research
8 **1 – 9 April 2017**	**Mid Semester Break**	**Research**
9 10 – 14 April 2017	Chapter 4	Installing tools for analysis Topic research
10 17 – 21 April 2017	Chapter 4	Collecting normal behavior of the application
11 24 – 28 April 2017	Chapter 4	Collecting normal behavior of the application

12 1 – 5 May 2017	Chapter 5	Collecting normal behavior of the application
13 8 – 12 May 2017	Chapter 5	Collecting normal behavior of the application
14 15 – 19 May 2017	Chapter 5	Collecting information of the application after the infection of the malware
15 22 – 26 May 2017	Chapter 5	Collecting information of the application after the infection of the malware
16 29 May – 2 June 2017	Chapter 5	Collecting information of the application after the infection of the malware
3 – 11 June 2017	**Semester Break**	**Research**
12 – 16 June 2017	Chapter 6	Complete the result of the project. Generate attack flow.
19 – 23 June 2017	Chapter 6	Complete the result of the project.
26 – 30 June 2017	Chapter 6	Complete the result of the project.
3 – 7 July 2017	Chapter 7	Complete the conclusion of the project
10 – 14 July 2017	Chapter 7	Complete the conclusion of the project
17 – 21 July 2017	Chapter 7	Complete the conclusion of the project
24 – 28 July 2017	Documenting Result	Documenting the project findings
31 July – 4 August 2017	Documenting Result	Documenting the project findings
7 – 11 August 2017	Documenting Result	Documenting the project findings

14 – 18 August 2017	Final Presentation	Presenting the project result to the supervisor and evaluator

3.4 Conclusion

This chapter is about the methodology that is used in the project and the description of each step. The milestones of this project are also included to keep students on track. The next chapter will be discussing on the design of the project and the implementation of the project.

CHAPTER IV

DESIGN

4.1 Introduction

This chapter defines the results of the analysis of the preliminary design and the result of the detailed design. There is network system architecture, logical, design, security requirement, and the conclusion for this chapter.

4.2 Ransomware Analysis Approach

In this section, both experimental and analysis design will be discussed.

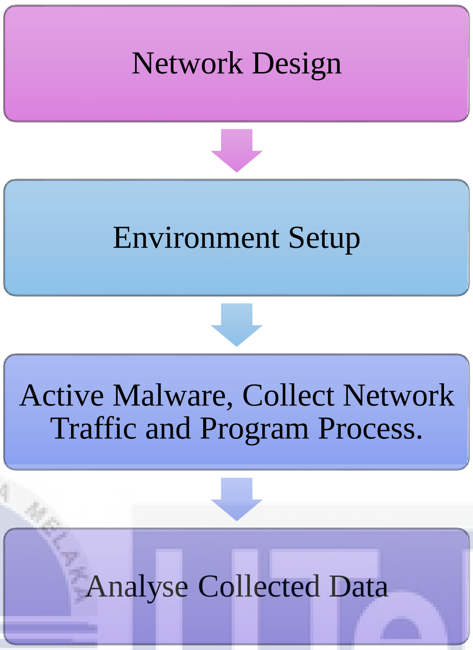

Network Design
Environment Setup
Active Malware, Collect Network Traffic and Program Process.
Analyse Collected Data

Figure 4.1: Analysis Approach

Figure 4.1 shows step by step to carry out the process of analysis ransomware. Next, first step which is network setup will be discussed further. While the second step environmental setup, third step active malware, collect network traffic and program process and the last step analyze collected data discussed in Chapter 5.

4.3 Logical and Physical Design

4.3.1 Logical Design

Figure 4.2 below shows the logical design of malware analysis environment, which consist of a workstation, one switch, one router, one virtual workstation and one malware remote server. The internet is connected.

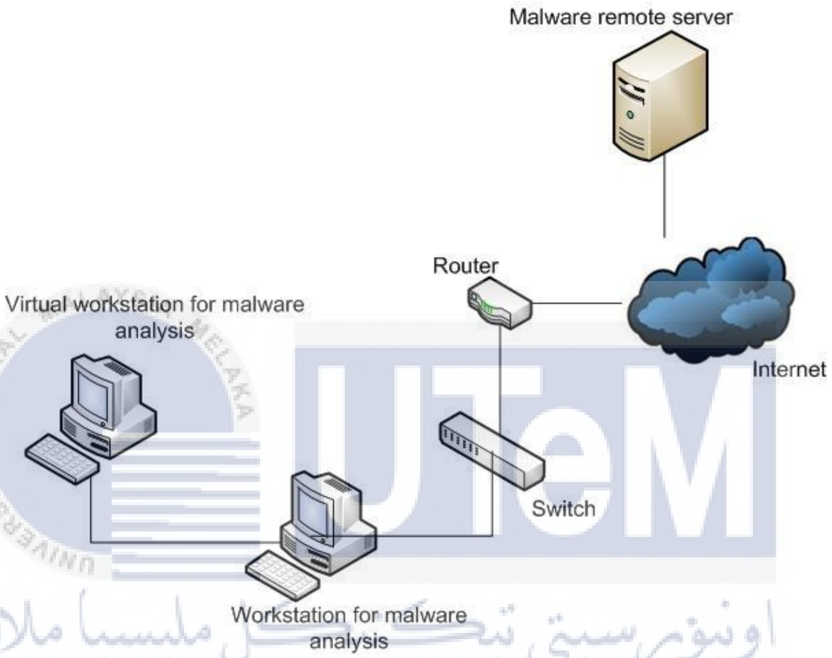

Malware remote server
Router
Virtual workstation for malware analysis
Internet
Switch
Workstation for malware analysis

Figure 4.2 Logical Design

A virtual workstation created to infects the ransomware on it. Then the workstation captured the data of network traffic and program process thus analyze the data collected.

4.3.2 Physical Design

This project does not need physical design because it only uses single personal computer equipped with virtual machine.

4.4 Requirement

4.4.1 Software Requirement

i. **Windows 7**

An operating system which is Windows 7 as a basic platform to install all the software required such as Wireshark, Process Monitor, Regshot.

ii. **VMware Workstation**

VMware's VM stands for virtual machine. It is software that offers a virtualization of Operating Systems. It also acts as a cloud computing software provider for x86 computers. It is developed by VMware Inc. The operating system installed in this VMware will have its own set of programs, as it has in its normal environment, and it can also connect to the internet as usual, if the host computer of the VMware has connection to the internet. The functions and operations of the virtual operating system will not be any differ from non-virtual operating systems.

iii. **Wireshark**

A network analysis monitoring tool which capture network packets in real time and tries to display that packet data in detailed and human-readable format. The features include in Wireshark are filters, color-coding etc. Wireshark is one of the most powerful tools in a network security analyst's toolkit.

iv. **Regshot**

This tool takes a snapshot of the Windows registry hives. For the purposes of this analysis, snapshot is taken before the malware is executed and another afterwards. Regshot then has the ability to juxtapose the two snapshots and display the results in manner that is easy to identify the differences and observe what changes the malware makes to registry settings.

v. **Process Monitor**

Process Monitors shows the monitors registry, file system, network, process, and thread activity. Process Monitor can filter the display to find items of interest easily even though all recorded events are kept. The machine will crash if it run it too long because it fills up all RAM. Process Monitor provides helpful automatic filters on its toolbar. This software allows us to examining registry operations, it can tell how a piece of malware installs itself in the registry. For the File System Exploring, file system interaction can show all files that the malware creates or configuration files it uses. While Process Activity Investigating, process activity can tell you whether the malware spawned additional processes and Network Identifying network connections can show you any ports on which the malware is listening.

4.4.2 Hardware Requirement

Hardware is chosen as workstation of project. Table 4.1 shows the details of hardware requirement.

Table 4.1: Details of hardware requirements

Device	CPU
Manufacture	Dell Inc.
Model	Dell OptiPlex 7010
Processor	Intel® Core™ i5 (3rd Gen) 3470 / 3.2 Ghz
Installed Memory (RAM)	2GB
Storage	250GB
System Table	32-bit Windows 7 Operating System

Thus, all the software requirements installed in the workstation for preceding the ransomware analysis.

4.5 Conclusion

This chapter is mainly about the design of the proposed project. Basically, it will further discuss about the requirements of software and hardware for environment setup, experimental design including the logical design.

CHAPTER V

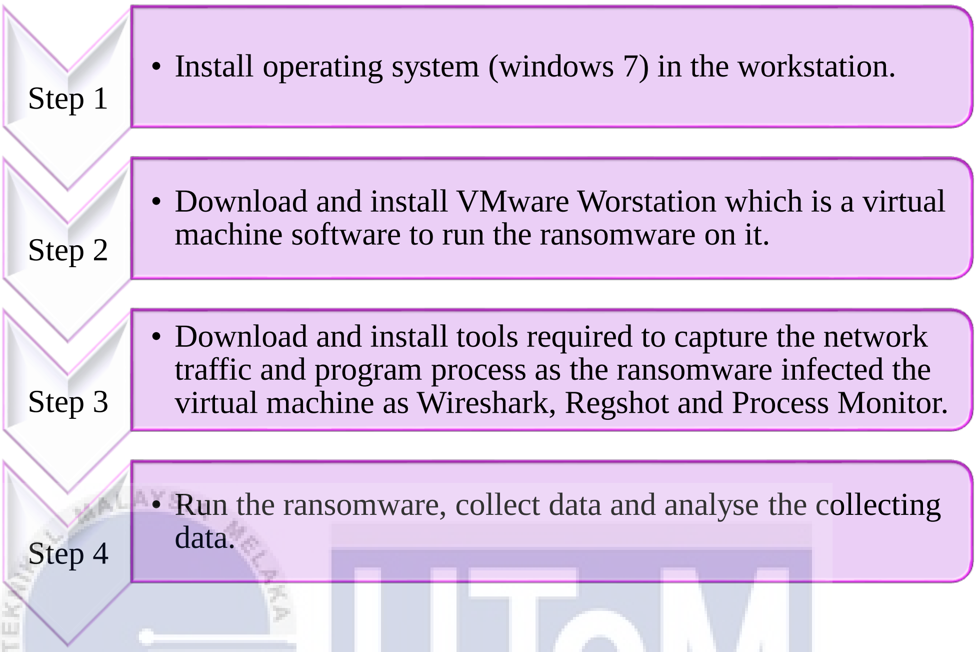
IMPLEMENTATION

5.1 Introduction

In this chapter, this project are discussing the experimental setup, process of malware analysis, thus explained how malware analysis is carried out on the process of collecting data and analyze collected data at the end of this chapter. More explanation about the ransomware analysis approach for the second step environmental setup stated in this chapter.

5.2 Environment Setup

Based on the network design, the actual environment will be setup as steps below to collect the data of network traffic and program process.



Step 1

- Install operating system (windows 7) in the workstation.

Step 2

- Download and install VMware Worstation which is a virtual machine software to run the ransomware on it.

Step 3

- Download and install tools required to capture the network traffic and program process as the ransomware infected the virtual machine as Wireshark, Regshot and Process Monitor.

Step 4

- Run the ransomware, collect data and analyse the collecting data.

Figure 5.1 Steps on Environmental Setup

During performing malware analysis, is isolated environment is needed to prevent the malware outbreak the network connection. The data in network traffic and program process collected for the next step.

5.3 Active Malware, Collect Network Traffic and Program Process

In this section, the process of collected data of network traffic is elaborated.

5.3.1 Process Collect Network Traffic Data

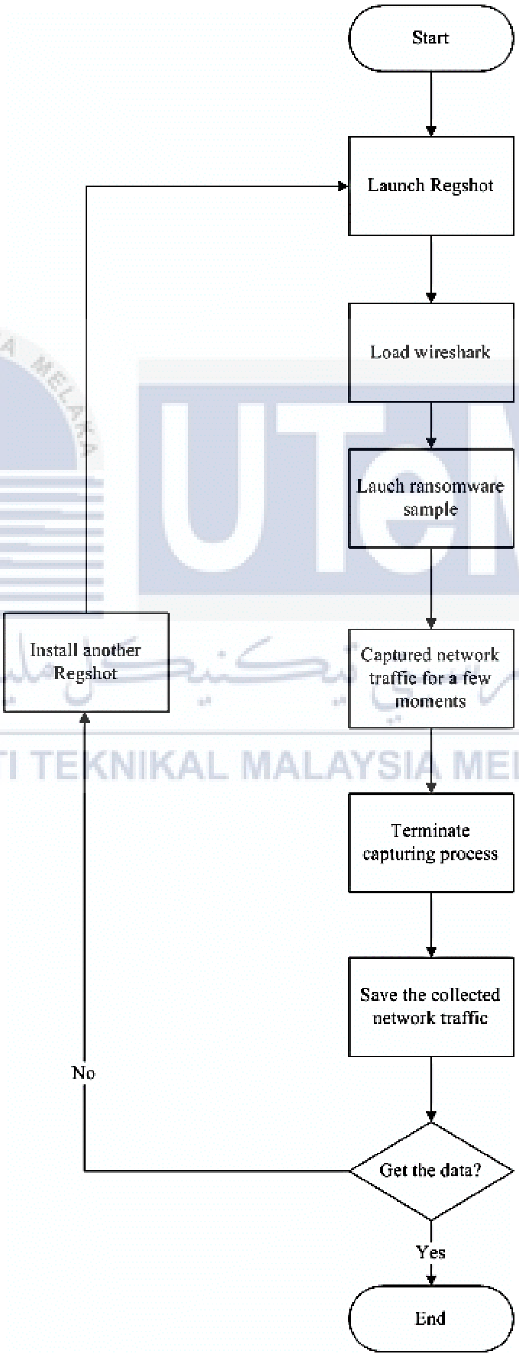

Start
Launch Regshot
Load wireshark
Lauch ransomware sample
Captured network traffic for a few moments
Terminate capturing process
Save the collected network traffic
Get the data?
Yes
End
No
Install another Regshot

Figure 5.2 Process of Collect Network Traffic

Sample 1: 2016-12-23-Afraidgate-Rig-V-sends-Locky-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Launch Regshot and click the 1st **shot** button.

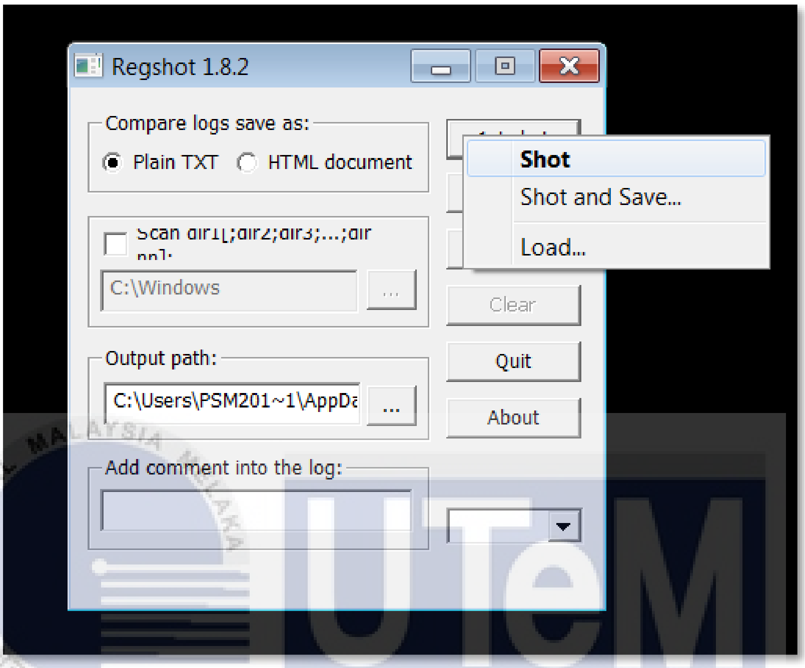


Figure 5.3 Select 1st shot from this screen

After launch Regshot, the display is as **Figure 5.3** and it will show the changes occur in registry from the time for first snapshot and the second snapshot. The first snapshot will automatically stop in a few minutes after button **Shot** is clicked.

Step 2: Load Wireshark and begin a packet capture on your local interface.

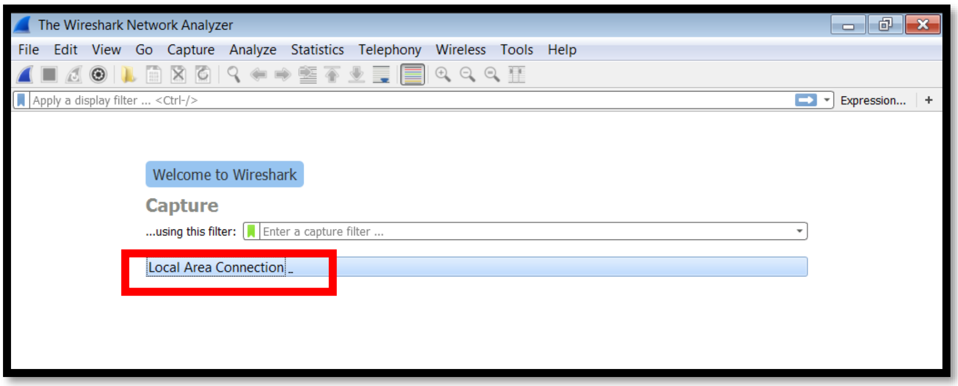
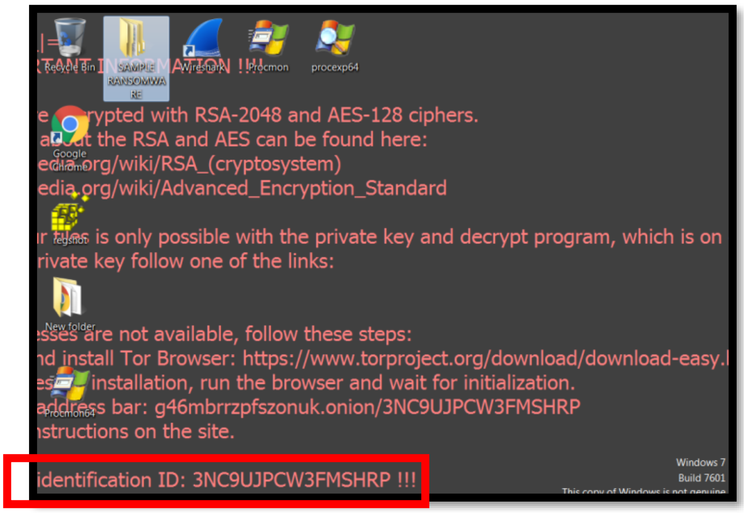

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Local Area Connection

Figure 5.4 Select your Local Area Connection and then click Start

For **Figure 5.4** above, double click the **Local Area Connection** to start packet capture of the network activities when the ransomware infecting the system.

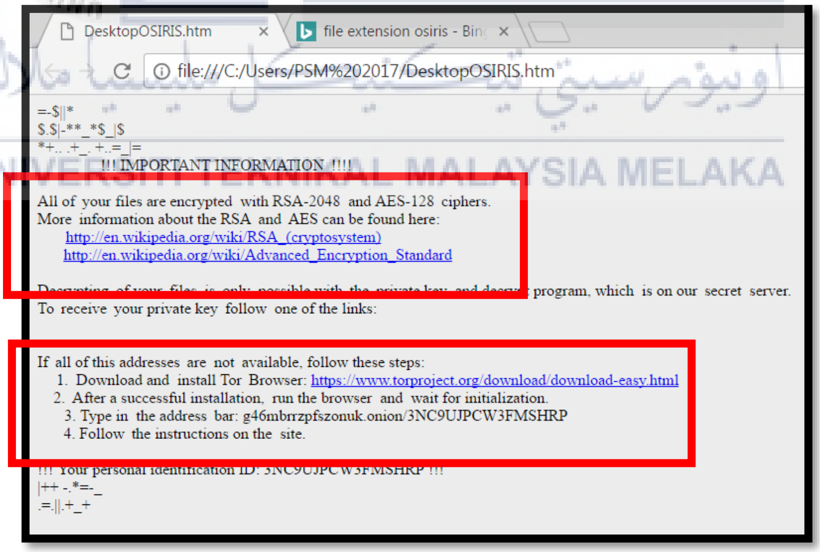
Step 3: Launch the **Locky** ransomware sample. After a few moments, the **Locky** ransomware screen will display.



```
|=
TANT INFORMATION !!!!
e    rypted with RSA-2048 and AES-128 ciphers.
a    t the RSA and AES can be found here:
edia.org/wiki/RSA_(cryptosystem)
edia.org/wiki/Advanced_Encryption_Standard

r files is only possible with the private key and decrypt program, which is on
rivate key follow one of the links:

sses are not available, follow these steps:
nd install Tor Browser: https://www.torproject.org/download/download-easy.
es    installation, run the browser and wait for initialization.
address bar: g46mbrrzpfszonuk.onion/3NC9UJPCW3FMSHRP
nstructions on the site.

identification ID: 3NC9UJPCW3FMSHRP !!!
```

Figure 5.5 Locky ransomware screen

Once executed this picture replaced the normal desktop background. As shows in the **Figure 5.5**, the owner of this ransomware provides the **identification ID: 3NC9UJPCW3FMSHRP** for the victim use to pay an amount of money to decrypt the encrypted file cause by the ransomware.



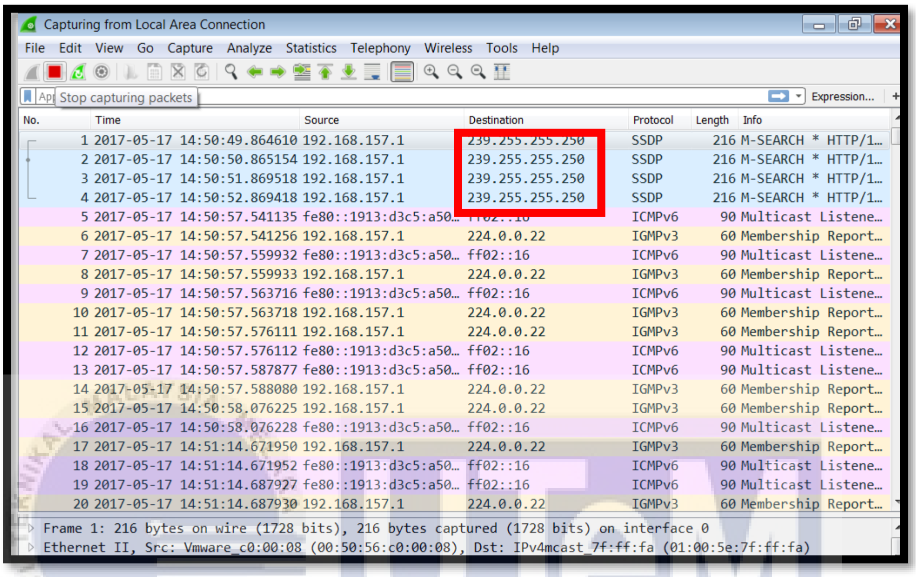
DesktopOSIRIS.htm
file extension osiris - Bing
file:///C:/Users/PSM%202017/DesktopOSIRIS.htm

```
=-$||*
$.$|-**_*$_|$
*+.. .+_. +.=_|=
      !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:


If all of this addresses are not available, follow these steps:
  1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
  2. After a successful installation, run the browser and wait for initialization.
   3. Type in the address bar: g46mbrrzpfszonuk.onion/3NC9UJPCW3FMSHRP
   4. Follow the instructions on the site.

!!! Your personal identification ID: 3NC9UJPCW3FMSHRP !!!
|++ -.*=-_
.=.||.+_+
```

Figure 5.6 File DesktopOSIRIS.htm displays in Google Chrome

Most ransomware variants also have a picture and a text file containing instructions on how to pay the ransom. As the **Figure 5.6**, the details information about the ransomware such as the type of encryption used to encrypt the victim files (**RSA-2048** and **AES-128)**, the ways to decrypt files and the steps to pay ransom.

Step 4: Stop the Wireshark packet capture and save the results to the desktop.

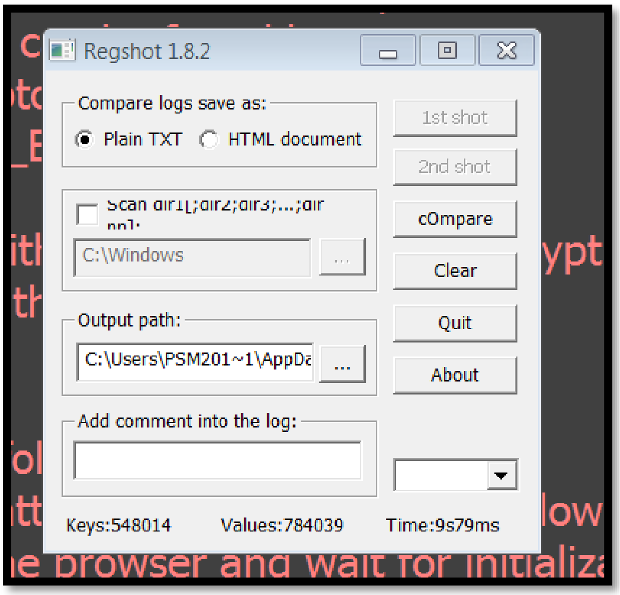

Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Stop capturing packets
Expression...

```
No.   Time                       Source                  Destination      Protocol  Length Info
    1 2017-05-17 14:50:49.864610 192.168.157.1           239.255.255.250  SSDP       216 M-SEARCH * HTTP/1…
    2 2017-05-17 14:50:50.865154 192.168.157.1           239.255.255.250  SSDP       216 M-SEARCH * HTTP/1…
    3 2017-05-17 14:50:51.869518 192.168.157.1           239.255.255.250  SSDP       216 M-SEARCH * HTTP/1…
    4 2017-05-17 14:50:52.869418 192.168.157.1           239.255.255.250  SSDP       216 M-SEARCH * HTTP/1…
    5 2017-05-17 14:50:57.541135 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
    6 2017-05-17 14:50:57.541256 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…
    7 2017-05-17 14:50:57.559932 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
    8 2017-05-17 14:50:57.559933 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…
    9 2017-05-17 14:50:57.563716 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
   10 2017-05-17 14:50:57.563718 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…
   11 2017-05-17 14:50:57.576111 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…
   12 2017-05-17 14:50:57.576112 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
   13 2017-05-17 14:50:57.587877 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
   14 2017-05-17 14:50:57.588080 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…
   15 2017-05-17 14:50:58.076225 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…
   16 2017-05-17 14:50:58.076228 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
   17 2017-05-17 14:51:14.671950 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…
   18 2017-05-17 14:51:14.671952 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
   19 2017-05-17 14:51:14.687927 fe80::1913:d3c5:a50…   ff02::16         ICMPv6      90 Multicast Listene…
   20 2017-05-17 14:51:14.687930 192.168.157.1           224.0.0.22       IGMPv3      60 Membership Report…

▷ Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
▷ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
```

Figure 5.7 Results from the Wireshark packet capture

Based on the **Figure 5.7**, after a few minutes the ransomware infecting the system, it can stop the packet capture and save the file to analyses the network activities of this malware. As example, the figure above shows this ransomware involved most **239.255.255.250** as Source IP Address. When search it on “whois” it shows owned by Internet Assigned Numbers Authority (IANA).

Step 5: Open Regshot and press the 2nd shot button.



Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]: C:\Windows

Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:548014 Values:784039 Time:9s79ms

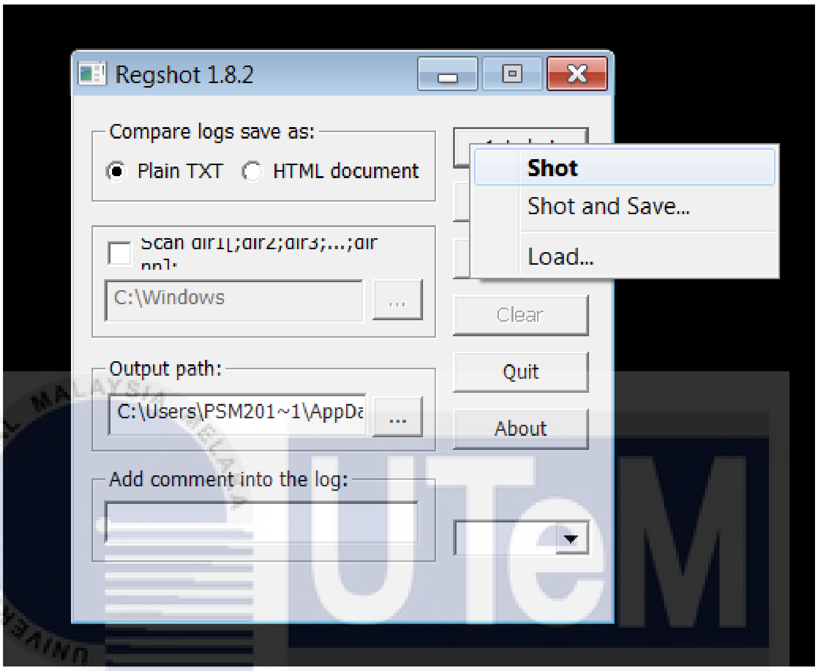
Figure 5.8 Regshot after 2nd shot

Once this is complete, press the Compare button and save the results to the desktop. Regshot gives you the option to save your comparison as plain text or HTML as in **Figure 5.8**. After the shot, it can compare the keys deleted, keys added, values deleted and total changes in registry.

Sample 2: 2017-01-05-psuedoDarkleech-Rig-V-sends-Cerber-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Launch Regshot and click the 1st **shot** button.



Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

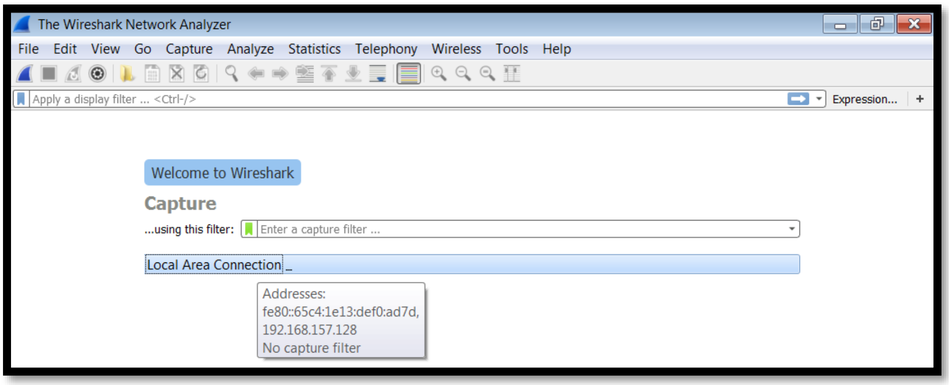
Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Figure 5.9 Select 1st shot from this screen

After launch Regshot, the display is as **Figure 5. 9** and it will show the changes occur in registry from the time for first snapshot and the second snapshot. The first snapshot will automatically stop in a few minutes after button **Shot** is clicked.

Step 2: Load Wireshark and begin a packet capture on your local interface.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Welcome to Wireshark
Capture

Apply a display filter ... <Ctrl-/>

...using this filter: Enter a capture filter ...

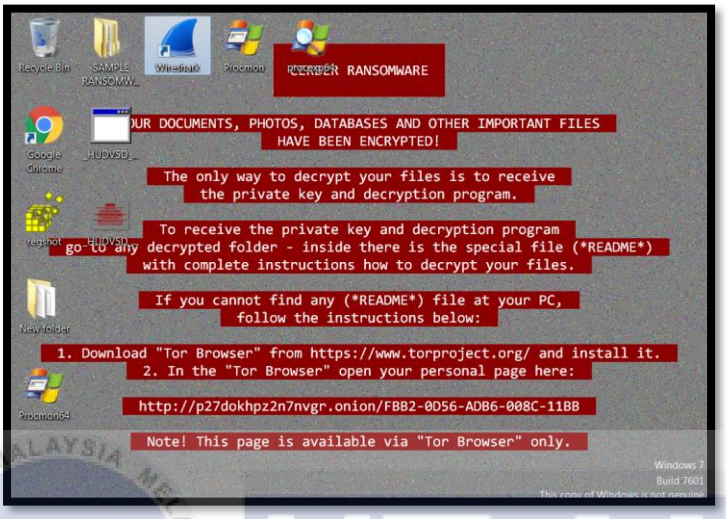
Local Area Connection

Addresses:
fe80::65c4:1e13:def0:ad7d,
192.168.157.128
No capture filter

Figure 5.10 Select your Local Area Connection and then click Start

For **Figure 5.10** above, double click the **Local Area Connection** to start packet capture of the network activities when the ransomware infecting the system.

Step 3: Launch the **Cerber** ransomware sample. After a few moments, the **Cerber** ransomware screen will display.



CERBER RANSOMWARE

OUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*README*)
with complete instructions how to decrypt your files.

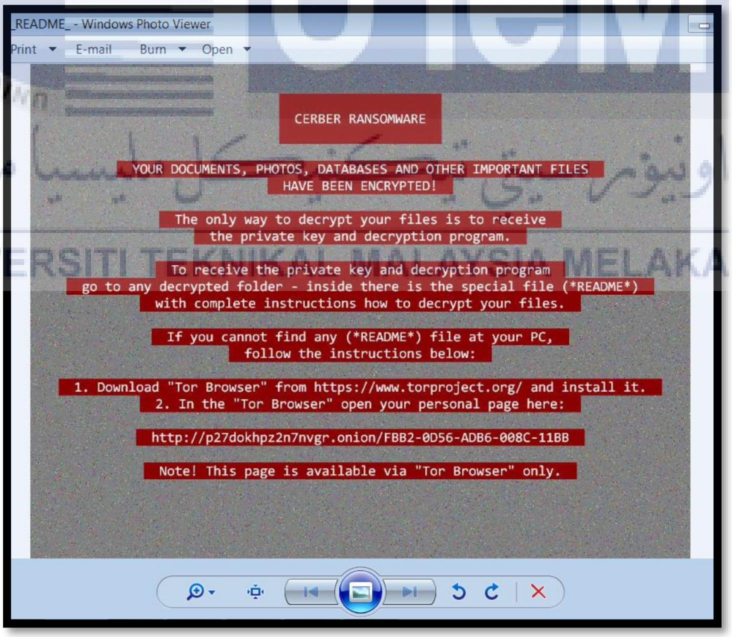
If you cannot find any (*README*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://p27dokhpz2n7nvgr.onion/FBB2-0D56-ADB6-008C-11BB

Note! This page is available via "Tor Browser" only.

Figure 5.11 Cerber ransomware screen



CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*README*)
with complete instructions how to decrypt your files.

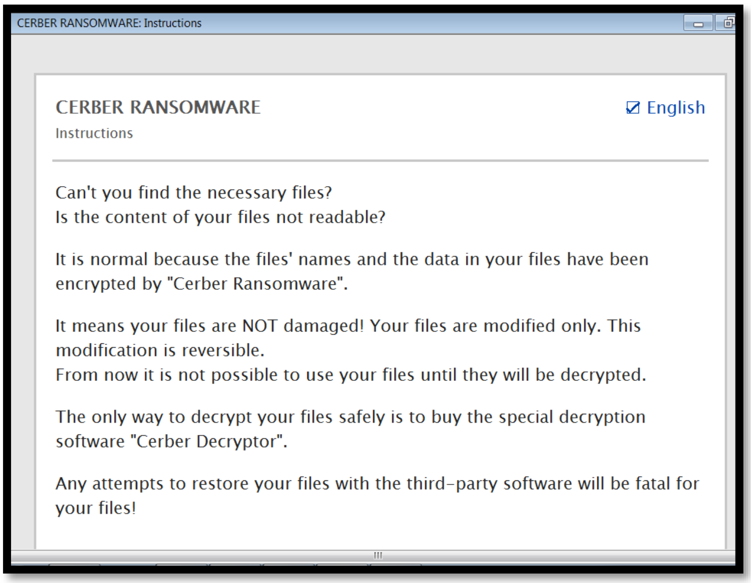
If you cannot find any (*README*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://p27dokhpz2n7nvgr.onion/FBB2-0D56-ADB6-008C-11BB

Note! This page is available via "Tor Browser" only.

Figure 5.12 Cerber ransomware screen



CERBER RANSOMWARE

Instructions

☑ English

Can't you find the necessary files?
Is the content of your files not readable?

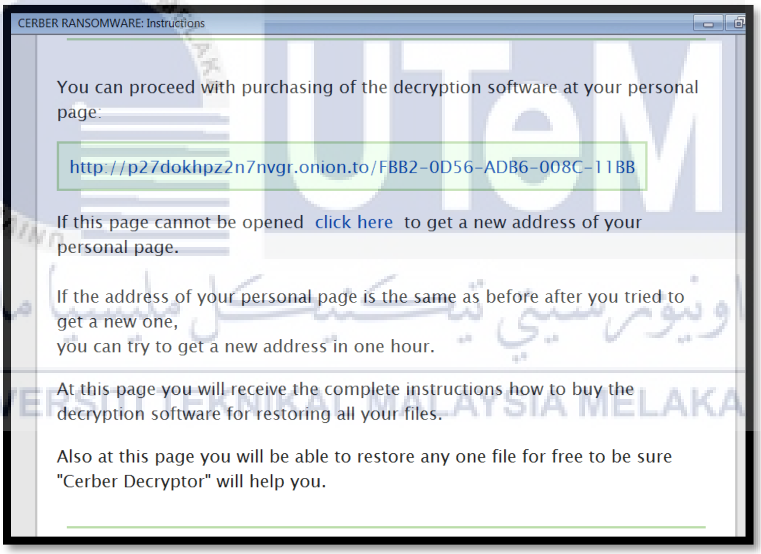
It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible.
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

Figure 5.13 Cerber ransomware screen



You can proceed with purchasing of the decryption software at your personal page:

http://p27dokhpz2n7nvgr.onion.to/FBB2-0D56-ADB6-008C-11BB

If this page cannot be opened click here to get a new address of your personal page.

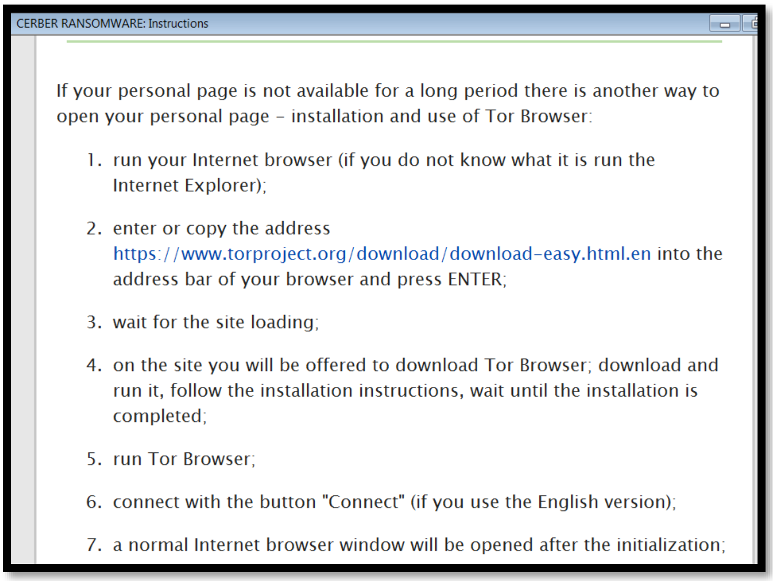
If the address of your personal page is the same as before after you tried to get a new one,
you can try to get a new address in one hour.

At this page you will receive the complete instructions how to buy the decryption software for restoring all your files.

Also at this page you will be able to restore any one file for free to be sure "Cerber Decryptor" will help you.

Figure 5.14 Cerber ransomware screen

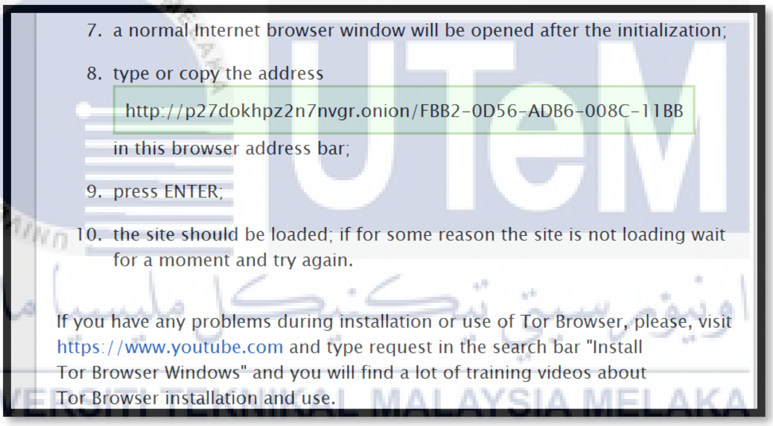
Cerber ransomware provide an image to the victim where the image contains instruction how to decrypt the file by pay the ransom. Cerber ransomware can encrypt database files: A new version of Cerber first discovered in October 2016 includes the ability to kill certain database processes in order to successfully encrypt data files. Researchers believe this change may indicate a shift to targeting businesses, specifically.


CERBER RANSOMWARE: Instructions

If your personal page is not available for a long period there is another way to open your personal page - installation and use of Tor Browser:

1. run your Internet browser (if you do not know what it is run the Internet Explorer);
2. enter or copy the address https://www.torproject.org/download/download-easy.html.en into the address bar of your browser and press ENTER;
3. wait for the site loading;
4. on the site you will be offered to download Tor Browser; download and run it, follow the installation instructions, wait until the installation is completed;
5. run Tor Browser;
6. connect with the button "Connect" (if you use the English version);
7. a normal Internet browser window will be opened after the initialization;

Figure 5.15 Cerber ransomware screen


7. a normal Internet browser window will be opened after the initialization;
8. type or copy the address

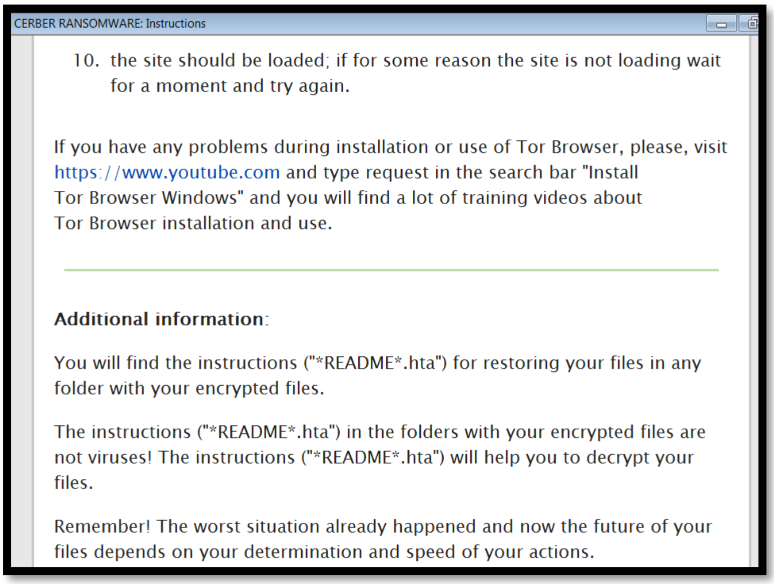
   http://p27dokhpz2n7nvgr.onion/FBB2-0D56-ADB6-008C-11BB

   in this browser address bar;
9. press ENTER;
10. the site should be loaded; if for some reason the site is not loading wait for a moment and try again.

If you have any problems during installation or use of Tor Browser, please, visit https://www.youtube.com and type request in the search bar "Install Tor Browser Windows" and you will find a lot of training videos about Tor Browser installation and use.

Figure 5.16 Cerber ransomware screen

Earlier version of Cerber renamed encrypted files with a .cerber extension. Newer versions now add a random file extension. Cerber also sports several novel features here this malware works offline: Cerber has the capability of operating without an active internet connection or need to connect to a command and control server (C&C). That means disconnecting an infected machine won’t stop encryption.



10. the site should be loaded; if for some reason the site is not loading wait for a moment and try again.

If you have any problems during installation or use of Tor Browser, please, visit https://www.youtube.com and type request in the search bar "Install Tor Browser Windows" and you will find a lot of training videos about Tor Browser installation and use.

Additional information:

You will find the instructions ("*README*.hta") for restoring your files in any folder with your encrypted files.

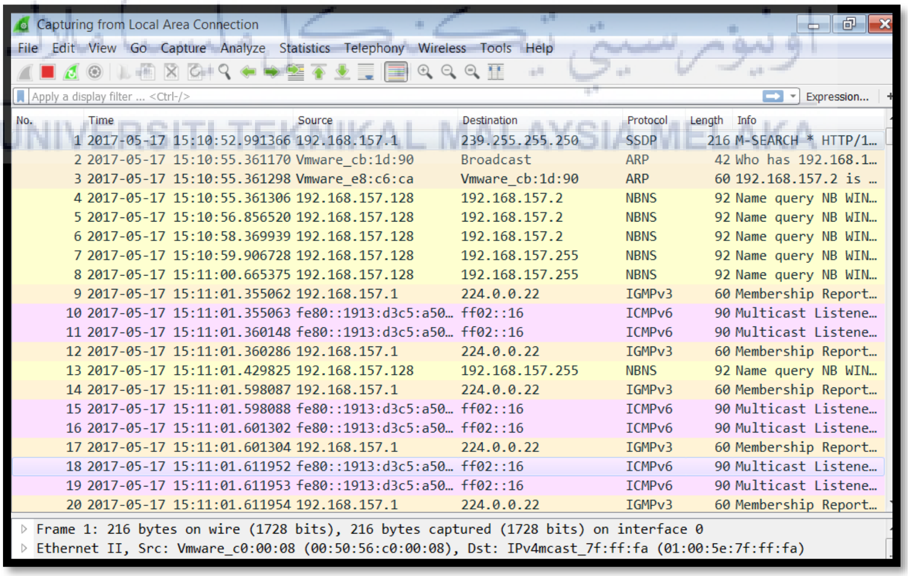
The instructions ("*README*.hta") in the folders with your encrypted files are not viruses! The instructions ("*README*.hta") will help you to decrypt your files.

Remember! The worst situation already happened and now the future of your files depends on your determination and speed of your actions.

Figure 5.17 Cerber ransomware screen

Most ransomware variants also have a picture and a text file containing instructions on how to pay the ransom. As the **Figure 5.11−5.17**, the details information about the ransomware such as the instruction to pay the ransom step-by-step within the link to **Cerber Decryption**.

Step 4: Stop the Wireshark packet capture and save the results to the desktop.



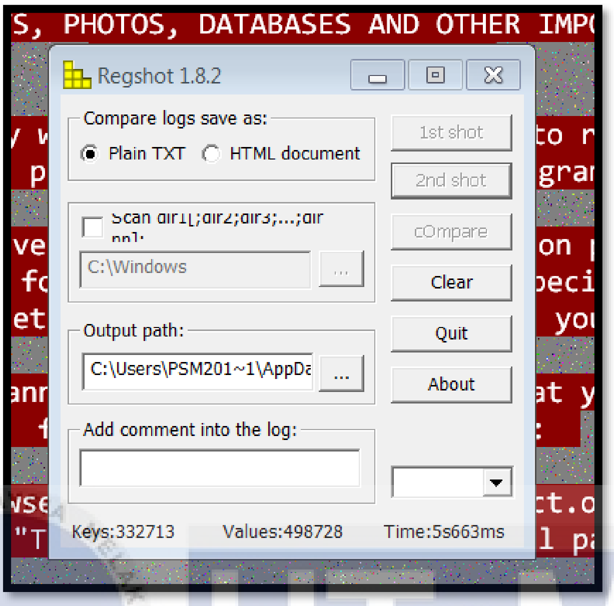
Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time                       Source                  Destination      Protocol  Length Info
    1 2017-05-17 15:10:52.991366 192.168.157.1           239.255.255.250  SSDP         216 M-SEARCH * HTTP/1…
    2 2017-05-17 15:10:55.361170 Vmware_cb:1d:90         Broadcast        ARP           42 Who has 192.168.1…
    3 2017-05-17 15:10:55.361298 Vmware_e8:c6:ca         Vmware_cb:1d:90  ARP           60 192.168.157.2 is …
    4 2017-05-17 15:10:55.361306 192.168.157.128         192.168.157.2    NBNS          92 Name query NB WIN…
    5 2017-05-17 15:10:56.856520 192.168.157.128         192.168.157.2    NBNS          92 Name query NB WIN…
    6 2017-05-17 15:10:58.369939 192.168.157.128         192.168.157.2    NBNS          92 Name query NB WIN…
    7 2017-05-17 15:10:59.906728 192.168.157.128         192.168.157.255  NBNS          92 Name query NB WIN…
    8 2017-05-17 15:11:00.665375 192.168.157.128         192.168.157.255  NBNS          92 Name query NB WIN…
    9 2017-05-17 15:11:01.355062 192.168.157.1           224.0.0.22       IGMPv3        60 Membership Report…
   10 2017-05-17 15:11:01.355063 fe80::1913:d3c5:a50…    ff02::16         ICMPv6        90 Multicast Listene…
   11 2017-05-17 15:11:01.360148 fe80::1913:d3c5:a50…    ff02::16         ICMPv6        90 Multicast Listene…
   12 2017-05-17 15:11:01.360286 192.168.157.1           224.0.0.22       IGMPv3        60 Membership Report…
   13 2017-05-17 15:11:01.429825 192.168.157.128         192.168.157.255  NBNS          92 Name query NB WIN…
   14 2017-05-17 15:11:01.598087 192.168.157.1           224.0.0.22       IGMPv3        60 Membership Report…
   15 2017-05-17 15:11:01.598088 fe80::1913:d3c5:a50…    ff02::16         ICMPv6        90 Multicast Listene…
   16 2017-05-17 15:11:01.601302 fe80::1913:d3c5:a50…    ff02::16         ICMPv6        90 Multicast Listene…
   17 2017-05-17 15:11:01.601304 192.168.157.1           224.0.0.22       IGMPv3        60 Membership Report…
   18 2017-05-17 15:11:01.611952 fe80::1913:d3c5:a50…    ff02::16         ICMPv6        90 Multicast Listene…
   19 2017-05-17 15:11:01.611953 fe80::1913:d3c5:a50…    ff02::16         ICMPv6        90 Multicast Listene…
   20 2017-05-17 15:11:01.611954 192.168.157.1           224.0.0.22       IGMPv3        60 Membership Report…

▷ Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
▷ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
```

Figure 5.18 Results from the Wireshark packet capture

Based on the **Figure 5.18**, after a few minutes the ransomware infecting the system, it can stop the packet capture and save the file to analyses the network activities of this malware. As example, the figure above shows this ransomware involved most **192.168.157.2** as Destination IP Address.

Step 5: Open Regshot and press the 2nd shot button.



Regshot 1.8.2

Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:332713 Values:498728 Time:5s663ms

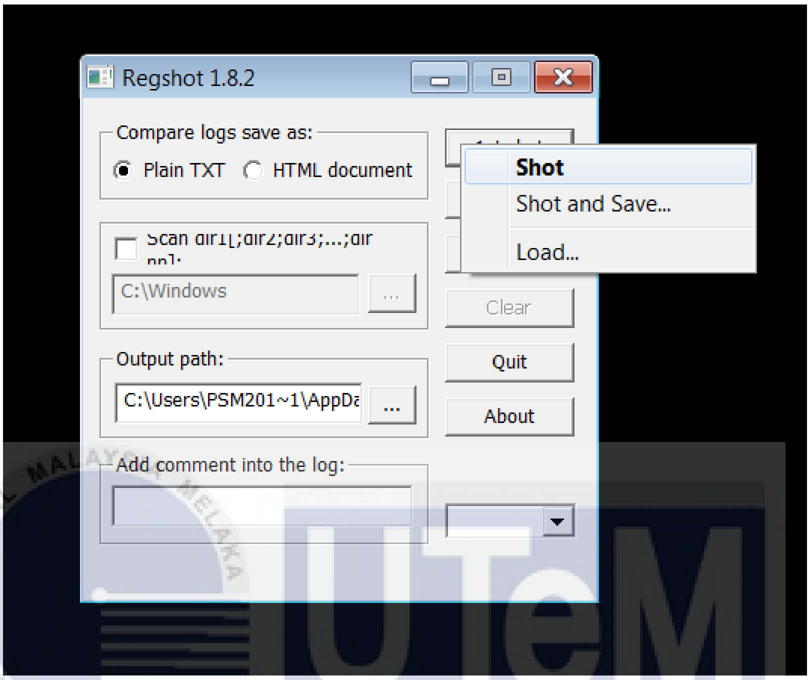
Figure 5.19 Regshot after 2nd shot

Once this is complete, press the Compare button and save the results to the desktop. Regshot gives you the option to save your comparison as plain text or HTML as in **Figure 5.19**.

Sample 3: 2017-01-12-EITest-Rig-V-sends-CryptoMix-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Launch Regshot and click the 1st **shot** button.


Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]: C:\Windows

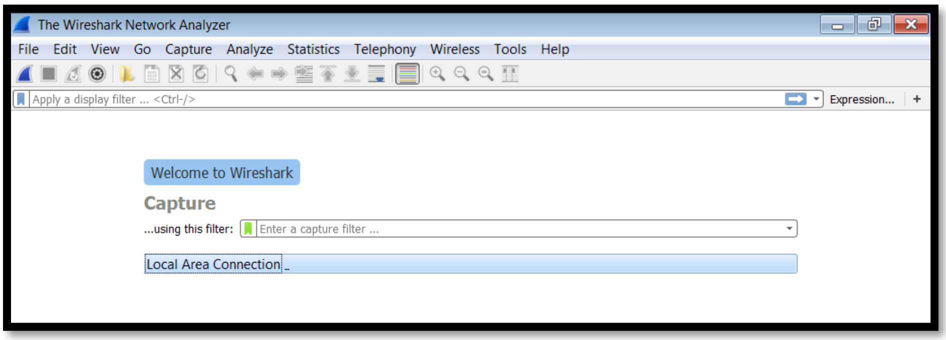
Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Figure 5.20 Select 1st shot from this screen

After launch Regshot, the display is as **Figure 5.20** and it will show the changes occur in registry from the time for first snapshot and the second snapshot. The first snapshot will automatically stop in a few minutes after button **Shot** is clicked.

Step 2: Load Wireshark and begin a packet capture on your local interface.


Apply a display filter ... <Ctrl-/>

...using this filter: Enter a capture filter ...

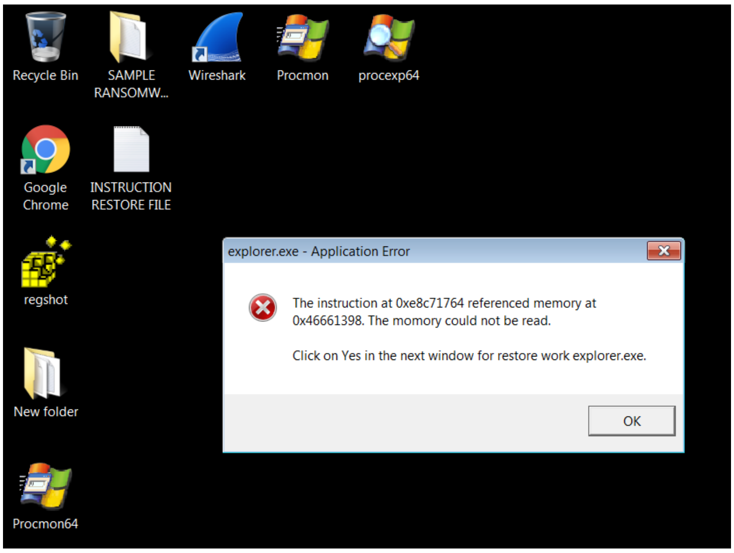
Local Area Connection

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Welcome to Wireshark
Capture

Figure 5.21 Select your Local Area Connection and then click Start

For **Figure 5.21** above, double click the **Local Area Connection** to start packet capture of the network activities when the ransomware infecting the system.

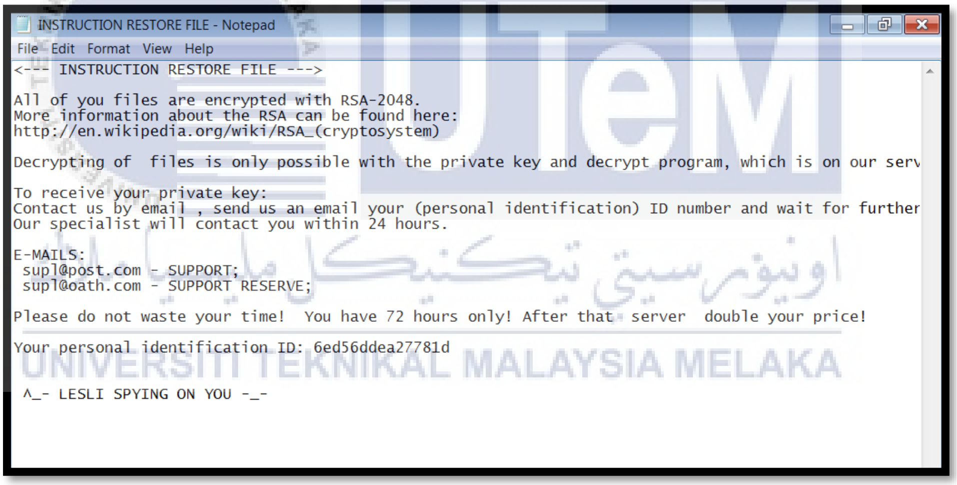
Step 3: Launch the **CryptoMix** ransomware sample. After a few moments, the **CryptoMix** ransomware screen will display.



The instruction at 0xe8c71764 referenced memory at 0x46661398. The momory could not be read.

Click on Yes in the next window for restore work explorer.exe.

Figure 5.22 CryptoMix ransomware screen

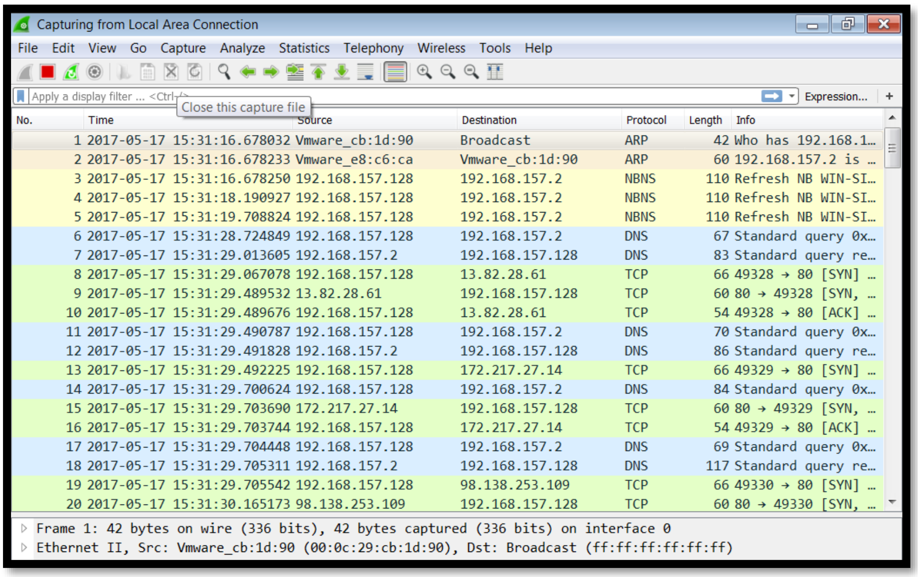

INSTRUCTION RESTORE FILE - Notepad
File Edit Format View Help

```
<--- INSTRUCTION RESTORE FILE --->

All of you files are encrypted with RSA-2048.
More information about the RSA can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)

Decrypting of  files is only possible with the private key and decrypt program, which is on our serv

To receive your private key:
Contact us by email , send us an email your (personal identification) ID number and wait for further
Our specialist will contact you within 24 hours.

E-MAILS:
 supl@post.com - SUPPORT;
 supl@oath.com - SUPPORT RESERVE;

Please do not waste your time!  You have 72 hours only! After that  server  double your price!

Your personal identification ID: 6ed56ddea27781d

 ^_- LESLI SPYING ON YOU -_-
```

Figure 5.23

Most ransomware variants also have a picture and a text file containing instructions on how to pay the ransom. As the **Figure 5.22**, the details information about the ransomware such as the windows popup appear in the screen about the memory could not be read after this malware encrypt it. In **Figure 5.23** is the instruction to decrypting the file, the type of encryption used: **RSA-2048**, and the personal identification of victims: **6ed56ddea27781d**.

Step 4: Stop the Wireshark packet capture and save the results to the desktop.

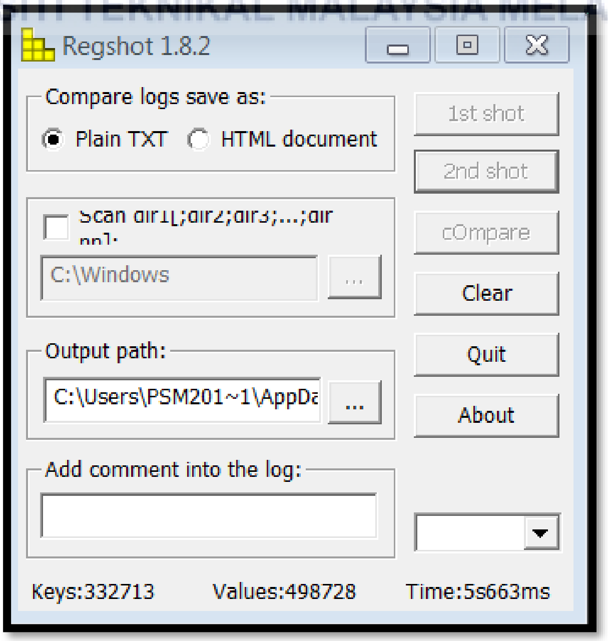

Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Close this capture file
Expression...

```
No.  Time                        Source           Destination      Protocol  Length  Info
   1 2017-05-17 15:31:16.678032 Vmware_cb:1d:90  Broadcast        ARP         42 Who has 192.168.1…
   2 2017-05-17 15:31:16.678233 Vmware_e8:c6:ca  Vmware_cb:1d:90  ARP         60 192.168.157.2 is …
   3 2017-05-17 15:31:16.678250 192.168.157.128  192.168.157.2    NBNS       110 Refresh NB WIN-SI…
   4 2017-05-17 15:31:18.190927 192.168.157.128  192.168.157.2    NBNS       110 Refresh NB WIN-SI…
   5 2017-05-17 15:31:19.708824 192.168.157.128  192.168.157.2    NBNS       110 Refresh NB WIN-SI…
   6 2017-05-17 15:31:28.724849 192.168.157.128  192.168.157.2    DNS         67 Standard query 0x…
   7 2017-05-17 15:31:29.013605 192.168.157.2    192.168.157.128  DNS         83 Standard query re…
   8 2017-05-17 15:31:29.067078 192.168.157.128  13.82.28.61      TCP         66 49328 → 80 [SYN] …
   9 2017-05-17 15:31:29.489532 13.82.28.61      192.168.157.128  TCP         60 80 → 49328 [SYN, …
  10 2017-05-17 15:31:29.489676 192.168.157.128  13.82.28.61      TCP         54 49328 → 80 [ACK] …
  11 2017-05-17 15:31:29.490787 192.168.157.128  192.168.157.2    DNS         70 Standard query 0x…
  12 2017-05-17 15:31:29.491828 192.168.157.2    192.168.157.128  DNS         86 Standard query re…
  13 2017-05-17 15:31:29.492225 192.168.157.128  172.217.27.14    TCP         66 49329 → 80 [SYN] …
  14 2017-05-17 15:31:29.700624 192.168.157.128  192.168.157.2    DNS         84 Standard query 0x…
  15 2017-05-17 15:31:29.703690 172.217.27.14    192.168.157.128  TCP         60 80 → 49329 [SYN, …
  16 2017-05-17 15:31:29.703744 192.168.157.128  172.217.27.14    TCP         54 49329 → 80 [ACK] …
  17 2017-05-17 15:31:29.704448 192.168.157.128  192.168.157.2    DNS         69 Standard query 0x…
  18 2017-05-17 15:31:29.705311 192.168.157.2    192.168.157.128  DNS        117 Standard query re…
  19 2017-05-17 15:31:29.705542 192.168.157.128  98.138.253.109   TCP         66 49330 → 80 [SYN] …
  20 2017-05-17 15:31:30.165173 98.138.253.109   192.168.157.128  TCP         60 80 → 49330 [SYN, …

▷ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▷ Ethernet II, Src: Vmware_cb:1d:90 (00:0c:29:cb:1d:90), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
```

Figure 5.24 Results from the Wireshark packet capture

Based on the **Figure 5.24**, after a few minutes the ransomware infecting the system, it can stop the packet capture and save the file to analyses the network activities of this malware. As example, the figure above shows this ransomware involved most **192.168.157.2** as Destination IP Address.

Step 5: Open Regshot and press the 2nd shot button.



Compare logs save as:
● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

Output path:
C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:332713 Values:498728 Time:5s663ms

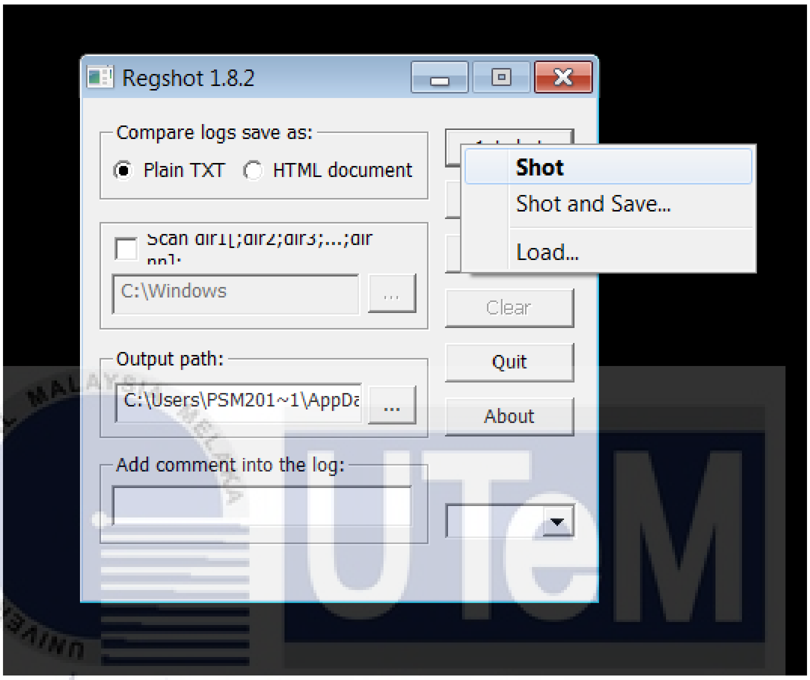
Figure 5.25 Regshot after 2nd shot

Once this is complete, press the Compare button and save the results to the desktop. Regshot gives you the option to save your comparison as plain text or HTML as in **Figure 5.25**.

Sample 4: 2017-01-30-EITest-fake-Chrome-popup-sends-Spora-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Launch Regshot and click the 1st **shot** button.



Regshot 1.8.2

Compare logs save as: ● Plain TXT ○ HTML document

☐ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

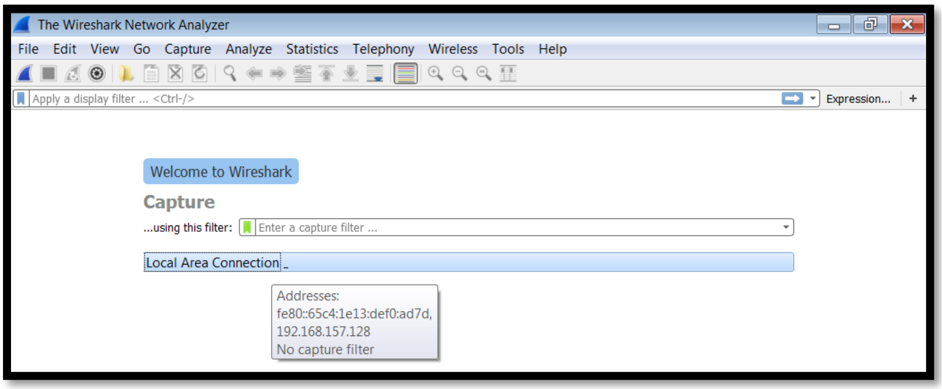
Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Figure 5.26 Select 1st shot from this screen

After launch Regshot, the display is as **Figure 5.26** and it will show the changes occur in registry from the time for first snapshot and the second snapshot. The first snapshot will automatically stop in a few minutes after button **Shot** is clicked.

Step 2: Load Wireshark and begin a packet capture on your local interface.



The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture

...using this filter: Enter a capture filter ...

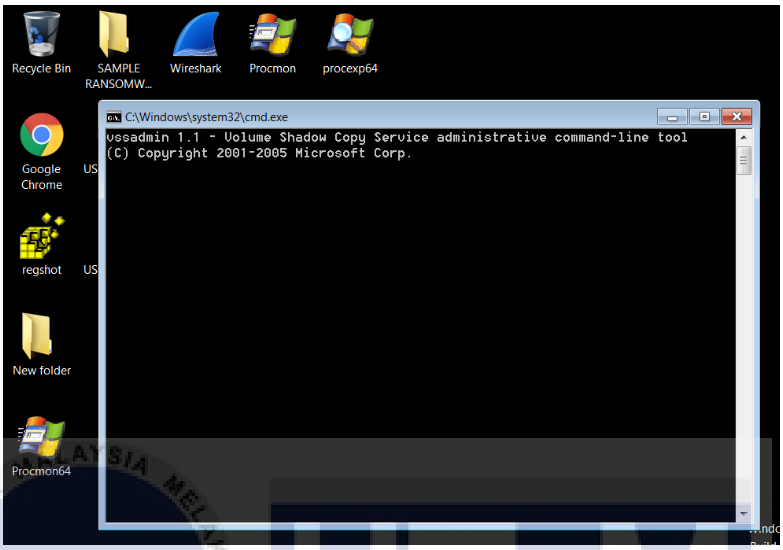
Local Area Connection

Addresses: fe80::65c4:1e13:def0:ad7d, 192.168.157.128
No capture filter

Figure 5.27 Select your Local Area Connection and then click Start

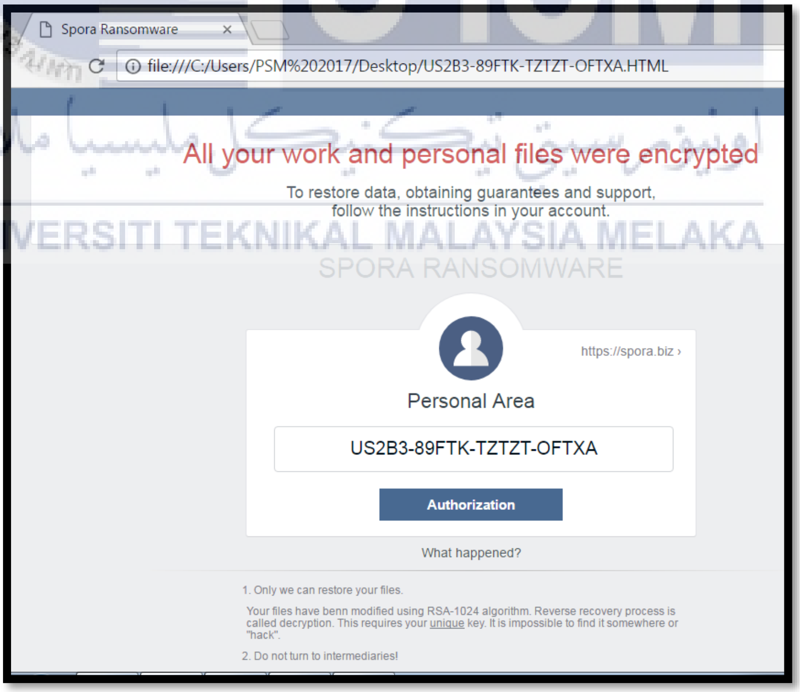
For **Figure 5.27** above, double click the **Local Area Connection** to start packet capture of the network activities when the ransomware infecting the system.

Step 3: Launch the **Spora** ransomware sample. After a few moments, the **Spora** ransomware screen will display.



```
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.
```

Figure 5.28 Spora ransomware screen



All your work and personal files were encrypted

To restore data, obtaining guarantees and support, follow the instructions in your account.

SPORA RANSOMWARE

US2B3-89FTK-TZTZT-OFTXA

1. Only we can restore your files.

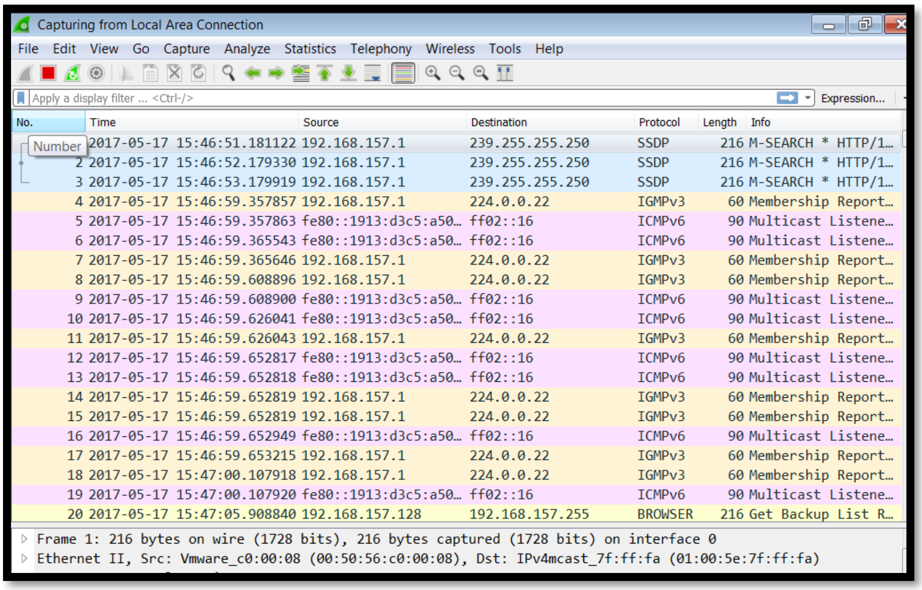
Your files have benn modified using RSA-1024 algorithm. Reverse recovery process is called decryption. This requires your unique key. It is impossible to find it somewhere or "hack".

2. Do not turn to intermediaries!

Figure 5.29 Spora ransomware screen

Most ransomware variants also have a picture and a text file containing instructions on how to pay the ransom. As the **Figure 5.28−Figure 5.29**, the details information about the ransomware such as the personal area for the victims.

Step 4: Stop the Wireshark packet capture and save the results to the desktop.


Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Number

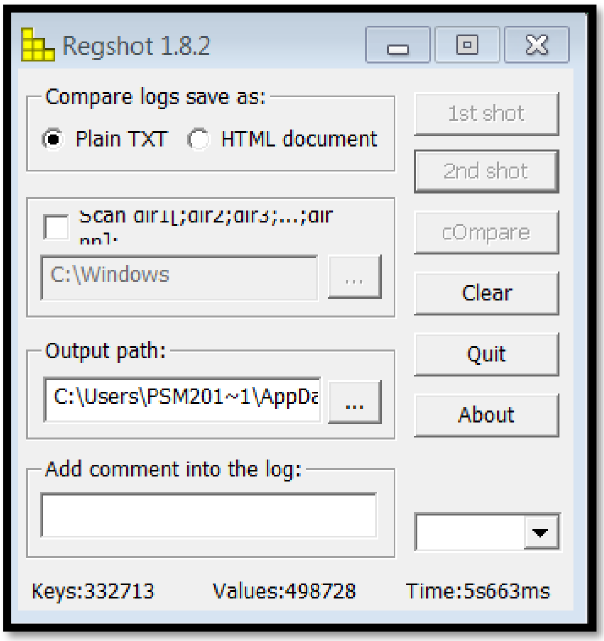
No.	Time	Source	Destination	Protocol	Length	Info
1	2017-05-17 15:46:51.181122	192.168.157.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1…
2	2017-05-17 15:46:52.179330	192.168.157.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1…
3	2017-05-17 15:46:53.179919	192.168.157.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1…
4	2017-05-17 15:46:59.357857	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
5	2017-05-17 15:46:59.357863	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
6	2017-05-17 15:46:59.365543	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
7	2017-05-17 15:46:59.365646	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
8	2017-05-17 15:46:59.608896	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
9	2017-05-17 15:46:59.608900	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
10	2017-05-17 15:46:59.626041	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
11	2017-05-17 15:46:59.626043	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
12	2017-05-17 15:46:59.652817	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
13	2017-05-17 15:46:59.652818	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
14	2017-05-17 15:46:59.652819	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
15	2017-05-17 15:46:59.652819	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
16	2017-05-17 15:46:59.652949	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
17	2017-05-17 15:46:59.653215	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
18	2017-05-17 15:47:00.107918	192.168.157.1	224.0.0.22	IGMPv3	60	Membership Report…
19	2017-05-17 15:47:00.107920	fe80::1913:d3c5:a50…	ff02::16	ICMPv6	90	Multicast Listene…
20	2017-05-17 15:47:05.908840	192.168.157.128	192.168.157.255	BROWSER	216	Get Backup List R…

```
▷ Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
▷ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
```

Figure 5.30 Results from the Wireshark packet capture

Based on the **Figure 5.30**, after a few minutes the ransomware infecting the system, it can stop the packet capture and save the file to analyses the network activities of this malware. As example, the figure above shows this ransomware involved most **192.168.157.1** as Source IP Address.

Step 5: Open Regshot and press the 2nd shot button.



Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:332713 Values:498728 Time:5s663ms

Figure 5.31 Regshot after 2nd shot

Once this is complete, press the Compare button and save the results to the desktop. Regshot gives you the option to save your comparison as plain text or HTML as in **Figure 5.31**.

5.3.2 Process Collect Program Process Data

In this section, the process of collected data of program process is elaborated.

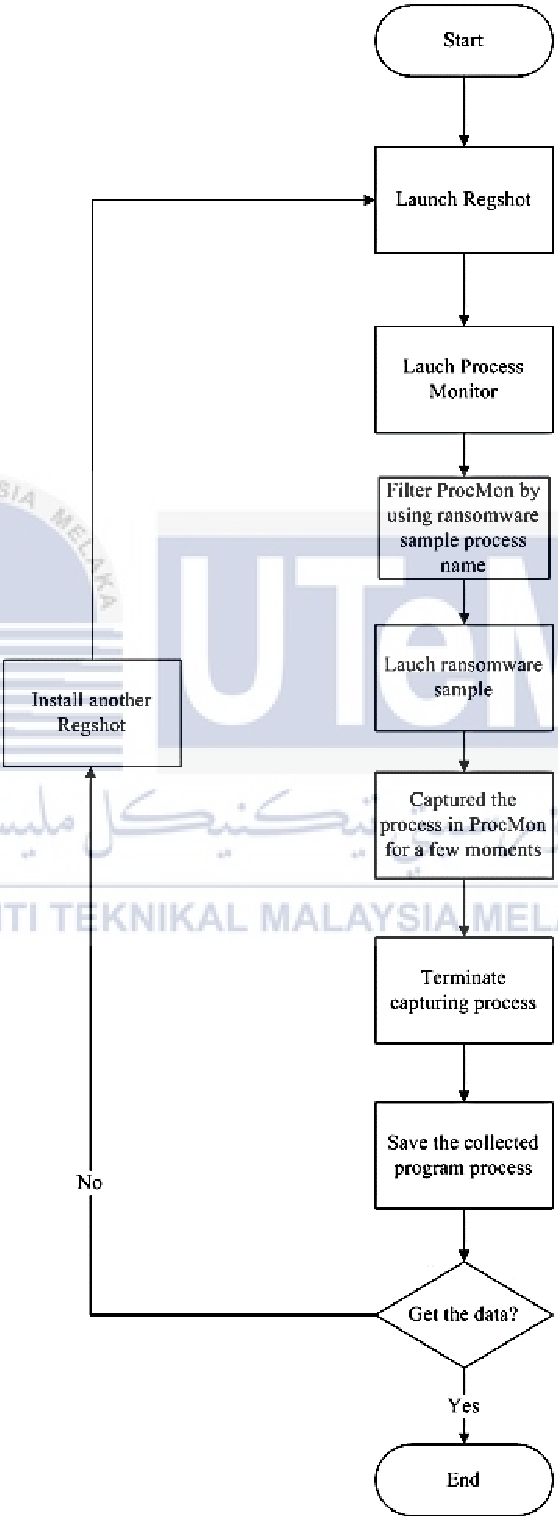

Start
Launch Regshot
Lauch Process Monitor
Filter ProcMon by using ransomware sample process name
Lauch ransomware sample
Captured the process in ProcMon for a few moments
Terminate capturing process
Save the collected program process
Get the data?
Yes
No
Install another Regshot
End

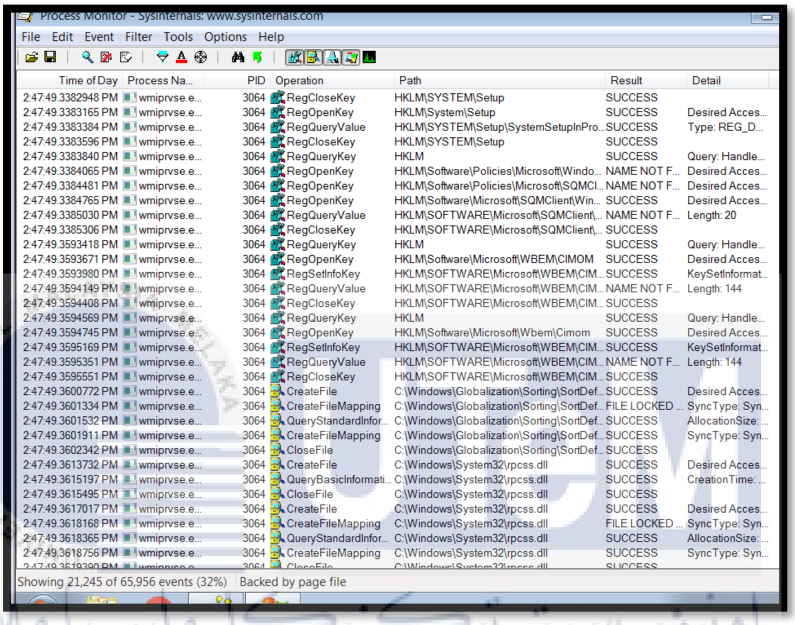
Figure 5.32 Process of Collect Program Process

Sample 1: 2016-12-23-Afraidgate-Rig-V-sends-Locky-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Refer to the Step 1 and **Figure 5.3** in the process collecting network traffic data.

Step 2: Launch Process Monitor then it displays **Figure 5.33**.

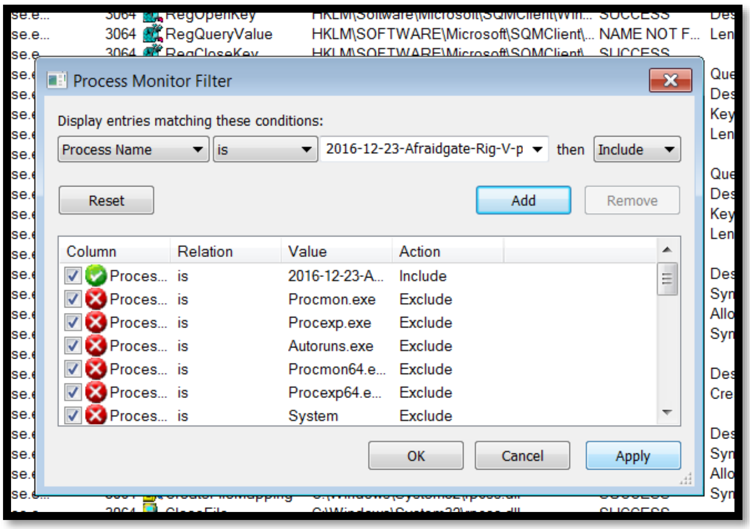


Process Monitor - Sysinternals: www.sysinternals.com

```
Time of Day         Process Na...   PID  Operation            Path                                      Result          Detail
2:47:49.3382948 PM  wmiprvse.e...  3064  RegCloseKey          HKLM\SYSTEM\Setup                         SUCCESS
2:47:49.3383165 PM  wmiprvse.e...  3064  RegOpenKey           HKLM\System\Setup                         SUCCESS         Desired Acces...
2:47:49.3383384 PM  wmiprvse.e...  3064  RegQueryValue        HKLM\SYSTEM\Setup\SystemSetupInPro...     SUCCESS         Type: REG_D...
2:47:49.3383596 PM  wmiprvse.e...  3064  RegCloseKey          HKLM\SYSTEM\Setup                         SUCCESS
2:47:49.3383840 PM  wmiprvse.e...  3064  RegQueryKey          HKLM                                      SUCCESS         Query: Handle...
2:47:49.3384065 PM  wmiprvse.e...  3064  RegOpenKey           HKLM\Software\Policies\Microsoft\Windo... NAME NOT F...   Desired Acces...
2:47:49.3384481 PM  wmiprvse.e...  3064  RegOpenKey           HKLM\Software\Policies\Microsoft\SQMCl... NAME NOT F...   Desired Acces...
2:47:49.3384765 PM  wmiprvse.e...  3064  RegOpenKey           HKLM\Software\Microsoft\SQMClient\Win...  SUCCESS         Desired Acces...
2:47:49.3385030 PM  wmiprvse.e...  3064  RegQueryValue        HKLM\SOFTWARE\Microsoft\SQMClient\...     NAME NOT F...   Length: 20
2:47:49.3385306 PM  wmiprvse.e...  3064  RegCloseKey          HKLM\SOFTWARE\Microsoft\SQMClient\...     SUCCESS
2:47:49.3593418 PM  wmiprvse.e...  3064  RegQueryKey          HKLM                                      SUCCESS         Query: Handle...
2:47:49.3593671 PM  wmiprvse.e...  3064  RegOpenKey           HKLM\Software\Microsoft\WBEM\CIMOM        SUCCESS         Desired Acces...
2:47:49.3593980 PM  wmiprvse.e...  3064  RegSetInfoKey        HKLM\SOFTWARE\Microsoft\WBEM\CIM...       SUCCESS         KeySetInformat...
2:47:49.3594149 PM  wmiprvse.e...  3064  RegQueryValue        HKLM\SOFTWARE\Microsoft\WBEM\CIM...       NAME NOT F...   Length: 144
2:47:49.3594408 PM  wmiprvse.e...  3064  RegCloseKey          HKLM\SOFTWARE\Microsoft\WBEM\CIM...       SUCCESS
2:47:49.3594569 PM  wmiprvse.e...  3064  RegQueryKey          HKLM                                      SUCCESS         Query: Handle...
2:47:49.3594745 PM  wmiprvse.e...  3064  RegOpenKey           HKLM\Software\Microsoft\Wbem\Cimom        SUCCESS         Desired Acces...
2:47:49.3595169 PM  wmiprvse.e...  3064  RegSetInfoKey        HKLM\SOFTWARE\Microsoft\WBEM\CIM...       SUCCESS         KeySetInformat...
2:47:49.3595351 PM  wmiprvse.e...  3064  RegQueryValue        HKLM\SOFTWARE\Microsoft\WBEM\CIM...       NAME NOT F...   Length: 144
2:47:49.3595551 PM  wmiprvse.e...  3064  RegCloseKey          HKLM\SOFTWARE\Microsoft\WBEM\CIM...       SUCCESS
2:47:49.3600772 PM  wmiprvse.e...  3064  CreateFile           C:\Windows\Globalization\Sorting\SortDef... SUCCESS       Desired Acces...
2:47:49.3601334 PM  wmiprvse.e...  3064  CreateFileMapping    C:\Windows\Globalization\Sorting\SortDef... FILE LOCKED ... SyncType: Syn...
2:47:49.3601532 PM  wmiprvse.e...  3064  QueryStandardInfor... C:\Windows\Globalization\Sorting\SortDef... SUCCESS      AllocationSize: ...
2:47:49.3601911 PM  wmiprvse.e...  3064  CreateFileMapping    C:\Windows\Globalization\Sorting\SortDef... SUCCESS       SyncType: Syn...
2:47:49.3602342 PM  wmiprvse.e...  3064  CloseFile            C:\Windows\Globalization\Sorting\SortDef... SUCCESS
2:47:49.3613732 PM  wmiprvse.e...  3064  CreateFile           C:\Windows\System32\rpcss.dll             SUCCESS         Desired Acces...
2:47:49.3615197 PM  wmiprvse.e...  3064  QueryBasicInformati... C:\Windows\System32\rpcss.dll            SUCCESS         CreationTime: ...
2:47:49.3615495 PM  wmiprvse.e...  3064  CloseFile            C:\Windows\System32\rpcss.dll             SUCCESS
2:47:49.3617017 PM  wmiprvse.e...  3064  CreateFile           C:\Windows\System32\rpcss.dll             SUCCESS         Desired Acces...
2:47:49.3618168 PM  wmiprvse.e...  3064  CreateFileMapping    C:\Windows\System32\rpcss.dll             FILE LOCKED ... SyncType: Syn...
2:47:49.3618365 PM  wmiprvse.e...  3064  QueryStandardInfor... C:\Windows\System32\rpcss.dll            SUCCESS         AllocationSize: ...
2:47:49.3618756 PM  wmiprvse.e...  3064  CreateFileMapping    C:\Windows\System32\rpcss.dll             SUCCESS         SyncType: Syn...
2:47:49.3619390 PM  wmiprvse.e...  3064  CloseFile            C:\Windows\System32\rpcss.dll             SUCCESS

Showing 21,245 of 65,956 events (32%)    Backed by page file
```

Figure 5.33 Process Monitor display

In the **Figure 5.33** shows when Process Monitor is launched, it displays all the current processes running on your system.



Process Monitor Filter

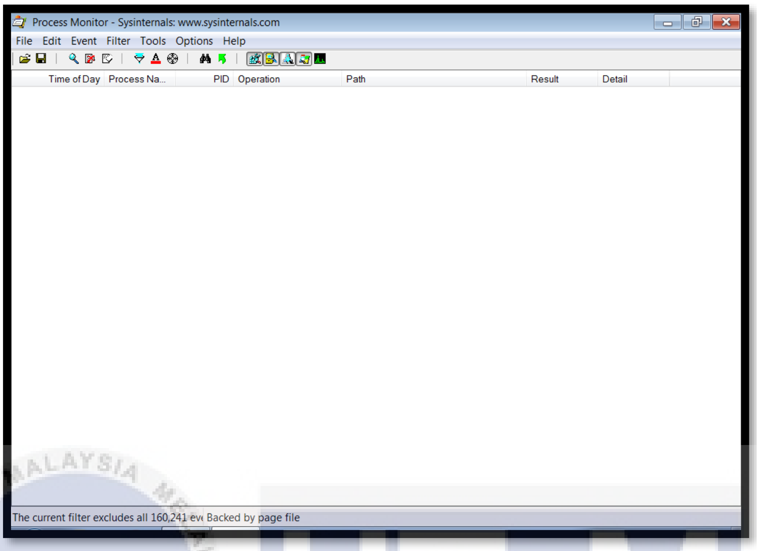
Display entries matching these conditions:

Process Name ▾ | is ▾ | 2016-12-23-Afraidgate-Rig-V-p ▾ | then | Include ▾

Column	Relation	Value	Action
☑ ✓ Proces...	is	2016-12-23-A...	Include
☑ ✗ Proces...	is	Procmon.exe	Exclude
☑ ✗ Proces...	is	Procexp.exe	Exclude
☑ ✗ Proces...	is	Autoruns.exe	Exclude
☑ ✗ Proces...	is	Procmon64.e...	Exclude
☑ ✗ Proces...	is	Procexp64.e...	Exclude
☑ ✗ Proces...	is	System	Exclude

Figure 5.34 Filter Process Name

Selecting Filter at the top displays in **Figure 5.34** the Process Monitor filter options. From here it will add in the name of our ransomware and select Add, click Apply then OK.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day
Process Na...
PID
Operation
Path
Result
Detail

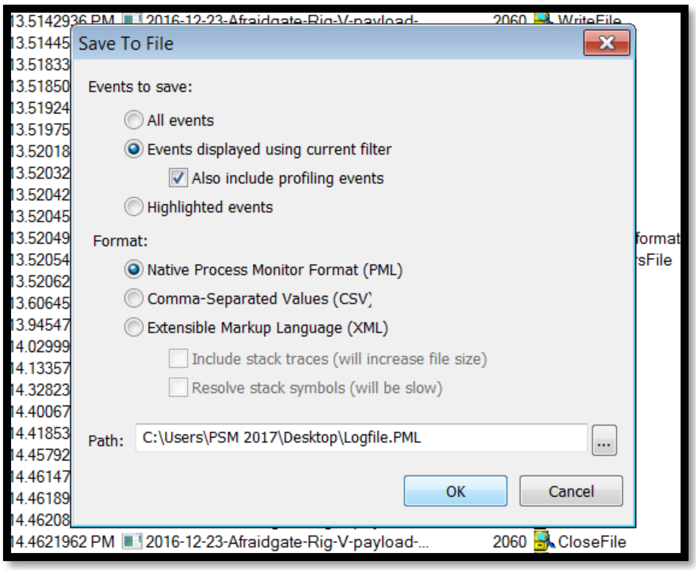
The current filter excludes all 160,241 eve Backed by page file

Figure 5.35 After filter display

Figure 5.35 shows once click OK the display filter is active and should be blank since it have not executed our malware yet the.

Step 3: Refer to the Step 3 and **Figure 5.5** – **Figure 5.6** in the process collecting network traffic data.

Step 4: Stop Process Monitor and save the results to the desktop.



Save To File

Events to save:

○ All events
● Events displayed using current filter
☑ Also include profiling events
○ Highlighted events

Format:

● Native Process Monitor Format (PML)
○ Comma-Separated Values (CSV)
○ Extensible Markup Language (XML)
☐ Include stack traces (will increase file size)
☐ Resolve stack symbols (will be slow)

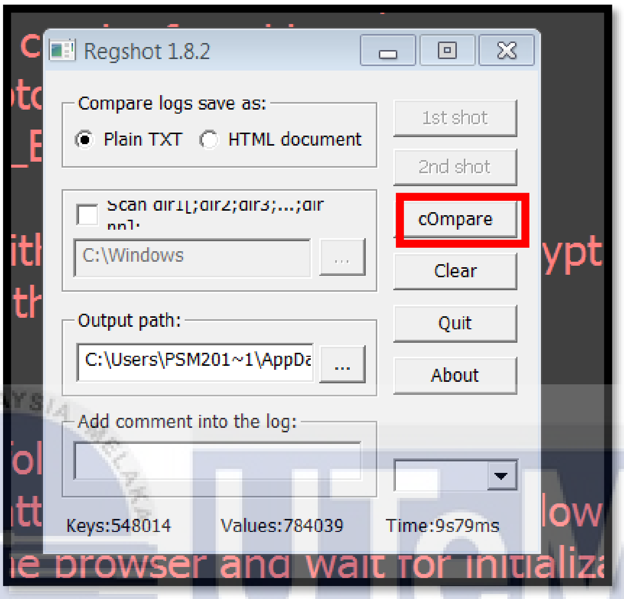
Path: C:\Users\PSM 2017\Desktop\Logfile.PML

```
14.4621962 PM    2016-12-23-Afraidgate-Rig-V-payload-...    2060    CloseFile
```

Figure 5.36 Save the Process Monitor results using the options shown here

For the Process Monitor in **Figure 5.36**, it can save in format **Native Process Monitor Format (PML)** where it shows the same as when open the Process Monitor. While **Comma-Separated Values (CSV)** it shows in excel file format.

Step 5: Open Regshot and press the 2nd shot button.



Regshot 1.8.2

Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:548014 Values:784039 Time:9s79ms

Figure 5.37 Regshot after 2nd shot

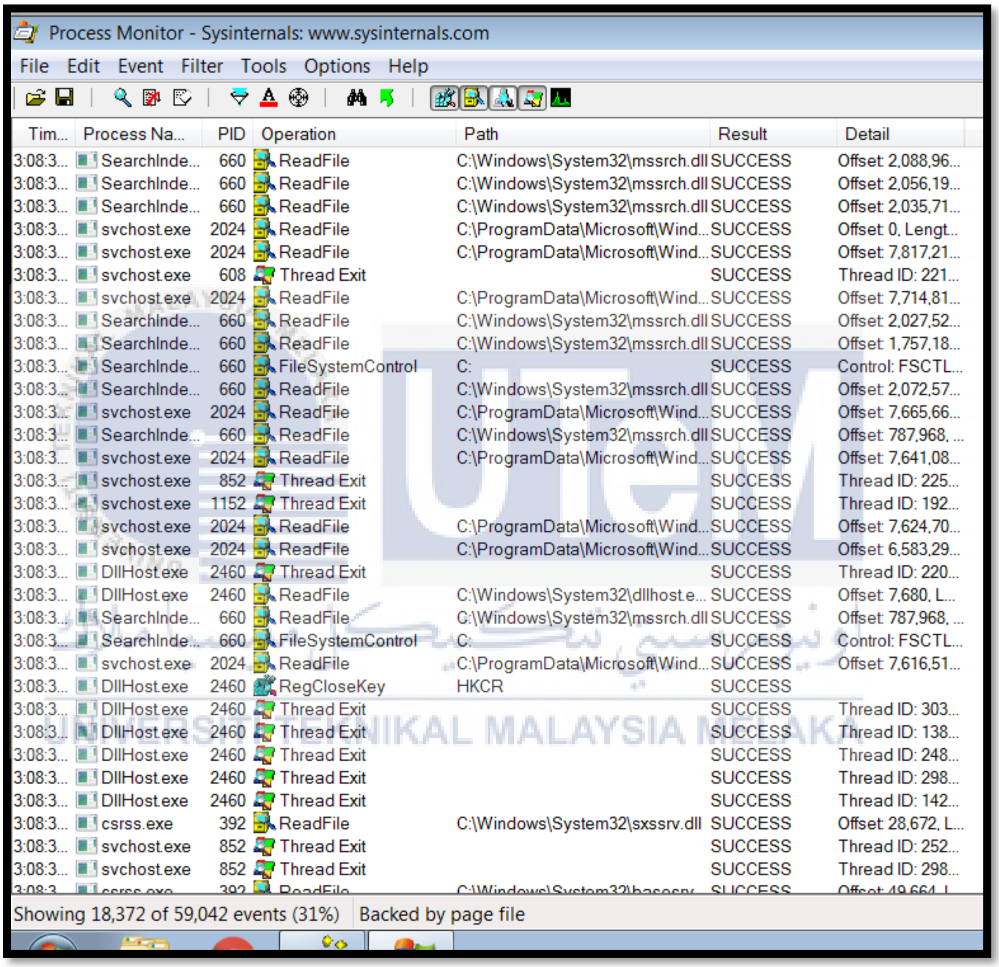
Once this is complete, press the Compare button and save the results to the desktop. Regshot gives you the option to save your comparison as plain text or HTML as shown in the **Figure 5.37** above.

2017-01-05-psuedoDarkleech-Rig-V-sends-Cerber-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Refer to the Step 1 and **Figure 5.3** in the process collecting network traffic data.

Step 2: Launch Process Monitor then it displays **Figure 5.38**.

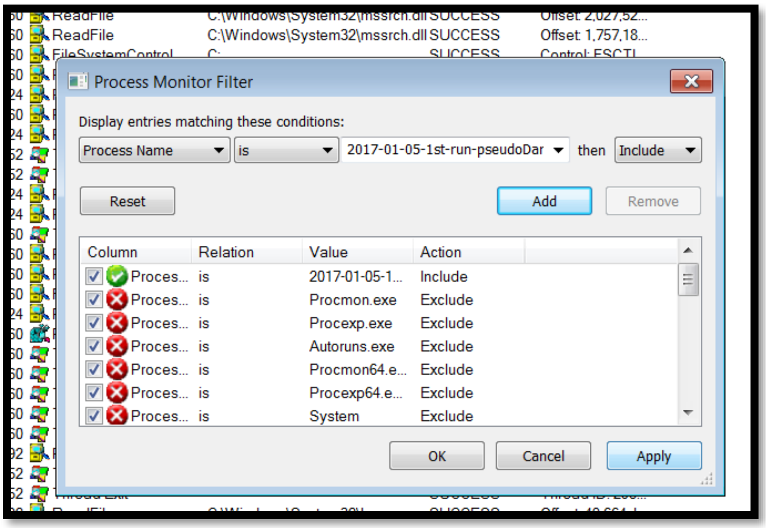


Tim...	Process Na...	PID	Operation	Path	Result	Detail
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,088,96...
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,056,19...
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,035,71...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 0, Lengt...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 7,817,21...
3:08:3...	svchost.exe	608	Thread Exit		SUCCESS	Thread ID: 221...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 7,714,81...
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,027,52...
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 1,757,18...
3:08:3...	SearchInde...	660	FileSystemControl	C:	SUCCESS	Control: FSCTL...
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,072,57...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 7,665,66...
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 787,968, ...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 7,641,08...
3:08:3...	svchost.exe	852	Thread Exit		SUCCESS	Thread ID: 225...
3:08:3...	svchost.exe	1152	Thread Exit		SUCCESS	Thread ID: 192...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 7,624,70...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 6,583,29...
3:08:3...	DllHost.exe	2460	Thread Exit		SUCCESS	Thread ID: 220...
3:08:3...	DllHost.exe	2460	ReadFile	C:\Windows\System32\dllhost.e...	SUCCESS	Offset: 7,680, L...
3:08:3...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 787,968, ...
3:08:3...	SearchInde...	660	FileSystemControl	C:	SUCCESS	Control: FSCTL...
3:08:3...	svchost.exe	2024	ReadFile	C:\ProgramData\Microsoft\Wind...	SUCCESS	Offset: 7,616,51...
3:08:3...	DllHost.exe	2460	RegCloseKey	HKCR	SUCCESS	
3:08:3...	DllHost.exe	2460	Thread Exit		SUCCESS	Thread ID: 303...
3:08:3...	DllHost.exe	2460	Thread Exit		SUCCESS	Thread ID: 138...
3:08:3...	DllHost.exe	2460	Thread Exit		SUCCESS	Thread ID: 248...
3:08:3...	DllHost.exe	2460	Thread Exit		SUCCESS	Thread ID: 298...
3:08:3...	DllHost.exe	2460	Thread Exit		SUCCESS	Thread ID: 142...
3:08:3...	csrss.exe	392	ReadFile	C:\Windows\System32\sxssrv.dll	SUCCESS	Offset: 28,672, L...
3:08:3...	svchost.exe	852	Thread Exit		SUCCESS	Thread ID: 252...
3:08:3...	svchost.exe	852	Thread Exit		SUCCESS	Thread ID: 298...
3:08:3	csrss.exe	392	ReadFile	C:\Windows\System32\basesrv...	SUCCESS	Offset: 49,664, L

Showing 18,372 of 59,042 events (31%) | Backed by page file

Figure 5.38 Process Monitor display

In the **Figure 5.38** shows when Process Monitor is launched, it displays all the current processes running on your system.


Process Monitor Filter

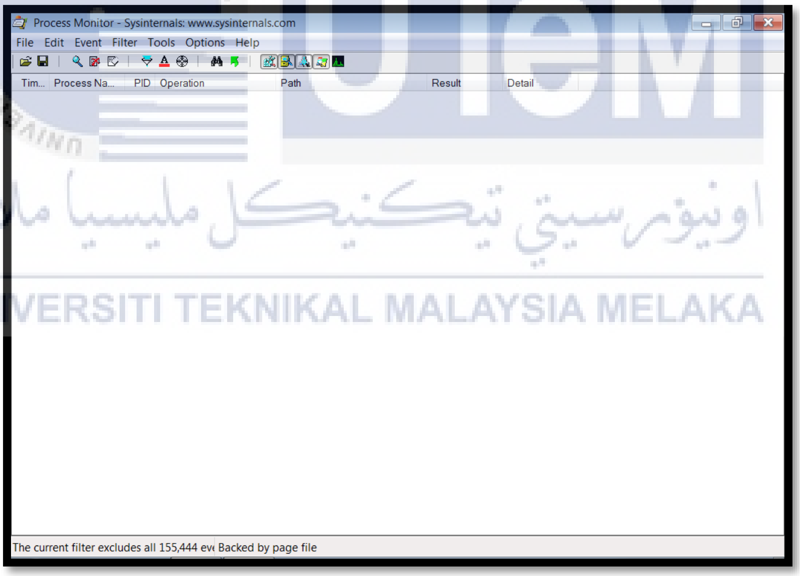
Display entries matching these conditions:

Process Name | is | 2017-01-05-1st-run-pseudoDar | then | Include

Column	Relation	Value	Action
☑ ✓ Proces...	is	2017-01-05-1...	Include
☑ ☒ Proces...	is	Procmon.exe	Exclude
☑ ☒ Proces...	is	Procexp.exe	Exclude
☑ ☒ Proces...	is	Autoruns.exe	Exclude
☑ ☒ Proces...	is	Procmon64.e...	Exclude
☑ ☒ Proces...	is	Procexp64.e...	Exclude
☑ ☒ Proces...	is	System	Exclude

Figure 5.39 Filter Process Name

Selecting Filter at the top displays in **Figure 5.39** the Process Monitor filter options. From here it will add in the name of our ransomware and select Add, click Apply then OK.


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help
Tim... Process Na... PID Operation Path Result Detail

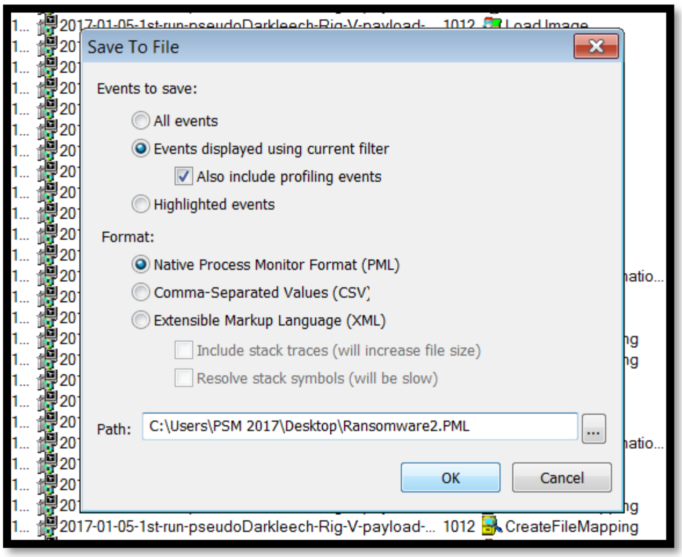
The current filter excludes all 155,444 ev Backed by page file

Figure 5.40 After filter display

Figure 5.40 shows once click OK the display filter is active and should be blank since it have not executed our malware yet the.

Step 3: Refer to the Step 3 and **Figure 5.11**– **Figure 5.17** in the process collecting network traffic data.

Step 4: Stop Process Monitor and save the results to the desktop.



Save To File

Events to save:

○ All events

● Events displayed using current filter

☑ Also include profiling events

○ Highlighted events

Format:

● Native Process Monitor Format (PML)

○ Comma-Separated Values (CSV)

○ Extensible Markup Language (XML)

□ Include stack traces (will increase file size)

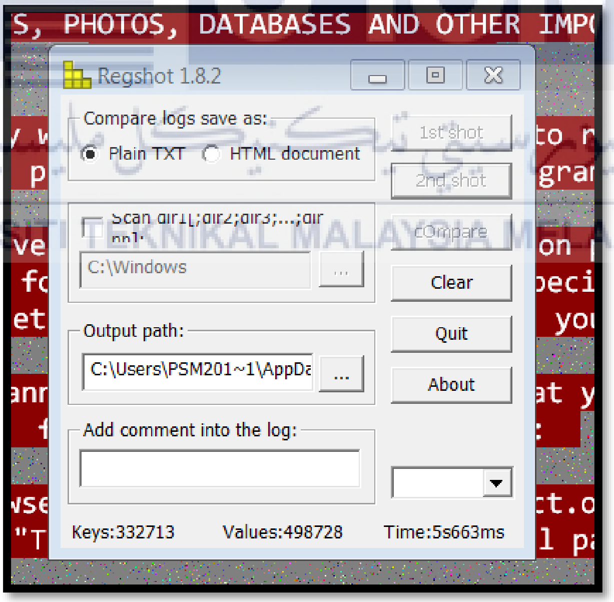
□ Resolve stack symbols (will be slow)

Path: C:\Users\PSM 2017\Desktop\Ransomware2.PML

Figure 5.41 Save the Process Monitor results using the options shown here

For the Process Monitor in **Figure 5.41**, it can save in format **Native Process Monitor Format (PML)** where it shows the same as when we open the Process Monitor. While **Comma-Separated Values (CSV)** it shows in excel file format.

Step 5: Open Regshot and press the 2nd shot button.



Regshot 1.8.2

Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

Output path: C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:332713 Values:498728 Time:5s663ms

Figure 5.42 Regshot after 2nd shot

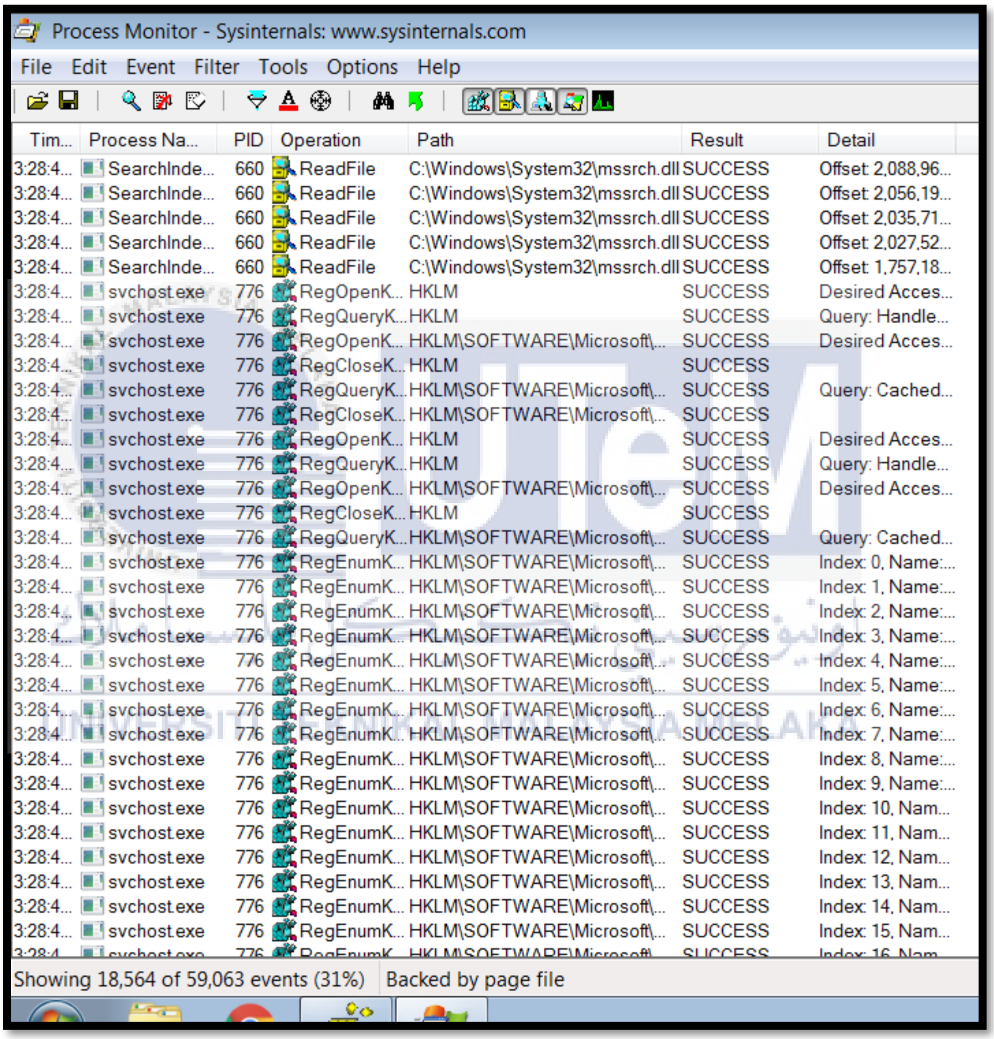
Once this is complete, press the Compare button and save the results to the desktop. Regshot gives the option to save your comparison as plain text or HTML as shown in the **Figure 5.42** above.

Sample 2: 2017-01-12-EITest-Rig-V-sends-CryptoMix-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Refer to the Step 1 and **Figure 5.3** in the process collecting network traffic data.

Step 2: Launch Process Monitor then it displays **Figure 5.43**.

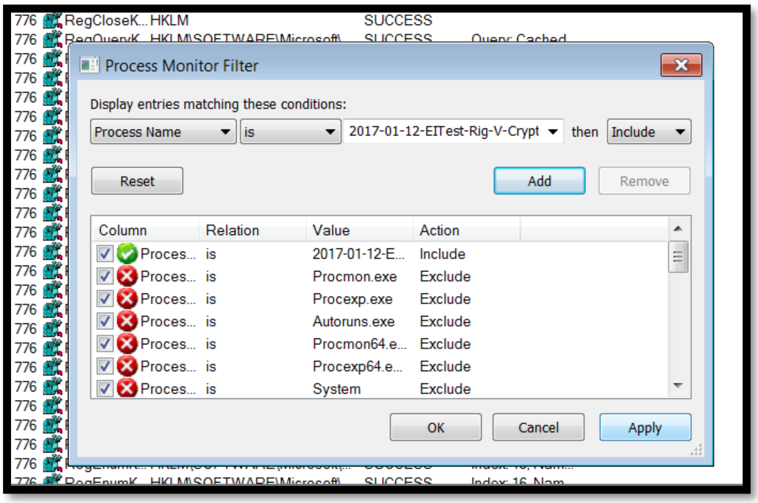


Tim...	Process Na...	PID	Operation	Path	Result	Detail
3:28:4...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,088,96...
3:28:4...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,056,19...
3:28:4...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,035,71...
3:28:4...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,027,52...
3:28:4...	SearchInde...	660	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 1,757,18...
3:28:4...	svchost.exe	776	RegOpenK...	HKLM	SUCCESS	Desired Acces...
3:28:4...	svchost.exe	776	RegQueryK...	HKLM	SUCCESS	Query: Handle...
3:28:4...	svchost.exe	776	RegOpenK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Desired Acces...
3:28:4...	svchost.exe	776	RegCloseK...	HKLM	SUCCESS	
3:28:4...	svchost.exe	776	RegQueryK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Query: Cached...
3:28:4...	svchost.exe	776	RegCloseK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	
3:28:4...	svchost.exe	776	RegOpenK...	HKLM	SUCCESS	Desired Acces...
3:28:4...	svchost.exe	776	RegQueryK...	HKLM	SUCCESS	Query: Handle...
3:28:4...	svchost.exe	776	RegOpenK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Desired Acces...
3:28:4...	svchost.exe	776	RegCloseK...	HKLM	SUCCESS	
3:28:4...	svchost.exe	776	RegQueryK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Query: Cached...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 0, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 1, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 2, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 3, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 4, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 5, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 6, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 7, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 8, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 9, Name:...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 10, Nam...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 11, Nam...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 12, Nam...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 13, Nam...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 14, Nam...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 15, Nam...
3:28:4...	svchost.exe	776	RegEnumK...	HKLM\SOFTWARE\Microsoft\...	SUCCESS	Index: 16, Nam...

Showing 18,564 of 59,063 events (31%) Backed by page file

Figure 5.43 Process Monitor display

In the **Figure 5.43** shows when Process Monitor is launched, it displays all the current processes running on your system.



Process Monitor Filter

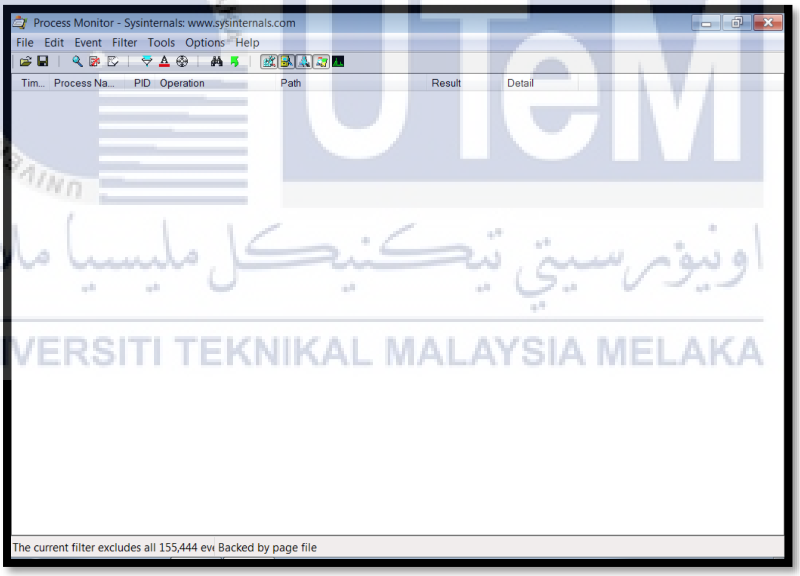
Display entries matching these conditions:

Process Name | is | 2017-01-12-EITest-Rig-V-Crypt | then | Include

Column	Relation	Value	Action
☑ ✓ Proces...	is	2017-01-12-E...	Include
☑ ☒ Proces...	is	Procmon.exe	Exclude
☑ ☒ Proces...	is	Procexp.exe	Exclude
☑ ☒ Proces...	is	Autoruns.exe	Exclude
☑ ☒ Proces...	is	Procmon64.e...	Exclude
☑ ☒ Proces...	is	Procexp64.e...	Exclude
☑ ☒ Proces...	is	System	Exclude

Figure 5.44 Filter Process Name

Selecting Filter at the top displays in **Figure 5.44** the Process Monitor filter options. From here it will add in the name of our ransomware and select Add, click Apply then OK.



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Tim... Process Na... PID Operation Path Result Detail

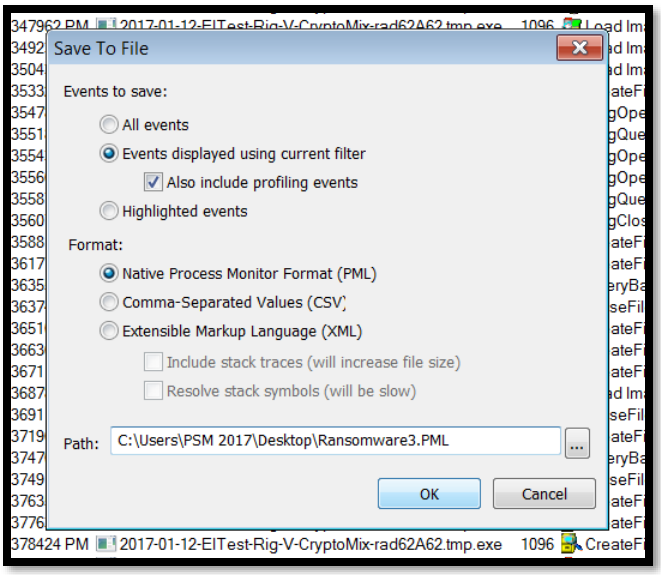
The current filter excludes all 155,444 eve Backed by page file

Figure 5.45 After filter display

Figure 5.45 shows once click OK the display filter is active and should be blank since it have not executed our malware yet the.

Step 3: Refer to the Step 3 and **Figure 5.22** – **Figure 5.23** in the process collecting network traffic data.

Step 4: Stop Process Monitor and save the results to the desktop.



Save To File

Events to save:

○ All events

● Events displayed using current filter

☑ Also include profiling events

○ Highlighted events

Format:

● Native Process Monitor Format (PML)

○ Comma-Separated Values (CSV)

○ Extensible Markup Language (XML)

□ Include stack traces (will increase file size)

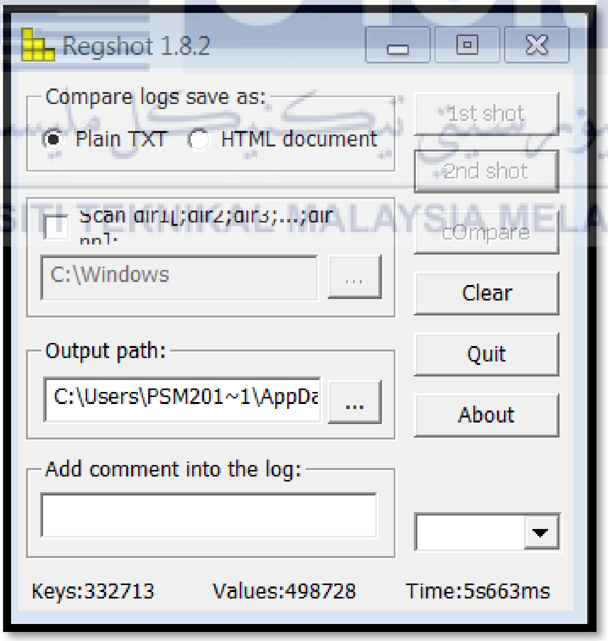
□ Resolve stack symbols (will be slow)

Path: C:\Users\PSM 2017\Desktop\Ransomware3.PML

Figure 5.46 Save the Process Monitor results using the options shown here

For the Process Monitor in **Figure 5.46**, it can save in format **Native Process Monitor Format (PML)** where it shows the same as when open the Process Monitor. While **Comma-Separated Values (CSV)** it shows in excel file format.

Step 5: Open Regshot and press the 2nd shot button.



Regshot 1.8.2

Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

Output path:

C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:332713 Values:498728 Time:5s663ms

Figure 5.47 Regshot after 2nd shot

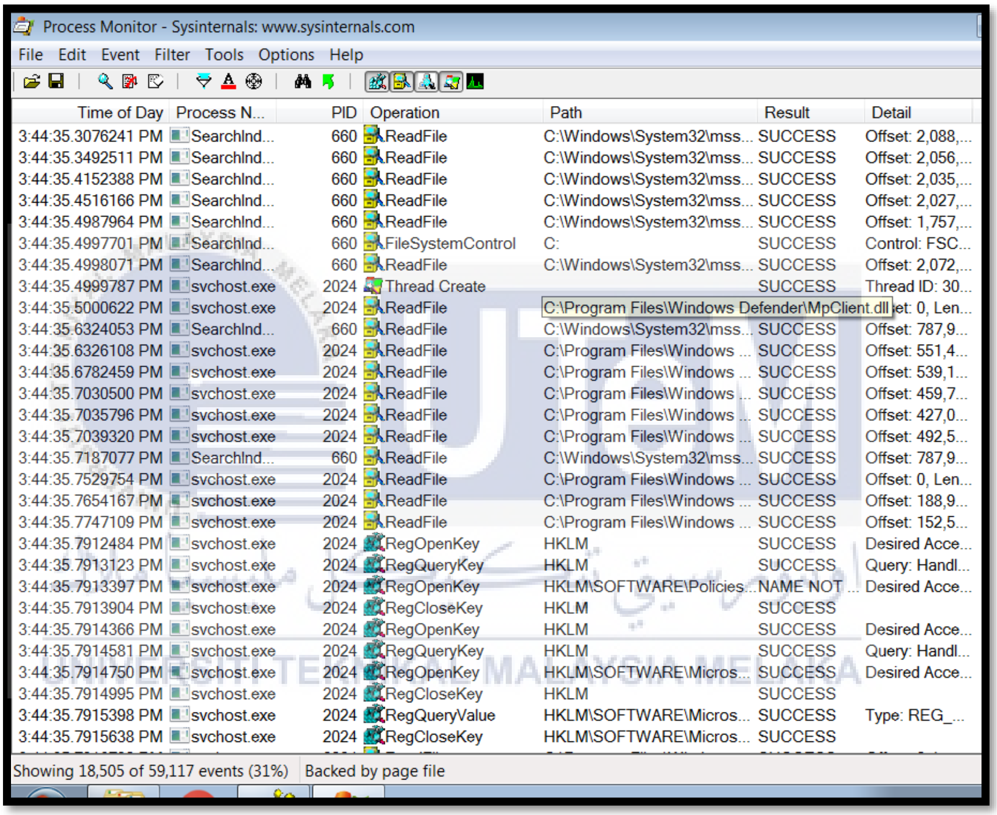
Once this is complete, press the Compare button and save the results to the desktop. Regshot gives you the option to save your comparison as plain text or HTML as shown in the **Figure 5.47** above.

Sample 4: 2017-01-30-EITest-fake-Chrome-popup-sends-Spora-malware-and-artifacts

The details of process collect network traffic are describes step by step as following.

Step 1: Refer to the Step 1 and **Figure 5.3** in the process collecting network traffic data.

Step 2: Launch Process Monitor then it displays **Figure 5.48**.



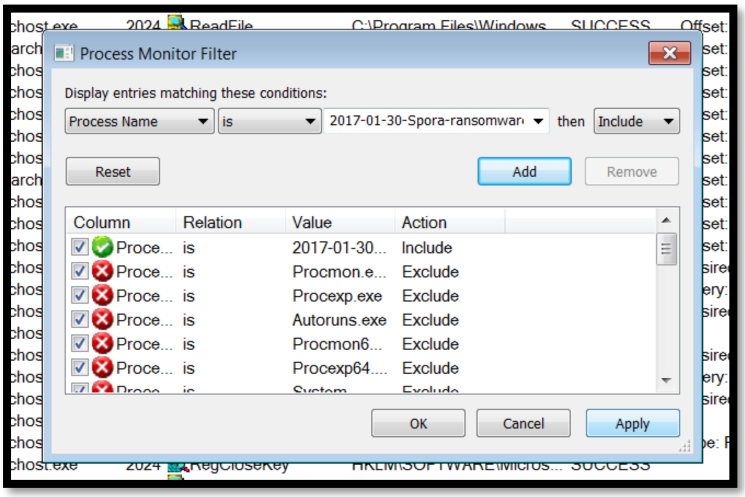
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time of Day	Process N...	PID	Operation	Path	Result	Detail
3:44:35.3076241 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 2,088,...
3:44:35.3492511 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 2,056,...
3:44:35.4152388 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 2,035,...
3:44:35.4516166 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 2,027,...
3:44:35.4987964 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 1,757,...
3:44:35.4997701 PM	SearchInd...	660	FileSystemControl	C:	SUCCESS	Control: FSC...
3:44:35.4998071 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 2,072,...
3:44:35.4999787 PM	svchost.exe	2024	Thread Create		SUCCESS	Thread ID: 30...
3:44:35.5000622 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows Defender\MpClient.dll		et: 0, Len...
3:44:35.6324053 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 787,9...
3:44:35.6326108 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 551,4...
3:44:35.6782459 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 539,1...
3:44:35.7030500 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 459,7...
3:44:35.7035796 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 427,0...
3:44:35.7039320 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 492,5...
3:44:35.7187077 PM	SearchInd...	660	ReadFile	C:\Windows\System32\mss...	SUCCESS	Offset: 787,9...
3:44:35.7529754 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 0, Len...
3:44:35.7654167 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 188,9...
3:44:35.7747109 PM	svchost.exe	2024	ReadFile	C:\Program Files\Windows ...	SUCCESS	Offset: 152,5...
3:44:35.7912484 PM	svchost.exe	2024	RegOpenKey	HKLM	SUCCESS	Desired Acce...
3:44:35.7913123 PM	svchost.exe	2024	RegQueryKey	HKLM	SUCCESS	Query: Handl...
3:44:35.7913397 PM	svchost.exe	2024	RegOpenKey	HKLM\SOFTWARE\Policies...	NAME NOT ...	Desired Acce...
3:44:35.7913904 PM	svchost.exe	2024	RegCloseKey	HKLM	SUCCESS	
3:44:35.7914366 PM	svchost.exe	2024	RegOpenKey	HKLM	SUCCESS	Desired Acce...
3:44:35.7914581 PM	svchost.exe	2024	RegQueryKey	HKLM	SUCCESS	Query: Handl...
3:44:35.7914750 PM	svchost.exe	2024	RegOpenKey	HKLM\SOFTWARE\Micros...	SUCCESS	Desired Acce...
3:44:35.7914995 PM	svchost.exe	2024	RegCloseKey	HKLM	SUCCESS	
3:44:35.7915398 PM	svchost.exe	2024	RegQueryValue	HKLM\SOFTWARE\Micros...	SUCCESS	Type: REG_...
3:44:35.7915638 PM	svchost.exe	2024	RegCloseKey	HKLM\SOFTWARE\Micros...	SUCCESS	

Showing 18,505 of 59,117 events (31%)   Backed by page file

Figure 5.48 Process Monitor display

In the **Figure 5.48** shows when Process Monitor is launched, it displays all the current processes running on your system.



Process Monitor Filter

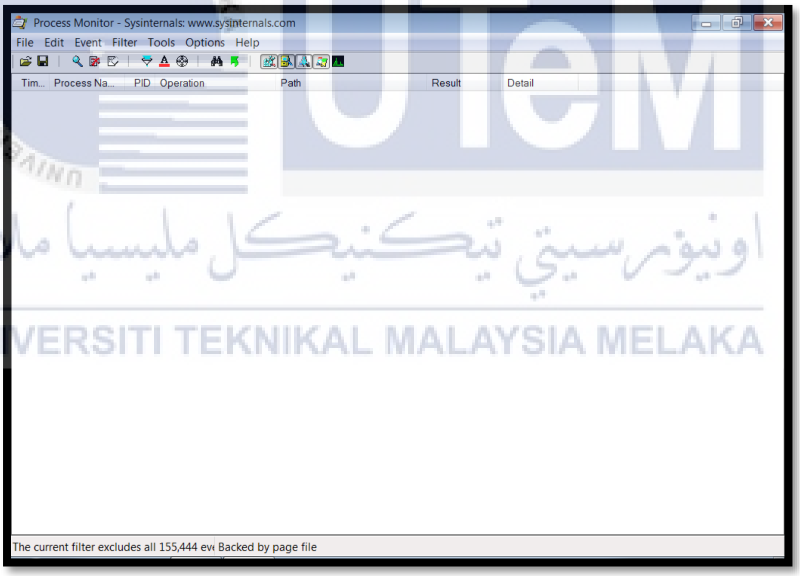
Display entries matching these conditions:

Process Name | is | 2017-01-30-Spora-ransomwar | then | Include

Column	Relation	Value	Action
☑ ✓ Proce...	is	2017-01-30...	Include
☑ ☒ Proce...	is	Procmon.e...	Exclude
☑ ☒ Proce...	is	Procexp.exe	Exclude
☑ ☒ Proce...	is	Autoruns.exe	Exclude
☑ ☒ Proce...	is	Procmon6...	Exclude
☑ ☒ Proce...	is	Procexp64....	Exclude
☑ ☒ Proce...	is	System	Exclude

Figure 5.49 Filter Process Name

Selecting Filter at the top displays in **Figure 5.49** the Process Monitor filter options. From here it will add in the name of our ransomware and select Add, click Apply then OK.



Process Monitor - Sysinternals: www.sysinternals.com

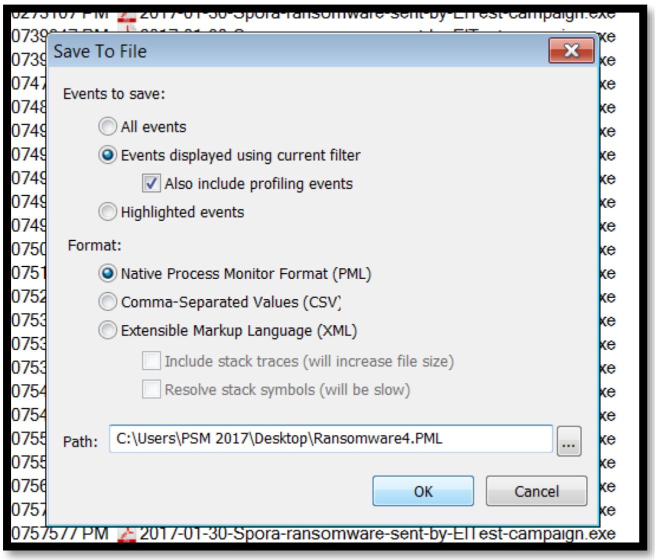
The current filter excludes all 155,444 eve Backed by page file

Figure 5.50 After filter display

Figure 5.50 shows once click OK the display filter is active and should be blank since it have not executed our malware yet the.

Step 3: Refer to the Step 3 and **Figure 5.28** – **Figure 5.29** in the process collecting network traffic data.

Step 4: Stop Process Monitor and save the results to the desktop.



Save To File

Events to save:

○ All events
● Events displayed using current filter
☑ Also include profiling events
○ Highlighted events

Format:

● Native Process Monitor Format (PML)
○ Comma-Separated Values (CSV)
○ Extensible Markup Language (XML)
□ Include stack traces (will increase file size)
□ Resolve stack symbols (will be slow)

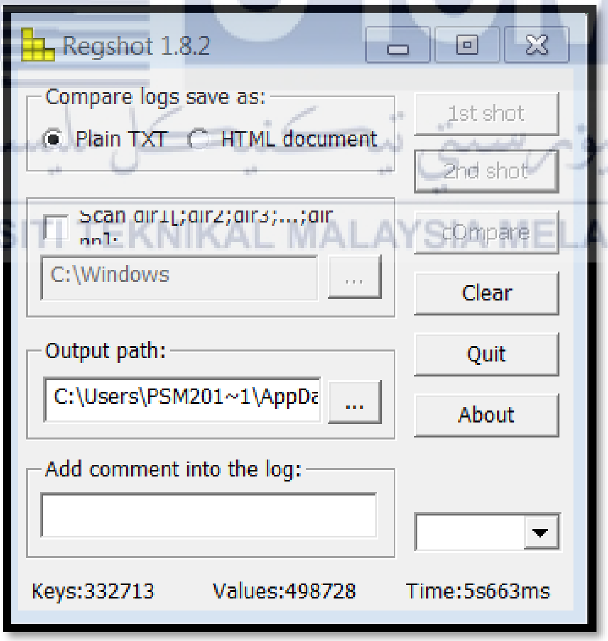
Path: C:\Users\PSM 2017\Desktop\Ransomware4.PML

...
OK
Cancel
0757577 PM 2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe

Figure 5.51 Save the Process Monitor results using the options shown here

For the Process Monitor in **Figure 5.51**, it can save in format **Native Process Monitor Format (PML)** where it shows the same as when open the Process Monitor. While **Comma-Separated Values (CSV)** it shows in excel file format.

Step 5: Open Regshot and press the 2nd shot button.



Regshot 1.8.2

Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

Output path:

C:\Users\PSM201~1\AppDa

Add comment into the log:

Keys:332713 Values:498728 Time:5s663ms

Figure 5.52 Regshot after 2nd shot

Once this is complete, press the Compare button and save the results to the desktop. Regshot gives you the option to save your comparison as plain text or HTML as shown in the **Figure 5.52** above.

5.4 Conclusion

The data of network traffic and program process has been captured in this chapter such as the file system analysis, network traffic analyzing and process monitor. The result will be used in chapter 6 which is testing and analysis.

CHAPTER VI

TESTING AND ANALYSIS

6.1 Introduction

This chapter briefly describe the activity involved in the implementation phase in this project and it also provide chapter outline diagram of Chapter VI. The result and analysis section consist of graphical results using the collected data from the implementation phase and critical analysis on the graphical results.

6.2 Results and Analysis

In previous chapter, all the ransomware samples as Locky ransomware, Cerber ransomware, CryptoMix ransomware, and Spora ransomware executed in a controlled environment and the results captured using dynamic analysis. Dynamic analysis allows the researcher to run the malware sample in a controlled environment and record any changes it makes to the infected system after execution. To do this, the tools used is: Wireshark, Regshot and Process Monitor.

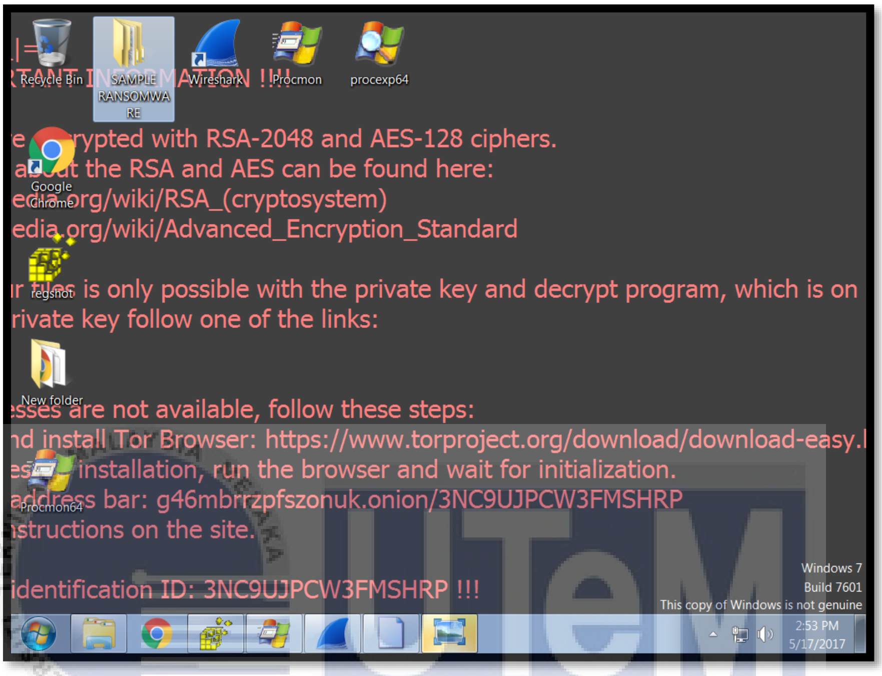
To analyze the collected data, these three tools used again with a new one, NetworkMiner. This tool is an excellent tool for performing network forensics. It could automatically carve out files from a packet capture and display the contracted host in an easy-to-follow and understand way. NetworkMiner also a free packet analysis tool that is frequently used in investigations and penetration testing, in addition to analyzing packets, it can also function as a network traffic sniffer and has a several useful features such as automatically extracting files from packet captures. Operating system fingerprinting, and displaying credentials captured found in packet captures.

Network Forensics

Network forensics is a critical step in any malware analysis process. Packet captures can contain information such as all the outbound hosts the malware contacted, any additional malware downloaded, and sometime even passwords that were sent to the attacker's systems.

Sample 1: 2016-12-23-Afraidgate-Rig-V-sends-Locky-malware-and-artifacts

For this analysis, first ransomware sample named Locky has been run in a controlled environment on a virtual machine. Shortly after executing the malware presented with a notification screen as in **Figure 6.1**



!!! RTANT INFORMATION !!!

e rypted with RSA-2048 and AES-128 ciphers.
a t the RSA and AES can be found here:
edia.org/wiki/RSA_(cryptosystem)
edia.org/wiki/Advanced_Encryption_Standard

ir files is only possible with the private key and decrypt program, which is on
rivate key follow one of the links:

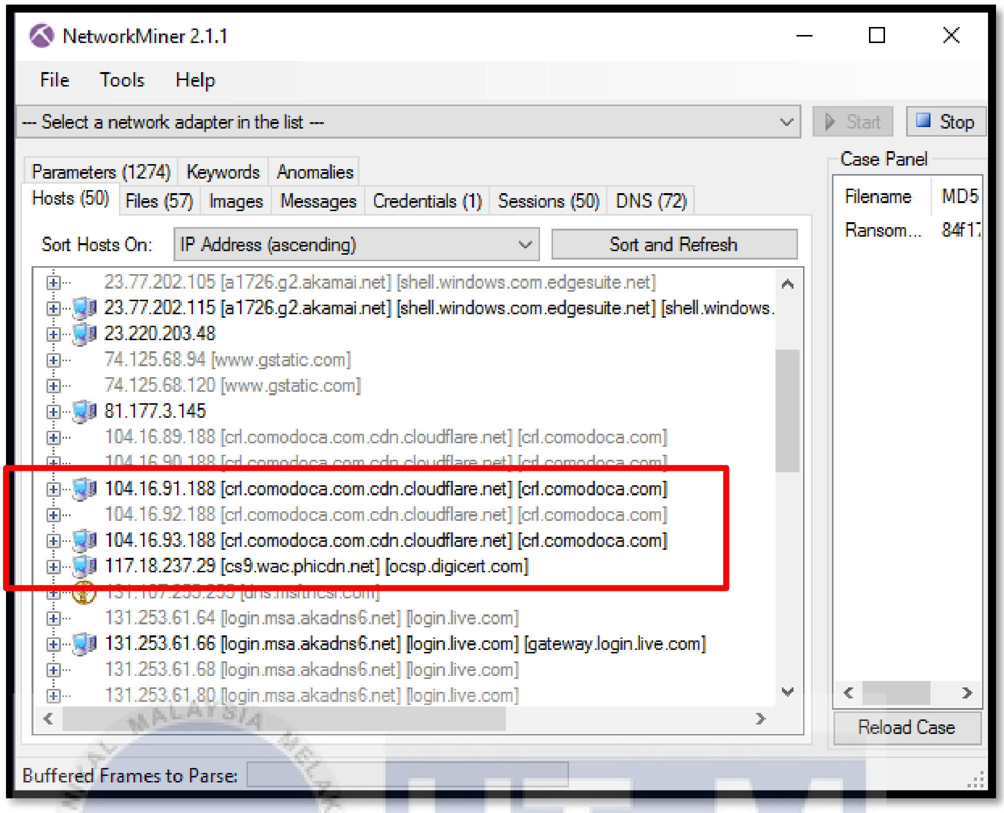
sses are not available, follow these steps:
nd install Tor Browser: https://www.torproject.org/download/download-easy.l
es installation, run the browser and wait for initialization.
address bar: g46mbrrzpfszonuk.onion/3NC9UJPCW3FMSHRP
nstructions on the site.

identification ID: 3NC9UJPCW3FMSHRP !!!

Figure 6.1: Locky ransomware screen

NetworkMinor Analysis

Examining the first sample, **Figure 6.2** below shows that our machine contacted over 50 different IP addresses and domains. If any researcher are new to network forensics, it is a good idea to use a command like 'whois' and see who owns each of these IP addresses.



--- Select a network adapter in the list ---

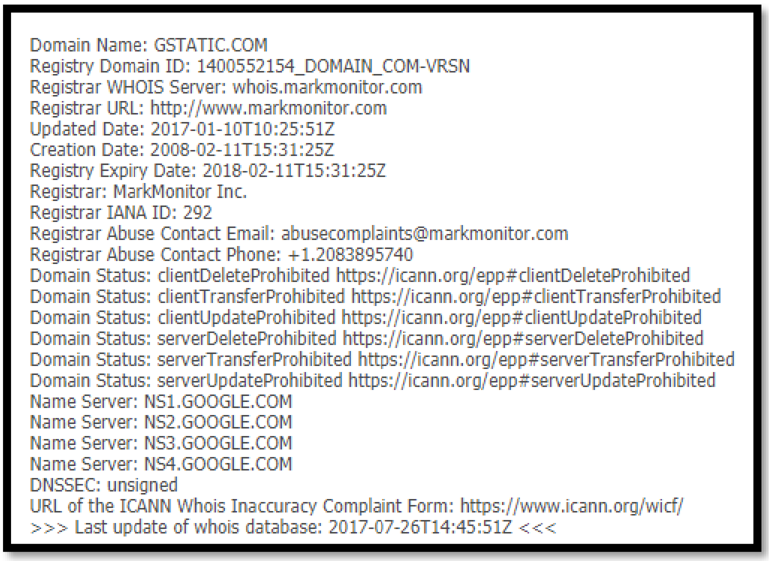
Sort Hosts On: IP Address (ascending)

```
23.77.202.105 [a1726.g2.akamai.net] [shell.windows.com.edgesuite.net]
23.77.202.115 [a1726.g2.akamai.net] [shell.windows.com.edgesuite.net] [shell.windows.
23.220.203.48
74.125.68.94 [www.gstatic.com]
74.125.68.120 [www.gstatic.com]
81.177.3.145
104.16.89.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.90.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.91.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.92.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.93.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
117.18.237.29 [cs9.wac.phicdn.net] [ocsp.digicert.com]
131.107.255.255 [dns.msftncsi.com]
131.253.61.64 [login.msa.akadns6.net] [login.live.com]
131.253.61.66 [login.msa.akadns6.net] [login.live.com] [gateway.login.live.com]
131.253.61.68 [login.msa.akadns6.net] [login.live.com]
131.253.61.80 [login.msa.akadns6.net] [login.live.com]
```

Ransom... 84f17

Figure 6.2: NetworkMiner Hosts tab

The **Figure 6.2** above show a suspicious host: **crl.comodoca.com.cdn.cloudflare.net** that used as baselined for the further analysis that is Wireshark Analysis. Typically, if an IP address or domain belong to a well-known company such as Microsoft, Akamai, or Globalsign, it can reasonably ignore these requests. For example, if 'whois' command is run on the gstatic.com domain, it shows that it is owned by Google as in **Figure 6.3**.



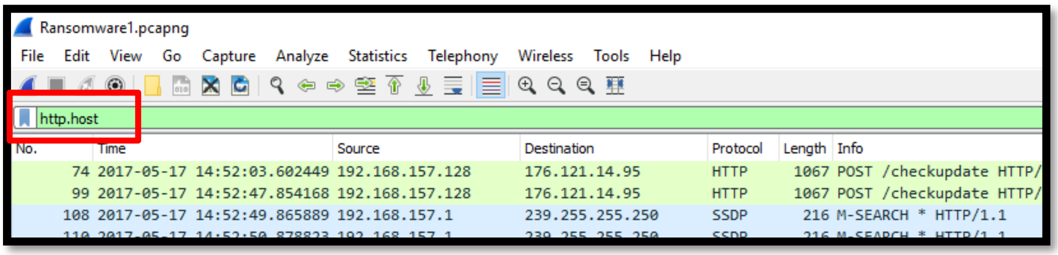
```
Domain Name: GSTATIC.COM
Registry Domain ID: 1400552154_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2017-01-10T10:25:51Z
Creation Date: 2008-02-11T15:31:25Z
Registry Expiry Date: 2018-02-11T15:31:25Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2017-07-26T14:45:51Z <<<
```

Figure 6.3: gstatic.com belongs to Google

Figure 6.3 above shows the results from ‘whois’ with IP Address **104.16.93.188** where the domain name belongs to **GSTATIC.COM** which it owned by **Google**. **crl.comodoca.com.cdn.cloudflare.net** in **Figure 6.2** that used as baselined for the further analysis in Wireshark Analysis.

Wireshark Analysis

With hundreds of IP addresses, protocols, and strings listed, examining a packet capture in Wireshark can be overwhelming. One of the best ways to locate the data quickly is to set a filter for relevant information. For this, “http.host” filter used as in **Figure 6.4**. With this filter, the exact domain of interest can be pinpoint and filter out the rest of the traffic. For this case, **crl.comodoca.com.cdn.cloudflare.net** domain searched in Wireshark as identified in NetworkMiner analysis.

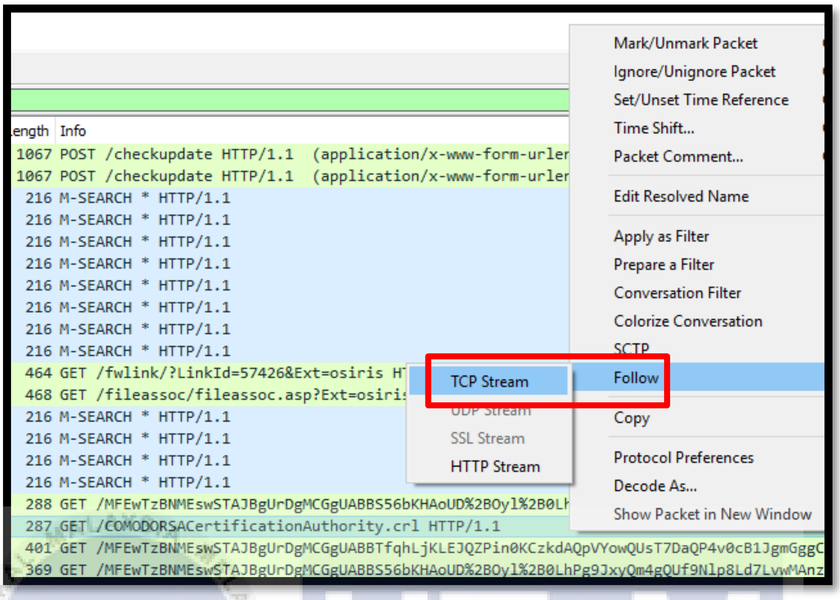


http.host

No.	Time	Source	Destination	Protocol	Length	Info
74	2017-05-17 14:52:03.602449	192.168.157.128	176.121.14.95	HTTP	1067	POST /checkupdate HTTP/
99	2017-05-17 14:52:47.854168	192.168.157.128	176.121.14.95	HTTP	1067	POST /checkupdate HTTP/
108	2017-05-17 14:52:49.865889	192.168.157.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
110	2017-05-17 14:52:50.878823	192.168.157.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

Figure 6.4: Wireshark http.host filter

After entering in the filter, only the packets matching “**http.host**” are displayed. Next, right click one of the entries and select **Follow - TCP Stream** as in **Figure 6.5**. This will show the raw packet details allowing for further analysis.

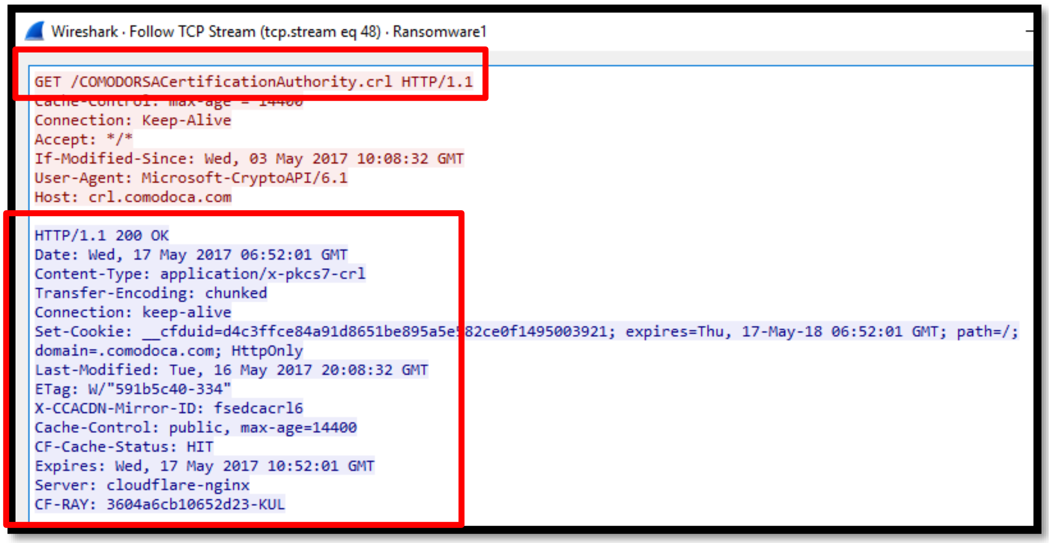


```
ength  Info
1067 POST /checkupdate HTTP/1.1  (application/x-www-form-urler
1067 POST /checkupdate HTTP/1.1  (application/x-www-form-urler
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 464 GET /fwlink/?LinkId=57426&Ext=osiris HT
 468 GET /fileassoc/fileassoc.asp?Ext=osiris
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 216 M-SEARCH * HTTP/1.1
 288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0Lh
 287 GET /COMODORSACertificationAuthority.crl HTTP/1.1
 401 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC
 369 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnz
```

Figure 6.5: Wireshark Follow TCP Stream

From the resulting screen **Figure 6.6**, several interesting things shows up. Starting at the top, it shows that this was an **HTTP GET request**. This means that our machine made a request (GET) to the remote site **crl.comodoca.com.cdn.cloudflare.net**. The remote site responded with an **HTTP/1.1 200 OK**, which shows that the server accepted the request.

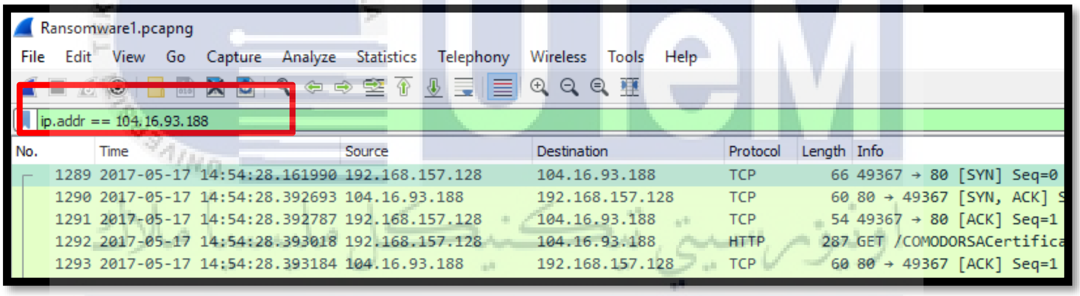
This also presented with the date of the request and information about the server. The version of PHP is running, as well as an indication of where the site is hosted. This Sample 1 result shows **Cloudflare**, which is a content delivery network in the United States.



```
Wireshark · Follow TCP Stream (tcp.stream eq 48) · Ransomware1

GET /COMODORSACertificationAuthority.crl HTTP/1.1
Cache-Control: max-age = 14400
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Wed, 03 May 2017 10:08:32 GMT
User-Agent: Microsoft-CryptoAPI/6.1
Host: crl.comodoca.com

HTTP/1.1 200 OK
Date: Wed, 17 May 2017 06:52:01 GMT
Content-Type: application/x-pkcs7-crl
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=d4c3ffce84a91d8651be895a5e582ce0f1495003921; expires=Thu, 17-May-18 06:52:01 GMT; path=/;
domain=.comodoca.com; HttpOnly
Last-Modified: Tue, 16 May 2017 20:08:32 GMT
ETag: W/"591b5c40-334"
X-CCACDN-Mirror-ID: fsedcacrl6
Cache-Control: public, max-age=14400
CF-Cache-Status: HIT
Expires: Wed, 17 May 2017 10:52:01 GMT
Server: cloudflare-nginx
CF-RAY: 3604a6cb10652d23-KUL
```

Figure 6.6: Wireshark TCP Stream details

Like the **http.host** filter, this Wireshark can also display activity from a specific IP address with the **ip.addr** filter in **Figure 6.7**.


Ransomware1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 104.16.93.188

No.   Time                       Source            Destination      Protocol  Length  Info
 1289 2017-05-17 14:54:28.161990 192.168.157.128   104.16.93.188    TCP        66 49367 → 80 [SYN] Seq=0
 1290 2017-05-17 14:54:28.392693 104.16.93.188     192.168.157.128  TCP        60 80 → 49367 [SYN, ACK] S
 1291 2017-05-17 14:54:28.392787 192.168.157.128   104.16.93.188    TCP        54 49367 → 80 [ACK] Seq=1
 1292 2017-05-17 14:54:28.393018 192.168.157.128   104.16.93.188    HTTP      287 GET /COMODORSACertifica
 1293 2017-05-17 14:54:28.393184 104.16.93.188     192.168.157.128  TCP        60 80 → 49367 [ACK] Seq=1
```

Figure 6.7: Wireshark TCP Stream details

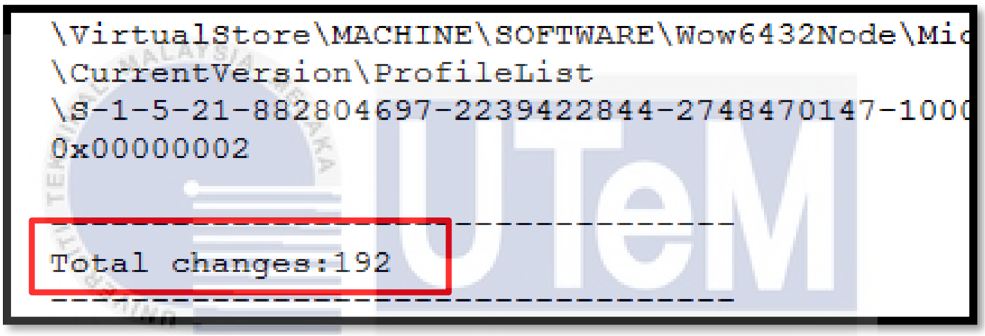
In this case, put in the filter of **ip.addr == 104.16.93.188**. This IP address is the one identified in NetworkMiner that belongs to the **crl.comodoca.com.cdn.cloudflare.net**.

File System Analysis

Analyzing the changes the ransomware made to the file system is another important step. With this, it shows what files the ransomware created, changed, or deleted from our system. These findings frequently include additional malware that is downloaded from external systems, changes to the Windows Registry, and any other file modifications such as deleted or modified files.

Regshot findings

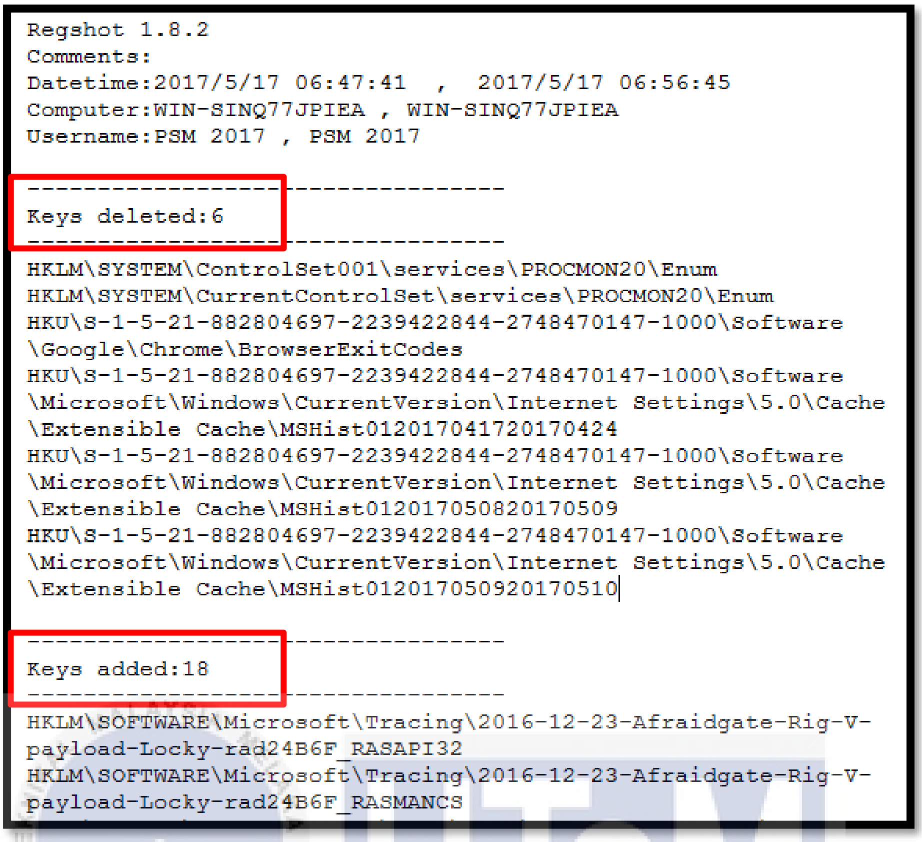
Regshot shows that over 100 changes were made to the Registry from the time the first and second snapshots were taken as in **Figure 6.8** below.



```
\VirtualStore\MACHINE\SOFTWARE\Wow6432Node\Mic
\CurrentVersion\ProfileList
\S-1-5-21-882804697-2239422844-2748470147-1000
0x00000002

----------------------------------------------------------------
Total changes:192
----------------------------------------------------------------
```

Figure 6.8: Regshot total changes

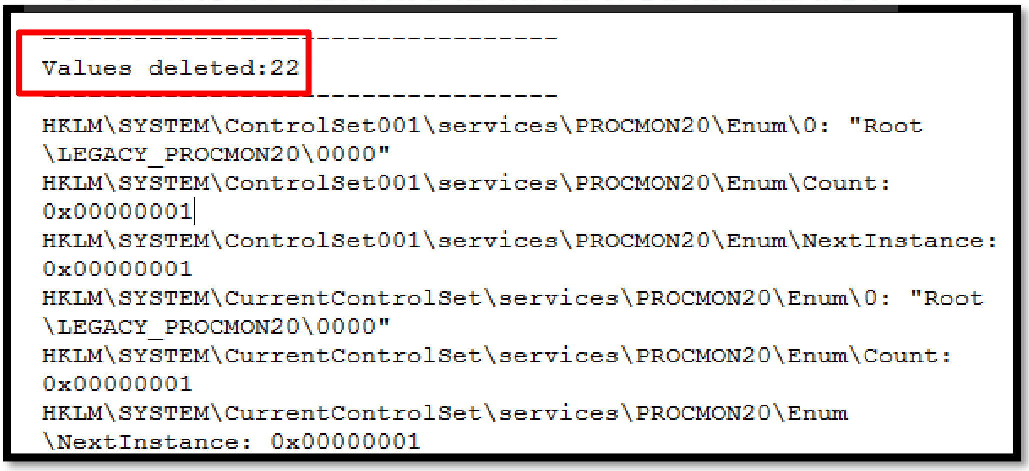
It shows that outlines several different aspects including the following. Remember that the numbers will vary based on the computer as **Total changes:192, Keys deleted: 6, Keys added: 18,** and **Values deleted: 22**. It shows which Registry keys were added or deleted in **Figure 6.9** and which values were deleted **Figure 6.10**.



```
Regshot 1.8.2
Comments:
Datetime:2017/5/17 06:47:41  ,  2017/5/17 06:56:45
Computer:WIN-SINQ77JPIEA , WIN-SINQ77JPIEA
Username:PSM 2017 , PSM 2017

----------------------------------
Keys deleted:6
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Google\Chrome\BrowserExitCodes
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017041720170424
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017050820170509
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017050920170510

----------------------------------
Keys added:18
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\2016-12-23-Afraidgate-Rig-V-
payload-Locky-rad24B6F_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\2016-12-23-Afraidgate-Rig-V-
payload-Locky-rad24B6F_RASMANCS
```

Figure 6.9: Regshot keys added

In addition to listing the changes, it provides in-depth details about which keys were altered by changing happen in the registry. This can be useful in case the researcher wants to manipulate those keys manually.



```
----------------------------------
Values deleted:22
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\0:  "Root
\LEGACY_PROCMON20\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\Count:
0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\NextInstance:
0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum\0:  "Root
\LEGACY_PROCMON20\0000"
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum\Count:
0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum
\NextInstance:  0x00000001
```

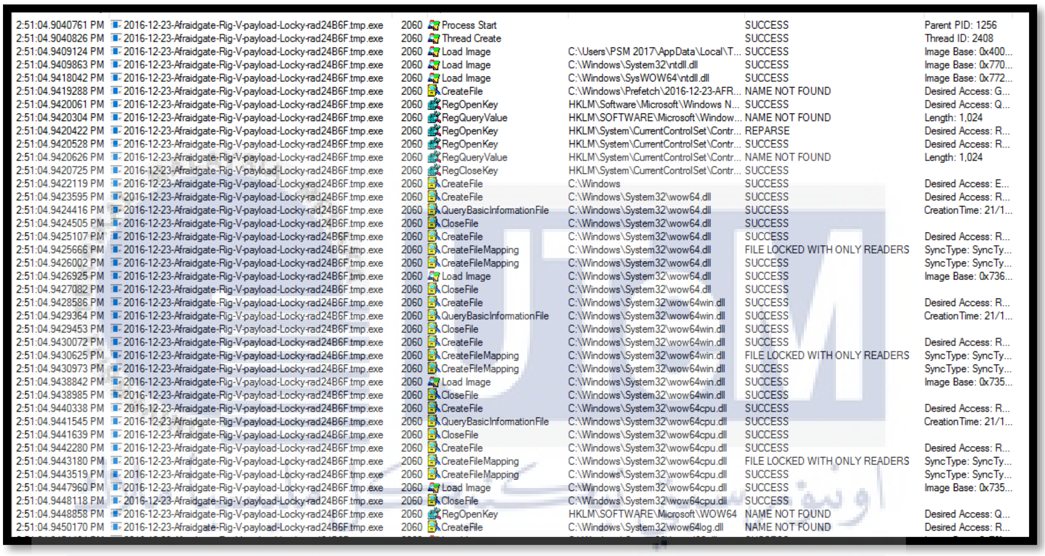
Figure 6.10: Regshot values deleted

It's important to remember that Regshot not only captures the changes that the ransomware made, it also captures the changes made by any other application, including the operating system. Because of this, it can be difficult to identify changes made by the malware if this project relies on this tool alone.

Process Monitor Analysis

Process Monitor also shows changes made to the Registry but it only captures those made by the API call, and may not show everything that occurred.

However, Process Monitor captures a whole lot more information. When viewing the saved output from Process monitor in **Figure 6.11**, the results can be staggering.

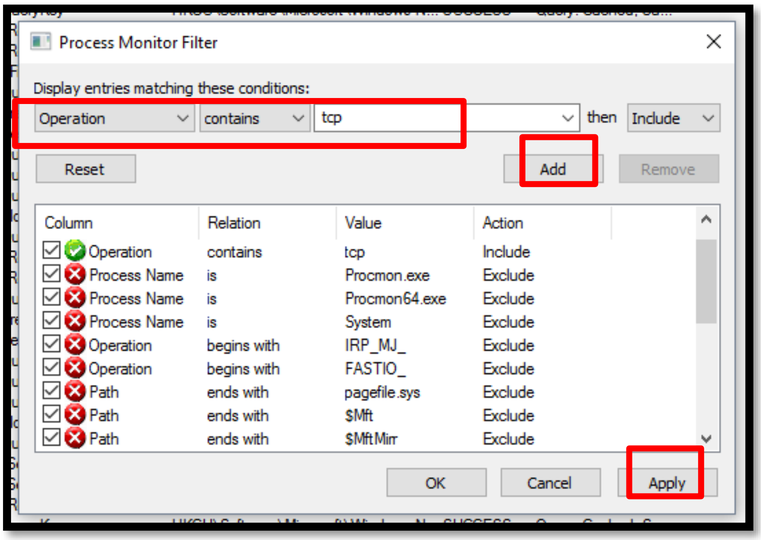


```
2:51:04.9040761 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Process Start                                                          SUCCESS                         Parent PID: 1256
2:51:04.9040826 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Thread Create                                                          SUCCESS                         Thread ID: 2408
2:51:04.9409124 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Load Image                 C:\Users\PSM 2017\AppData\Local\T...        SUCCESS                         Image Base: 0x400...
2:51:04.9409863 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Load Image                 C:\Windows\System32\ntdll.dll               SUCCESS                         Image Base: 0x770...
2:51:04.9418042 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Load Image                 C:\Windows\SysWOW64\ntdll.dll               SUCCESS                         Image Base: 0x772...
2:51:04.9419288 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\Prefetch\2016-12-23-AFR...       NAME NOT FOUND                  Desired Access: G...
2:51:04.9420061 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegOpenKey                 HKLM\Software\Microsoft\Windows N...        SUCCESS                         Desired Access: Q...
2:51:04.9420304 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegQueryValue              HKLM\SOFTWARE\Microsoft\Window...           NAME NOT FOUND                  Length: 1,024
2:51:04.9420422 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegOpenKey                 HKLM\System\CurrentControlSet\Contr...      REPARSE                         Desired Access: R...
2:51:04.9420528 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegOpenKey                 HKLM\System\CurrentControlSet\Contr...      SUCCESS                         Desired Access: R...
2:51:04.9420626 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegQueryValue              HKLM\System\CurrentControlSet\Contr...      NAME NOT FOUND                  Length: 1,024
2:51:04.9420725 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegCloseKey                HKLM\System\CurrentControlSet\Contr...      SUCCESS
2:51:04.9422119 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows                                  SUCCESS                         Desired Access: E...
2:51:04.9423595 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\System32\wow64.dll               SUCCESS                         Desired Access: R...
2:51:04.9424416 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  QueryBasicInformationFile  C:\Windows\System32\wow64.dll               SUCCESS                         CreationTime: 21/1...
2:51:04.9424505 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CloseFile                  C:\Windows\System32\wow64.dll               SUCCESS
2:51:04.9425107 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\System32\wow64.dll               SUCCESS                         Desired Access: R...
2:51:04.9425666 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFileMapping          C:\Windows\System32\wow64.dll               FILE LOCKED WITH ONLY READERS   SyncType: SyncTy...
2:51:04.9426002 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFileMapping          C:\Windows\System32\wow64.dll               SUCCESS                         SyncType: SyncTy...
2:51:04.9426925 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Load Image                 C:\Windows\System32\wow64.dll               SUCCESS                         Image Base: 0x736...
2:51:04.9427082 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CloseFile                  C:\Windows\System32\wow64.dll               SUCCESS
2:51:04.9428586 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\System32\wow64win.dll            SUCCESS                         Desired Access: R...
2:51:04.9429364 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  QueryBasicInformationFile  C:\Windows\System32\wow64win.dll            SUCCESS                         CreationTime: 21/1...
2:51:04.9429453 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CloseFile                  C:\Windows\System32\wow64win.dll            SUCCESS
2:51:04.9430072 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\System32\wow64win.dll            SUCCESS                         Desired Access: R...
2:51:04.9430625 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFileMapping          C:\Windows\System32\wow64win.dll            FILE LOCKED WITH ONLY READERS   SyncType: SyncTy...
2:51:04.9430973 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFileMapping          C:\Windows\System32\wow64win.dll            SUCCESS                         SyncType: SyncTy...
2:51:04.9438842 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Load Image                 C:\Windows\System32\wow64win.dll            SUCCESS                         Image Base: 0x735...
2:51:04.9438985 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CloseFile                  C:\Windows\System32\wow64win.dll            SUCCESS
2:51:04.9440338 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\System32\wow64cpu.dll            SUCCESS                         Desired Access: R...
2:51:04.9441545 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  QueryBasicInformationFile  C:\Windows\System32\wow64cpu.dll            SUCCESS                         CreationTime: 21/1...
2:51:04.9441639 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CloseFile                  C:\Windows\System32\wow64cpu.dll            SUCCESS
2:51:04.9442280 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\System32\wow64cpu.dll            SUCCESS                         Desired Access: R...
2:51:04.9443180 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFileMapping          C:\Windows\System32\wow64cpu.dll            FILE LOCKED WITH ONLY READERS   SyncType: SyncTy...
2:51:04.9443519 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFileMapping          C:\Windows\System32\wow64cpu.dll            SUCCESS                         SyncType: SyncTy...
2:51:04.9447960 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  Load Image                 C:\Windows\System32\wow64cpu.dll            SUCCESS                         Image Base: 0x735...
2:51:04.9448118 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CloseFile                  C:\Windows\System32\wow64cpu.dll            SUCCESS
2:51:04.9448858 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegOpenKey                 HKLM\SOFTWARE\Microsoft\WOW64               NAME NOT FOUND                  Desired Access: Q...
2:51:04.9450170 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  CreateFile                 C:\Windows\System32\wow64log.dll            NAME NOT FOUND                  Desired Access: R...
```

Figure 6.11: Process Monitor initial screen

Again, an easy way to cut through the noise and find interesting artifacts from the ransomware is to use display filters. These filters function much like those in Wireshark, where it can search on specific keywords and ignore the rest of the data.

To use a filter, click on the Filter at the top of the screen and then select **Operation** in the drop-down box on the left. In the next box, select **Contains** and, in the final field, enter “tcp” as in **Figure 6.12**. This will display any TCP connections that were attempted by the Locky ransomware. The results can differ from what is detected in Wireshark packet capture.



Process Monitor Filter

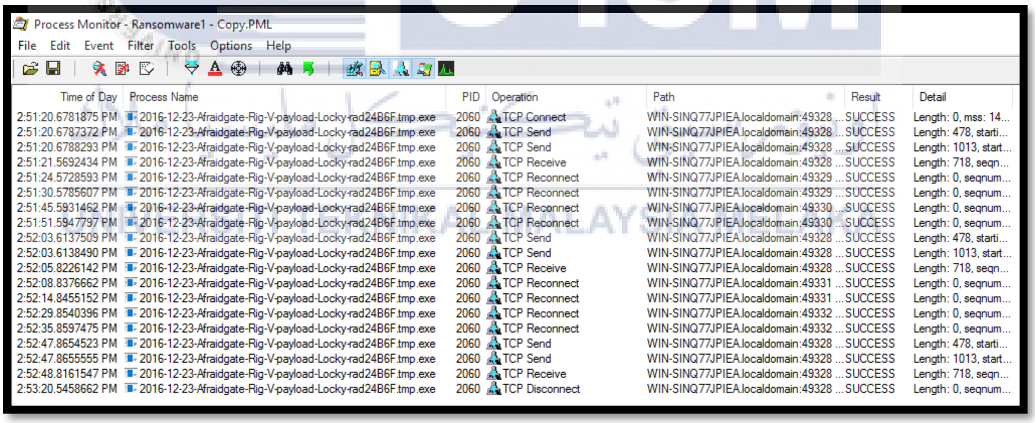
Display entries matching these conditions:

Operation | contains | tcp | then Include

Column	Relation	Value	Action
☑ ✓ Operation	contains	tcp	Include
☑ ☒ Process Name	is	Procmon.exe	Exclude
☑ ☒ Process Name	is	Procmon64.exe	Exclude
☑ ☒ Process Name	is	System	Exclude
☑ ☒ Operation	begins with	IRP_MJ_	Exclude
☑ ☒ Operation	begins with	FASTIO_	Exclude
☑ ☒ Path	ends with	pagefile.sys	Exclude
☑ ☒ Path	ends with	$Mft	Exclude
☑ ☒ Path	ends with	$MftMirr	Exclude

Figure 6.12: Procmon filter TCP

The filtered results in Process Monitor now show a new TCP host that wasn't easily identifiable in the NetworkMiner display in **Figure 6.13**. Therefore, it is important to use the output from multiple tools for this analysis. If had not checked this filter in Procmon, it's possible that could have missed this domain.

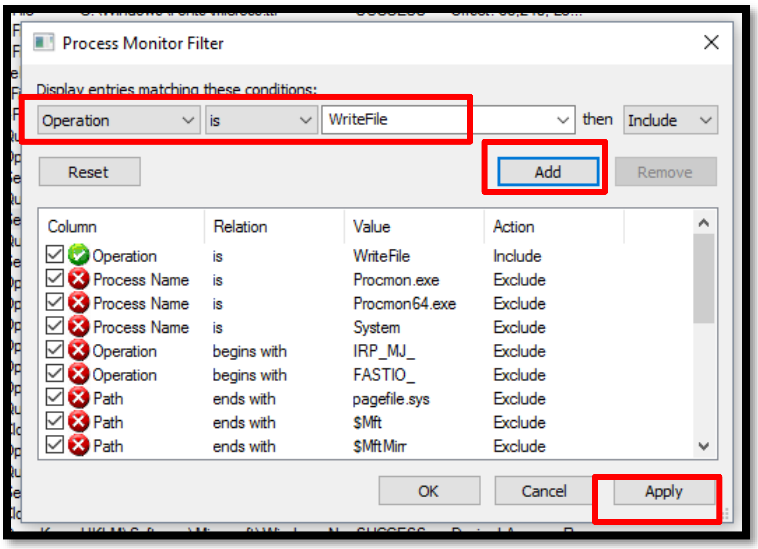


Process Monitor - Ransomware1 - Copy.PML

Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:51:20.6781875 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Connect	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 0, mss: 14...
2:51:20.6787372 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Send	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 478, starti...
2:51:20.6788293 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Send	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 1013, start...
2:51:21.5692434 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Receive	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 718, seqn...
2:51:24.5728593 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49329 ...	SUCCESS	Length: 0, seqnum...
2:51:30.5785607 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49329 ...	SUCCESS	Length: 0, seqnum...
2:51:45.5931462 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49330 ...	SUCCESS	Length: 0, seqnum...
2:51:51.5947797 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49330 ...	SUCCESS	Length: 0, seqnum...
2:52:03.6137509 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Send	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 478, starti...
2:52:03.6138490 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Send	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 1013, start...
2:52:05.8226142 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Receive	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 718, seqn...
2:52:08.8376662 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49331 ...	SUCCESS	Length: 0, seqnum...
2:52:14.8455152 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49331 ...	SUCCESS	Length: 0, seqnum...
2:52:29.8540396 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49332 ...	SUCCESS	Length: 0, seqnum...
2:52:35.8597475 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49332 ...	SUCCESS	Length: 0, seqnum...
2:52:47.8654523 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Send	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 478, starti...
2:52:47.8655555 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Send	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 1013, start...
2:52:48.8161547 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Receive	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 718, seqn...
2:53:20.5458662 PM	2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe	2060	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 0, seqnum...

Figure 6.13: Procmon filter results

Process Monitor can also use a display filter to show any files that were written to the drive by the malware. Next, filter for any Operation matching "WriteFile" to display this in **Figure 6.14**. Knowing what files are created on the system can help to identify additional malware that was downloaded, as well as help build out a list of identifiers that can be search for later.



Process Monitor Filter

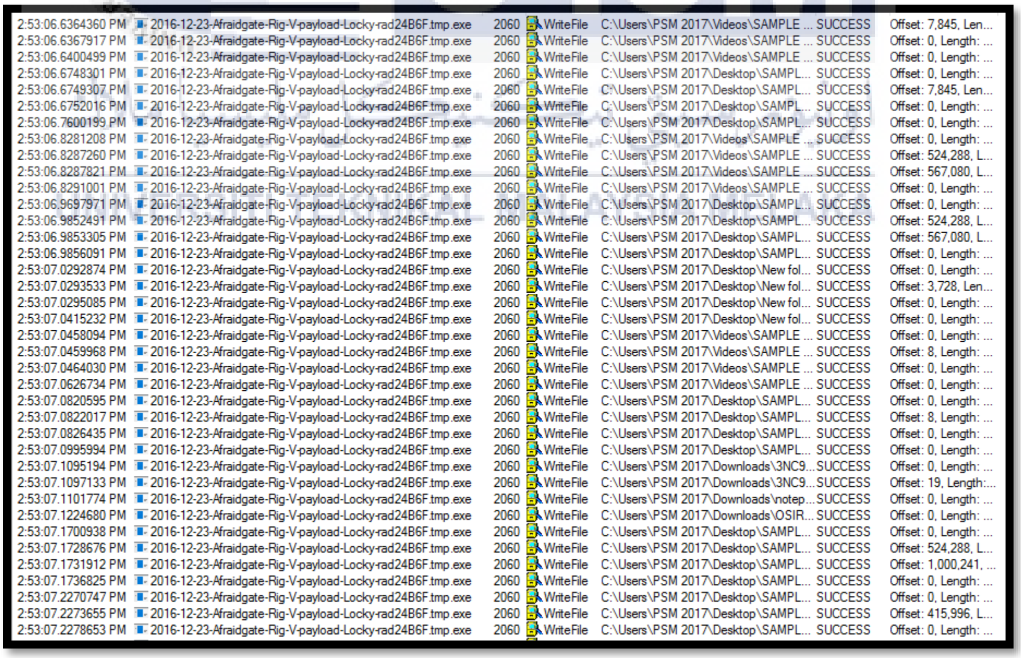
Display entries matching these conditions:

Operation | is | WriteFile | then | Include

Column	Relation	Value	Action
☑ Operation	is	WriteFile	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Path	ends with	pagefile.sys	Exclude
☑ Path	ends with	$Mft	Exclude
☑ Path	ends with	$MftMirr	Exclude

Figure 6.14: Procmon filter Writefile

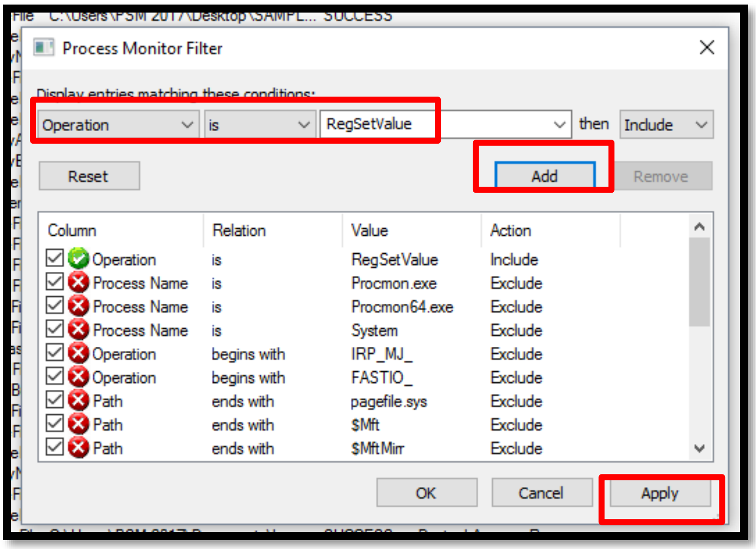
From these filtered results in **Figure 6.15**, this first malware sample, 2016-12-23-Afraidgate-Rig-V-sends-Locky-malware-and-artifacts.exe, created several files on the system.



```
2:53:06.6364360 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 7,845, Len...
2:53:06.6367917 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 0, Length: ...
2:53:06.6400499 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 0, Length: ...
2:53:06.6748301 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:06.6749307 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 7,845, Len...
2:53:06.6752016 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:06.7600199 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:06.8281208 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 0, Length: ...
2:53:06.8287260 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 524,288, L...
2:53:06.8287821 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 567,080, L...
2:53:06.8291001 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 0, Length: ...
2:53:06.9697971 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:06.9852491 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 524,288, L...
2:53:06.9853305 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 567,080, L...
2:53:06.9856091 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:07.0292874 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\New fol...  SUCCESS  Offset: 0, Length: ...
2:53:07.0293533 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\New fol...  SUCCESS  Offset: 3,728, Len...
2:53:07.0295085 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\New fol...  SUCCESS  Offset: 0, Length: ...
2:53:07.0415232 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\New fol...  SUCCESS  Offset: 0, Length: ...
2:53:07.0458094 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 0, Length: ...
2:53:07.0459968 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 8, Length: ...
2:53:07.0464030 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 0, Length: ...
2:53:07.0626734 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Videos\SAMPLE ...  SUCCESS  Offset: 0, Length: ...
2:53:07.0820595 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:07.0822017 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 8, Length: ...
2:53:07.0826435 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:07.0995994 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:07.1095194 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Downloads\3NC9...SUCCESS  Offset: 0, Length: ...
2:53:07.1097133 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Downloads\3NC9...SUCCESS  Offset: 19, Length:...
2:53:07.1101774 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Downloads\notep...SUCCESS  Offset: 0, Length: ...
2:53:07.1224680 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Downloads\OSIR...SUCCESS  Offset: 0, Length: ...
2:53:07.1700938 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:07.1728676 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 524,288, L...
2:53:07.1731912 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 1,000,241, ...
2:53:07.1736825 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:07.2270747 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
2:53:07.2273655 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 415,996, L...
2:53:07.2278653 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  WriteFile  C:\Users\PSM 2017\Desktop\SAMPL...  SUCCESS  Offset: 0, Length: ...
```

Figure 6.15: Procmon filter WriteFile results

Procmon also display any changes 2016-12-23-Afraidgate-Rig-V-sends-Locky-malware-and-artifacts.exe made to the Windows Registry. For this, it shows for the value named RegSetValue in **Figure 6.16** below.



Process Monitor Filter

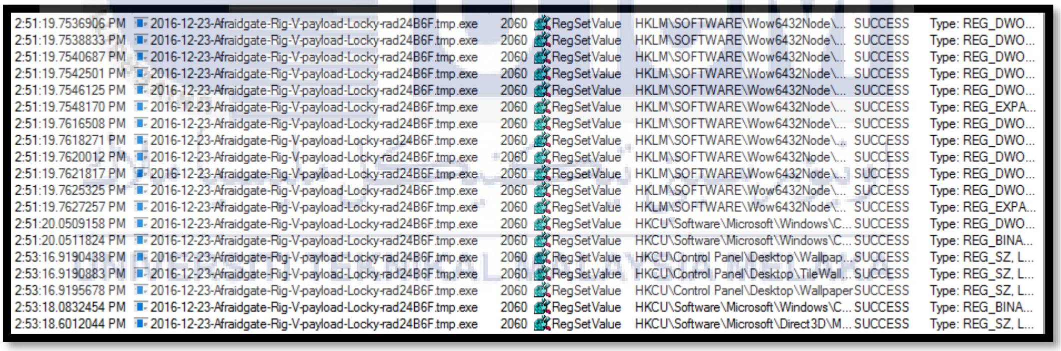
Display entries matching these conditions:

Operation · is · RegSetValue · then · Include

Column	Relation	Value	Action
☑ ✓ Operation	is	RegSetValue	Include
☑ ☒ Process Name	is	Procmon.exe	Exclude
☑ ☒ Process Name	is	Procmon64.exe	Exclude
☑ ☒ Process Name	is	System	Exclude
☑ ☒ Operation	begins with	IRP_MJ_	Exclude
☑ ☒ Operation	begins with	FASTIO_	Exclude
☑ ☒ Path	ends with	pagefile.sys	Exclude
☑ ☒ Path	ends with	$Mft	Exclude
☑ ☒ Path	ends with	$MftMirr	Exclude

Figure 6.16: Procmon filter RegSetValue

After applying our filter, it shows that 2016-12-23-Afraidgate-Rig-V-sends-Locky-malware-and-artifacts.exe made several changes to the registry when it executed in **Figure 6.17**.

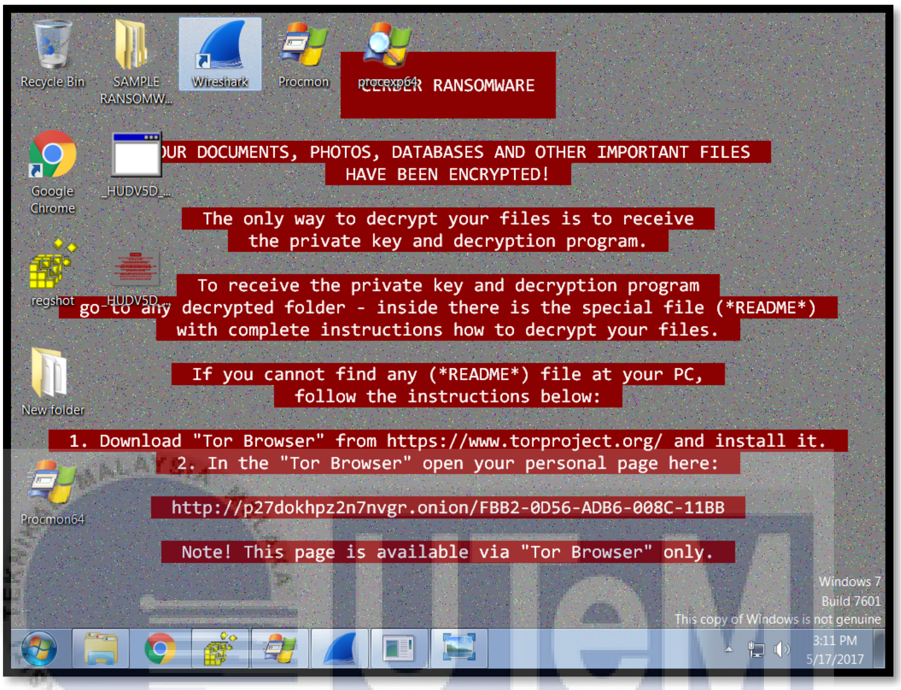


```
2:51:19.7536906 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7538833 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7540687 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7542501 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7546125 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7548170 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_EXPA...
2:51:19.7616508 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7618271 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7620012 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7621817 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7625325 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
2:51:19.7627257 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_EXPA...
2:51:20.0509158 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_DWO...
2:51:20.0511824 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_BINA...
2:53:16.9190438 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKCU\Control Panel\Desktop\Wallpap...  SUCCESS  Type: REG_SZ, L...
2:53:16.9190883 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKCU\Control Panel\Desktop\TileWall...  SUCCESS  Type: REG_SZ, L...
2:53:16.9195678 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKCU\Control Panel\Desktop\Wallpaper  SUCCESS  Type: REG_SZ, L...
2:53:18.0832454 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_BINA...
2:53:18.6012044 PM  2016-12-23-Afraidgate-Rig-V-payload-Locky-rad24B6F.tmp.exe  2060  RegSetValue  HKCU\Software\Microsoft\Direct3D\M...  SUCCESS  Type: REG_SZ, L...
```

Figure 6.17: Procmon filter RegSetValue results

2017-01-05-psuedoDarkleech-Rig-V-sends-Cerber-malware-and-artifacts

Second ransomware sample named Cerber has been run in a controlled environment on a virtual machine. Shortly after executing the malware presented with a notification screen as in **Figure 6.18**.



CERBER RANSOMWARE

OUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*README*)
with complete instructions how to decrypt your files.

If you cannot find any (*README*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

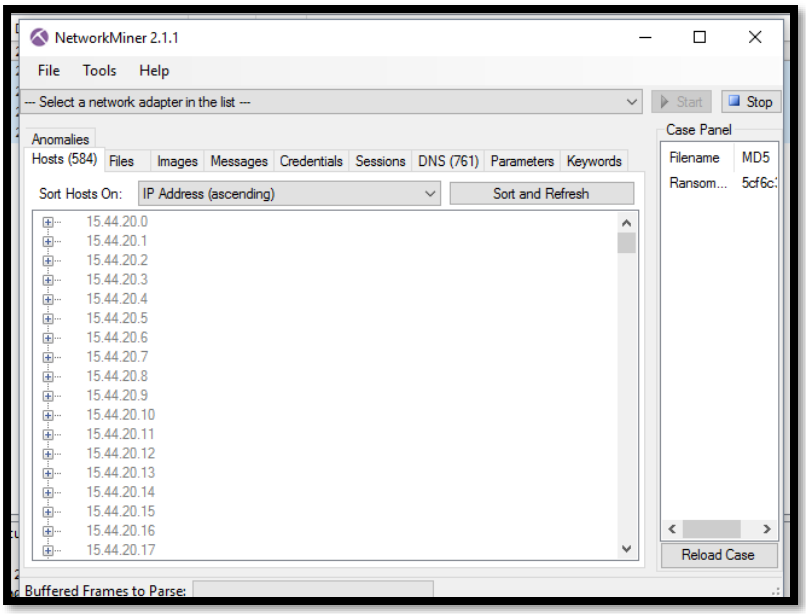
http://p27dokhpz2n7nvgr.onion/FBB2-0D56-ADB6-008C-11BB

Note! This page is available via "Tor Browser" only.

Figure 6.18: Cerber ransomware screen

NetworkMinor Analysis

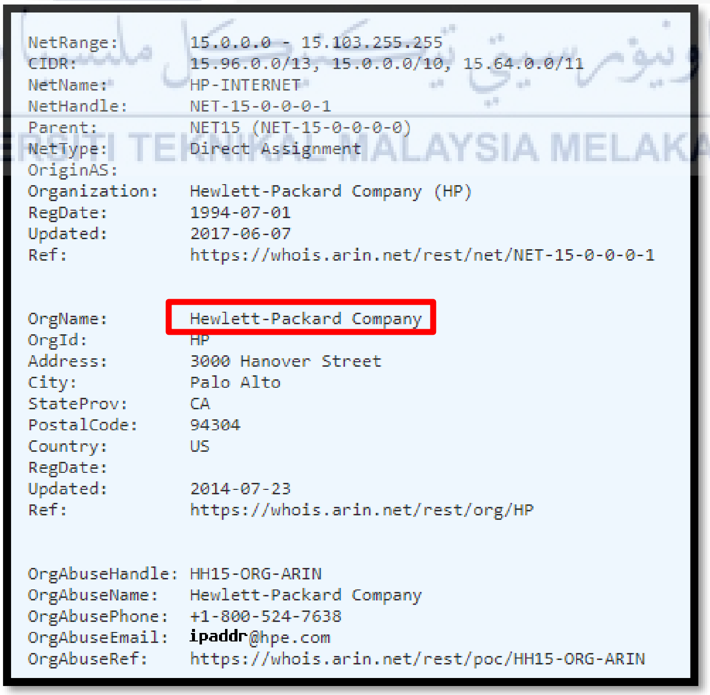
Examining the second sample, it shows that our machine contacted over 50 different IP addresses and domains as in **Figure 6.19**. If you are new to network forensics, it is a good idea to use a command like ‘whois’ and see who owns each of these IP addresses.



```
15.44.20.0
15.44.20.1
15.44.20.2
15.44.20.3
15.44.20.4
15.44.20.5
15.44.20.6
15.44.20.7
15.44.20.8
15.44.20.9
15.44.20.10
15.44.20.11
15.44.20.12
15.44.20.13
15.44.20.14
15.44.20.15
15.44.20.16
15.44.20.17
```

Figure 6.19: NetworkMiner Hosts tab

The **Figure 6.19** above show about **584** hosts in the **.pcap** file during the execution of Cerber ransomware. Run the 'whois' command on the one of the IP Address "**192.44.20.0**", it shows that owned by **Hewlett-Packard Company** which it is a computer that used to do the investigation of Cerber ransomware as in **Figure 6.20**.

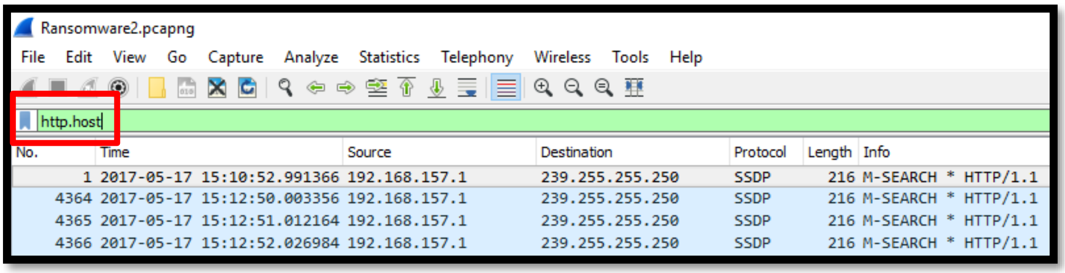


```
NetRange:       15.0.0.0 - 15.103.255.255
CIDR:           15.96.0.0/13, 15.0.0.0/10, 15.64.0.0/11
NetName:        HP-INTERNET
NetHandle:      NET-15-0-0-0-1
Parent:         NET15 (NET-15-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   Hewlett-Packard Company (HP)
RegDate:        1994-07-01
Updated:        2017-06-07
Ref:            https://whois.arin.net/rest/net/NET-15-0-0-0-1


OrgName:        Hewlett-Packard Company
OrgId:          HP
Address:        3000 Hanover Street
City:           Palo Alto
StateProv:      CA
PostalCode:     94304
Country:        US
RegDate:
Updated:        2014-07-23
Ref:            https://whois.arin.net/rest/org/HP


OrgAbuseHandle: HH15-ORG-ARIN
OrgAbuseName:   Hewlett-Packard Company
OrgAbusePhone:  +1-800-524-7638
OrgAbuseEmail:  ipaddr@hpe.com
OrgAbuseRef:    https://whois.arin.net/rest/poc/HH15-ORG-ARIN
```

Figure 6.20: IP Address 192.44.20.0 belongs to Hewlett-Packard Company

Wireshark Analysis

Same as Wireshark Analysis on first sample: Locky ransomware. Open the .pcapng file that saved during the execution of Cerber ransomware in Wireshark, and search for "**http.host**" as shows in results in **Figure 6.21**.



http.host

```
No.     Time                        Source           Destination       Protocol  Length Info
      1 2017-05-17 15:10:52.991366 192.168.157.1    239.255.255.250   SSDP         216 M-SEARCH * HTTP/1.1
   4364 2017-05-17 15:12:50.003356 192.168.157.1    239.255.255.250   SSDP         216 M-SEARCH * HTTP/1.1
   4365 2017-05-17 15:12:51.012164 192.168.157.1    239.255.255.250   SSDP         216 M-SEARCH * HTTP/1.1
   4366 2017-05-17 15:12:52.026984 192.168.157.1    239.255.255.250   SSDP         216 M-SEARCH * HTTP/1.1
```

Figure 6.21: Wireshark "http.host" filter

After entering in the filter, only the packets matching "**http.host**" are displayed. Next, right click one of the entries and select **Follow - UDP Stream** as in **Figure 6.22**. This will show the raw packet details allowing for further analysis.

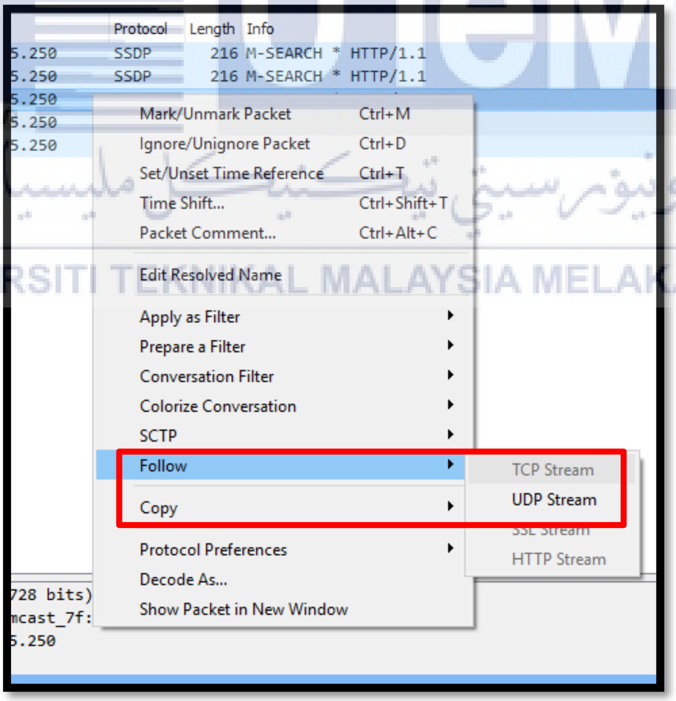
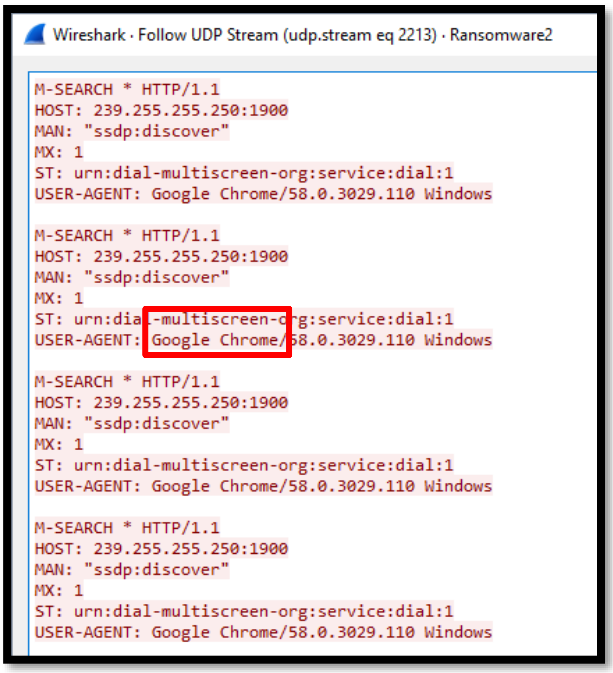

```
        Protocol  Length Info
5.250   SSDP        216 M-SEARCH * HTTP/1.1
5.250   SSDP        216 M-SEARCH * HTTP/1.1
5.250
5.250
5.250
728 bits)
mcast_7f:
5.250
```

Figure 6.22: Wireshark Follow UDP Stream

From the resulting screen **Figure 6.23**, there are no suspicious information shows up. In **UDP Stream** only state about the **Google Chrome**.



Wireshark · Follow UDP Stream (udp.stream eq 2213) · Ransomware2

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows
```

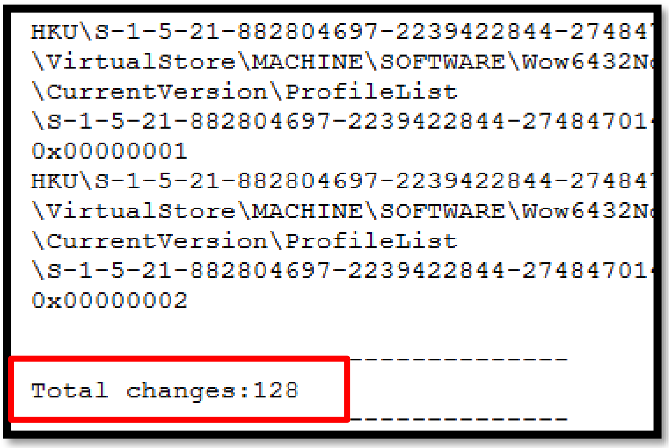
Figure 6.23: Wireshark TCP Stream details

The details of Follow UDP Stream, it shows about the **Host: "239.255.255.250"** that this analysis assume there is no bad outbound network connection occurs. It just belongs **Google Chrome**.

File System Analysis

Regshot findings

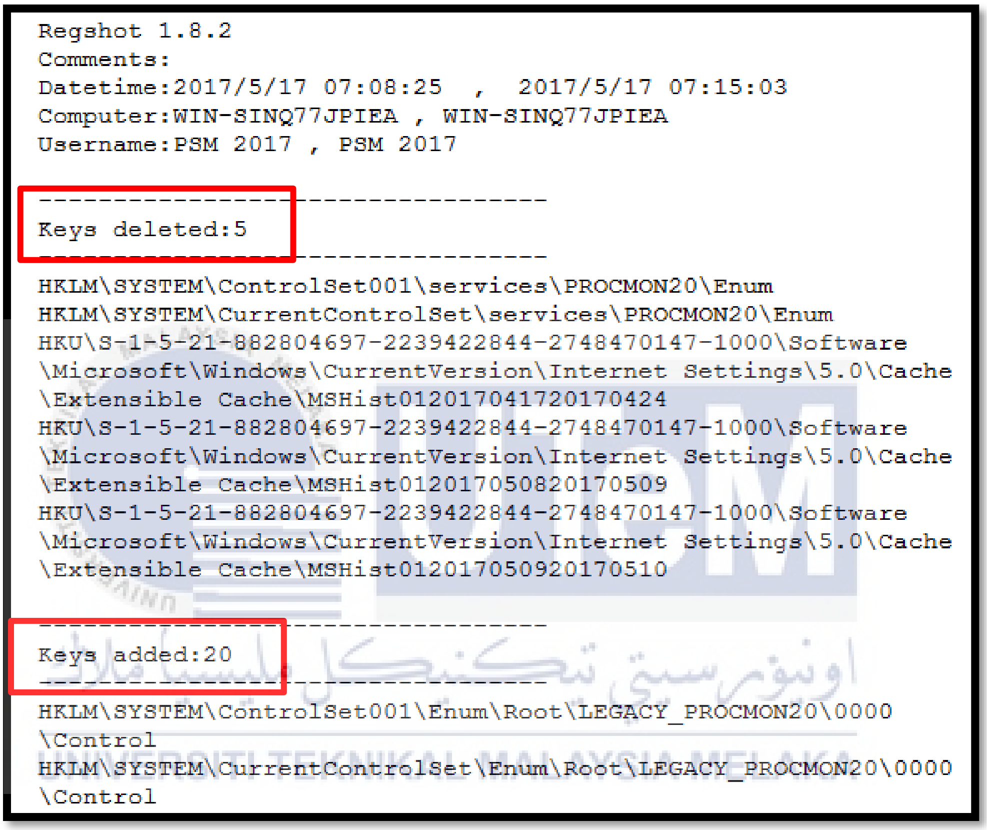
Regshot shows that over 100 changes were made to the Registry from the time the first and second snapshots were taken as in **Figure 6.24** below.



```
HKU\S-1-5-21-882804697-2239422844-27484
\VirtualStore\MACHINE\SOFTWARE\Wow6432N
\CurrentVersion\ProfileList
\S-1-5-21-882804697-2239422844-27484701
0x00000001
HKU\S-1-5-21-882804697-2239422844-27484
\VirtualStore\MACHINE\SOFTWARE\Wow6432N
\CurrentVersion\ProfileList
\S-1-5-21-882804697-2239422844-27484701
0x00000002

                                -----------------
Total changes:128
                                -----------------
```

Figure 6.24: Regshot total changes

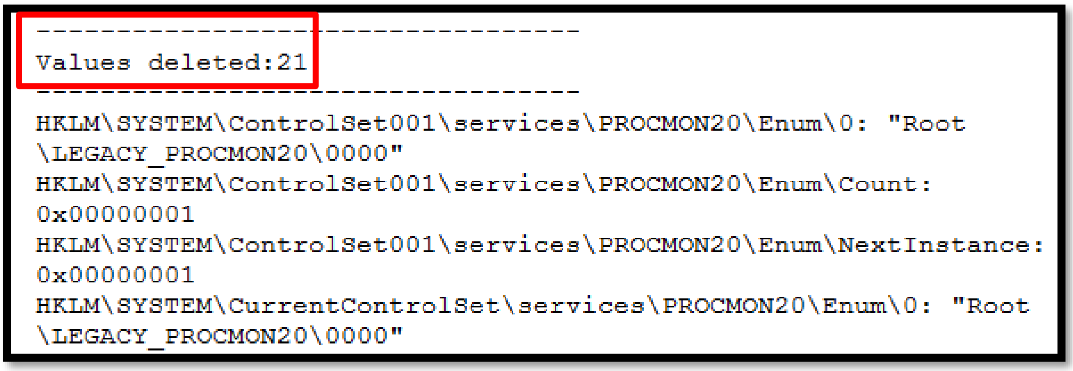
If continue to scroll down the document, it shows that it outlines several different aspects including the following. Remember that the numbers will vary based on the computer as **Total changes:128, Keys deleted: 5, Keys added: 20,** and **Values deleted: 21**. It shows which Registry keys were added or deleted in **Figure 6.25** and which values were deleted **Figure 6.26**.



```
Regshot 1.8.2
Comments:
Datetime:2017/5/17 07:08:25  ,  2017/5/17 07:15:03
Computer:WIN-SINQ77JPIEA , WIN-SINQ77JPIEA
Username:PSM 2017 , PSM 2017

----------------------------------
Keys deleted:5
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017041720170424
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017050820170509
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017050920170510

----------------------------------
Keys added:20
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON20\0000
\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON20\0000
\Control
```

Figure 6.25: Regshot keys added

In addition to listing the changes, it provides in-depth details about which keys were altered by changing happen in the registry. This can be useful in case researcher want to manipulate those keys manually.



```
-----------------------------------
Values deleted:21
-----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\0: "Root
\LEGACY_PROCMON20\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\Count:
0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\NextInstance:
0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum\0: "Root
\LEGACY_PROCMON20\0000"
```

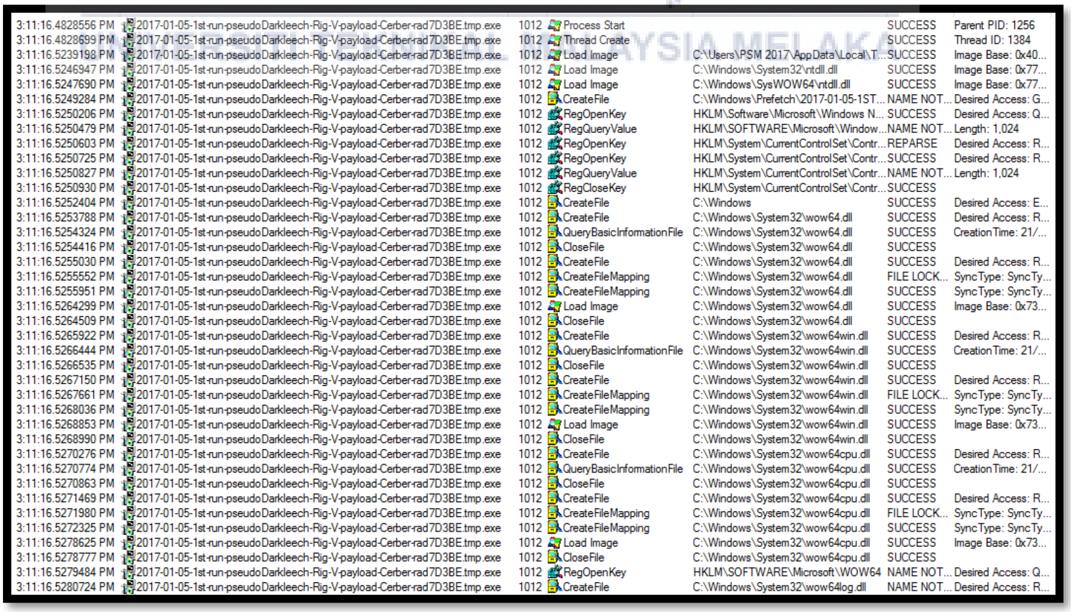
Figure 6.26: Regshot values deleted

Both ransomware not showing much of differences for the registry changes. But two more sample are not reveals yet to see the general changes in registry if this malware infected the computer.

Process Monitor Analysis

Process Monitor also shows changes made to the Registry but it only captures those made by the API call, and may not show everything that occurred.

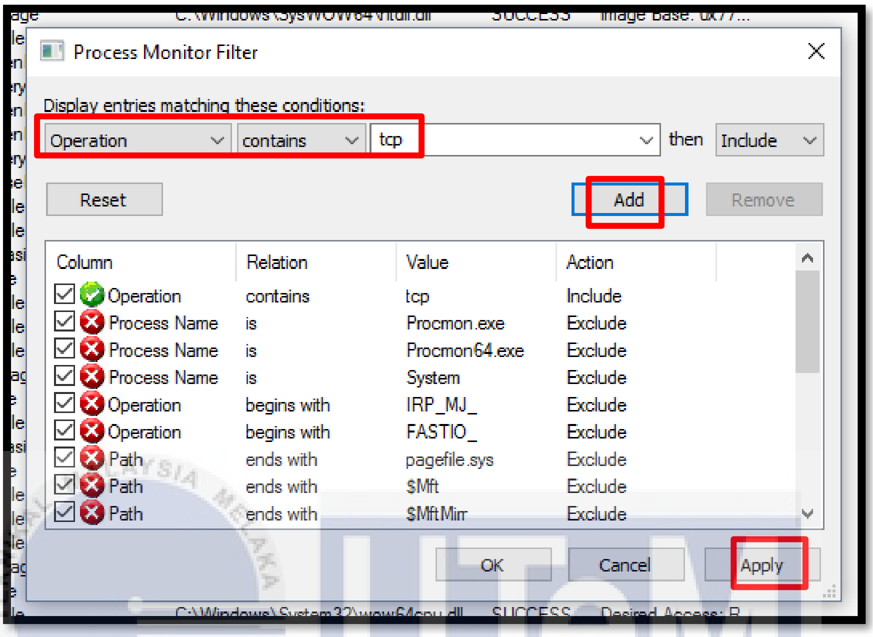
However, Process Monitor captures a whole lot more information. When viewing the saved output from Process monitor in **Figure 6.27**, the results can be staggering



```
3:11:16.4828556 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Process Start                                                      SUCCESS      Parent PID: 1256
3:11:16.4828699 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Thread Create                                                      SUCCESS      Thread ID: 1384
3:11:16.5239198 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Load Image                C:\Users\PSM 2017\AppData\Local\T...     SUCCESS      Image Base: 0x40...
3:11:16.5246947 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Load Image                C:\Windows\System32\ntdll.dll            SUCCESS      Image Base: 0x77...
3:11:16.5247690 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Load Image                C:\Windows\SysWOW64\ntdll.dll            SUCCESS      Image Base: 0x77...
3:11:16.5249284 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\Prefetch\2017-01-05-1ST...    NAME NOT...  Desired Access: G...
3:11:16.5250206 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  RegOpenKey                HKLM\Software\Microsoft\Windows N...     SUCCESS      Desired Access: Q...
3:11:16.5250479 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  RegQueryValue             HKLM\SOFTWARE\Microsoft\Window...        NAME NOT...  Length: 1,024
3:11:16.5250603 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  RegOpenKey                HKLM\System\CurrentControlSet\Contr...   REPARSE      Desired Access: R...
3:11:16.5250725 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  RegOpenKey                HKLM\System\CurrentControlSet\Contr...   SUCCESS      Desired Access: R...
3:11:16.5250827 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  RegQueryValue             HKLM\System\CurrentControlSet\Contr...   NAME NOT...  Length: 1,024
3:11:16.5250930 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  RegCloseKey               HKLM\System\CurrentControlSet\Contr...   SUCCESS
3:11:16.5252404 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows                               SUCCESS      Desired Access: E...
3:11:16.5253788 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\System32\wow64.dll            SUCCESS      Desired Access: R...
3:11:16.5254324 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  QueryBasicInformationFile C:\Windows\System32\wow64.dll            SUCCESS      CreationTime: 21/...
3:11:16.5254416 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CloseFile                 C:\Windows\System32\wow64.dll            SUCCESS
3:11:16.5255030 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\System32\wow64.dll            SUCCESS      Desired Access: R...
3:11:16.5255552 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFileMapping         C:\Windows\System32\wow64.dll            FILE LOCK... SyncType: SyncTy...
3:11:16.5255951 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFileMapping         C:\Windows\System32\wow64.dll            SUCCESS      SyncType: SyncTy...
3:11:16.5264299 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Load Image                C:\Windows\System32\wow64.dll            SUCCESS      Image Base: 0x73...
3:11:16.5264509 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CloseFile                 C:\Windows\System32\wow64.dll            SUCCESS
3:11:16.5265922 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\System32\wow64win.dll         SUCCESS      Desired Access: R...
3:11:16.5266444 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  QueryBasicInformationFile C:\Windows\System32\wow64win.dll         SUCCESS      CreationTime: 21/...
3:11:16.5266535 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CloseFile                 C:\Windows\System32\wow64win.dll         SUCCESS
3:11:16.5267150 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\System32\wow64win.dll         SUCCESS      Desired Access: R...
3:11:16.5267661 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFileMapping         C:\Windows\System32\wow64win.dll         FILE LOCK... SyncType: SyncTy...
3:11:16.5268036 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFileMapping         C:\Windows\System32\wow64win.dll         SUCCESS      SyncType: SyncTy...
3:11:16.5268853 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Load Image                C:\Windows\System32\wow64win.dll         SUCCESS      Image Base: 0x73...
3:11:16.5268990 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CloseFile                 C:\Windows\System32\wow64win.dll         SUCCESS
3:11:16.5270276 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\System32\wow64cpu.dll         SUCCESS      Desired Access: R...
3:11:16.5270774 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  QueryBasicInformationFile C:\Windows\System32\wow64cpu.dll         SUCCESS      CreationTime: 21/...
3:11:16.5270863 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CloseFile                 C:\Windows\System32\wow64cpu.dll         SUCCESS
3:11:16.5271469 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\System32\wow64cpu.dll         SUCCESS      Desired Access: R...
3:11:16.5271980 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFileMapping         C:\Windows\System32\wow64cpu.dll         FILE LOCK... SyncType: SyncTy...
3:11:16.5272325 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFileMapping         C:\Windows\System32\wow64cpu.dll         SUCCESS      SyncType: SyncTy...
3:11:16.5278625 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  Load Image                C:\Windows\System32\wow64cpu.dll         SUCCESS      Image Base: 0x73...
3:11:16.5278777 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CloseFile                 C:\Windows\System32\wow64cpu.dll         SUCCESS
3:11:16.5279484 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  RegOpenKey                HKLM\SOFTWARE\Microsoft\WOW64            NAME NOT...  Desired Access: Q...
3:11:16.5280724 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  CreateFile                C:\Windows\System32\wow64log.dll         NAME NOT...  Desired Access: R...
```

Figure 6.27: Process Monitor initial screen

To use a filter, click on the Filter at the top of the screen and then select Operation in the drop-down box on the left. In the next box, select Contains and, in the final field, enter "tcp" **Figure 6.28**. This will display any TCP connections that were attempted by the malware. The results can differ from what Wireshark packet capture detected.



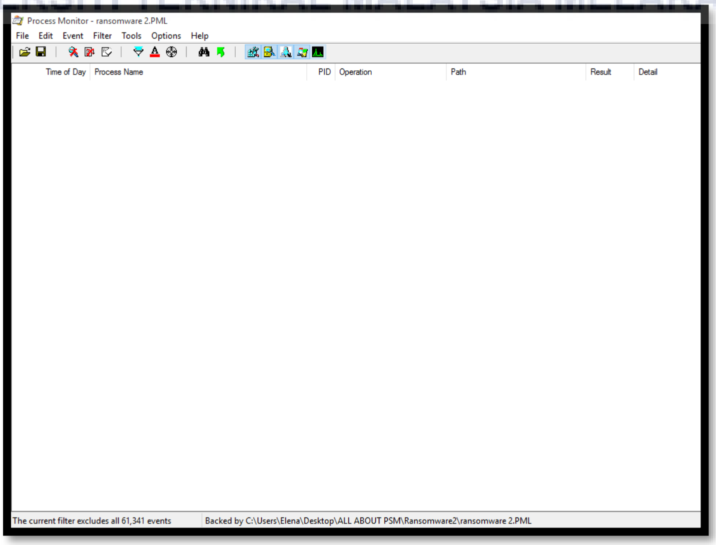
Display entries matching these conditions:

Operation | contains | tcp | then Include

	Column	Relation	Value	Action
☑	✓ Operation	contains	tcp	Include
☑	☒ Process Name	is	Procmon.exe	Exclude
☑	☒ Process Name	is	Procmon64.exe	Exclude
☑	☒ Process Name	is	System	Exclude
☑	☒ Operation	begins with	IRP_MJ_	Exclude
☑	☒ Operation	begins with	FASTIO_	Exclude
☑	☒ Path	ends with	pagefile.sys	Exclude
☑	☒ Path	ends with	$Mft	Exclude
☑	☒ Path	ends with	$MftMirr	Exclude

Figure 6.28: Procmon filter TCP

After filtering, the results of **Operation** contain **TCP** in **Figure 6.29** do not showed up, this is means no TCP connection when this sample infected the computer.

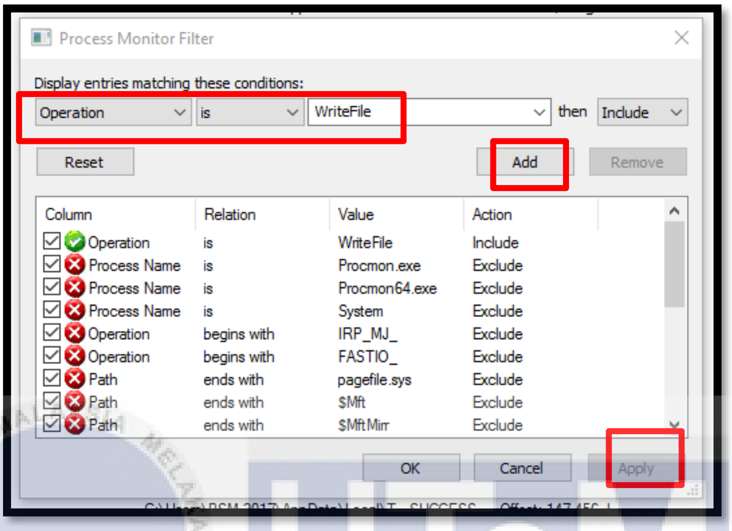


The current filter excludes all 61,341 events

Backed by C:\Users\Elena\Desktop\ALL ABOUT PSM\Ransomware2\ransomware 2.PML

Figure 6.29: Procmon filter results

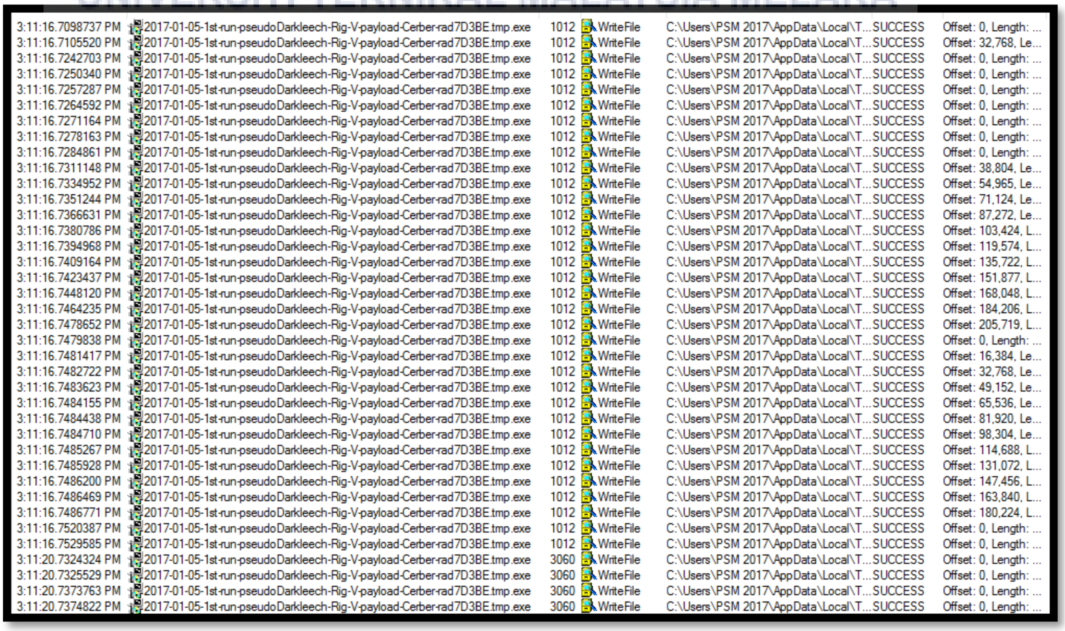
Process Monitor can also use a display filter to show any files that were written to the drive by the malware. Filter for any Operation matching "WriteFile" to display this in **Figure 6.30**. Knowing what files are created on the system can help us identify additional malware that was downloaded, as well as help build out a list of identifiers that can search for later.



Column	Relation	Value	Action
☑ Operation	is	WriteFile	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Path	ends with	pagefile.sys	Exclude
☑ Path	ends with	$Mft	Exclude
☑ Path	ends with	$MftMirr	Exclude

Figure 6.30: Procmon filter Writefile

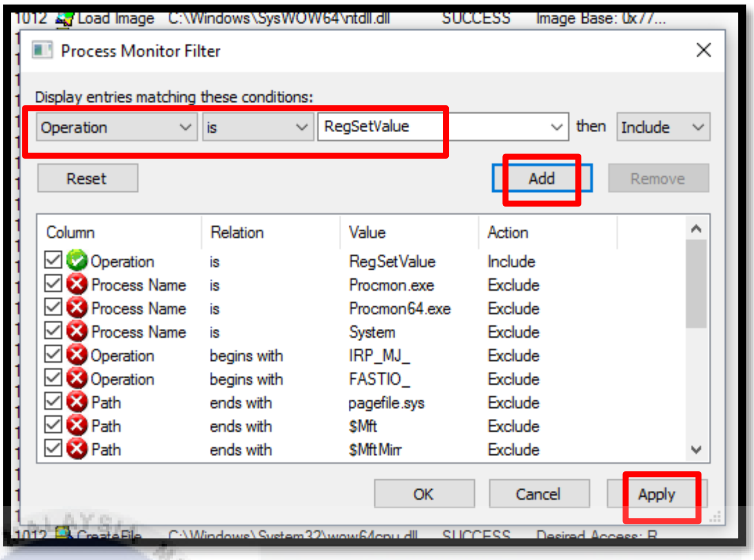
From these filtered results in **Figure 6.31**, it shows that our malware sample, 2017-01-05-psuedoDarkleech-Rig-V-sends-Cerber-malware-and-artifacts.exe, created several files on the system.



```
3:11:16.7098737 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7105520 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 32,768, Le...
3:11:16.7242703 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7250340 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7257287 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7264592 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7271164 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7278163 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7284861 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7311148 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 38,804, Le...
3:11:16.7334952 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 54,965, Le...
3:11:16.7351244 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 71,124, Le...
3:11:16.7366631 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 87,272, Le...
3:11:16.7380786 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 103,424, L...
3:11:16.7394968 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 119,574, L...
3:11:16.7409164 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 135,722, L...
3:11:16.7423437 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 151,877, L...
3:11:16.7448120 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 168,048, L...
3:11:16.7464235 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 184,206, L...
3:11:16.7478652 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 205,719, L...
3:11:16.7479838 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7481417 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 16,384, Le...
3:11:16.7482722 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 32,768, Le...
3:11:16.7483623 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 49,152, Le...
3:11:16.7484155 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 65,536, Le...
3:11:16.7484438 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 81,920, Le...
3:11:16.7484710 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 98,304, Le...
3:11:16.7485267 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 114,688, L...
3:11:16.7485928 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 131,072, L...
3:11:16.7486200 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 147,456, L...
3:11:16.7486469 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 163,840, L...
3:11:16.7486771 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 180,224, L...
3:11:16.7520387 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:16.7529585 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  1012  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:20.7324324 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:20.7325529 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:20.7373763 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
3:11:20.7374822 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  WriteFile  C:\Users\PSM 2017\AppData\Local\T...SUCCESS  Offset: 0, Length: ...
```

Figure 6.31: Procmon filter WriteFile results

it can also display any changes 2017-01-05-psuedoDarkleech-Rig-V-sends-Cerber-malware-and-artifacts.exe made to the Windows Registry. For this, it will look for the value named RegSetValue in **Figure 6.32** below.



```
1012  Load Image  C:\Windows\SysWOW64\ntdll.dll  SUCCESS  Image Base: 0x77...
```

Process Monitor Filter

Display entries matching these conditions:

Operation | is | RegSetValue | then | Include

Reset | Add | Remove

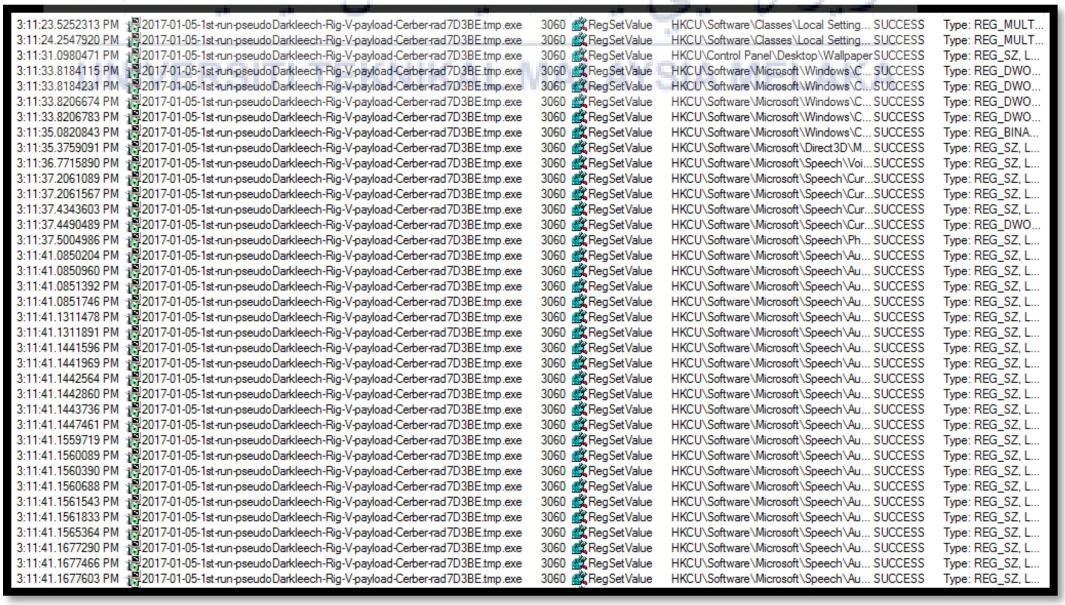
Column	Relation	Value	Action
☑ Operation	is	RegSetValue	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Path	ends with	pagefile.sys	Exclude
☑ Path	ends with	$Mft	Exclude
☑ Path	ends with	$MftMirr	Exclude

OK | Cancel | Apply

```
1012  CreateFile  C:\Windows\System32\wow64cpu.dll  SUCCESS  Desired Access: R...
```

Figure 6.32: Procmon filter RegSetValue

After applying our filter, it shows that 2017-01-05-psuedoDarkleech-Rig-V-sends-Cerber-malware-and-artifacts.exe made several changes to the registry when it executed in **Figure 6.33**.

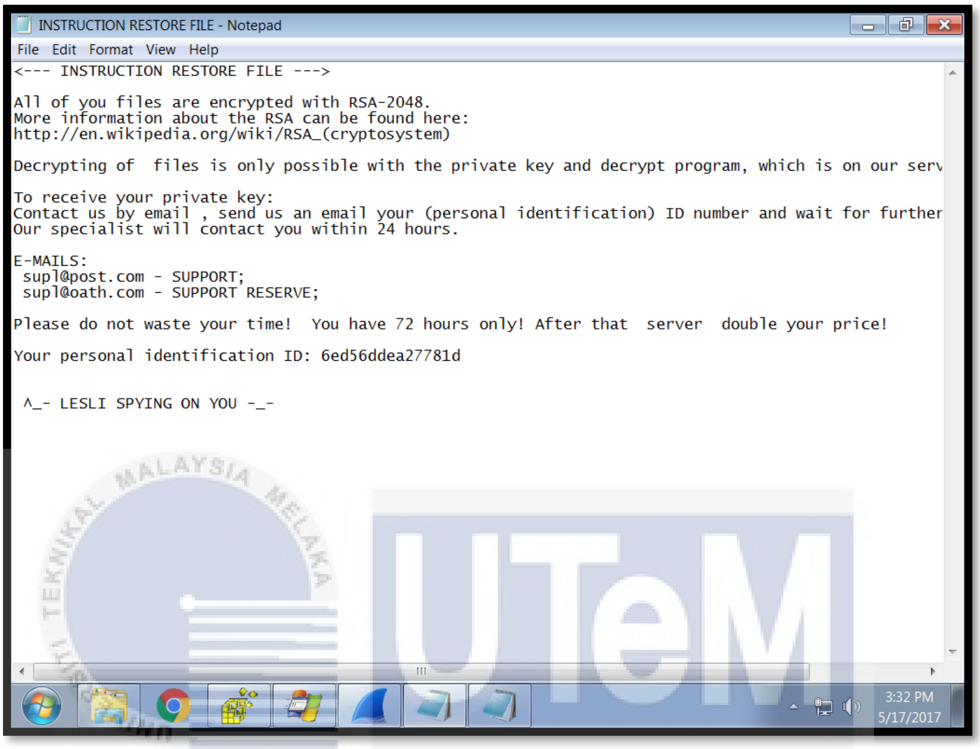


```
3:11:23.5252313 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Classes\Local Setting...  SUCCESS  Type: REG_MULT...
3:11:24.2547920 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Classes\Local Setting...  SUCCESS  Type: REG_MULT...
3:11:31.0980471 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Control Panel\Desktop\Wallpaper  SUCCESS  Type: REG_SZ, L...
3:11:33.8184115 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_DWO...
3:11:33.8184231 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_DWO...
3:11:33.8206674 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_DWO...
3:11:33.8206783 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_DWO...
3:11:35.0820843 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Windows\C...  SUCCESS  Type: REG_BINA...
3:11:35.3759091 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Direct3D\M...  SUCCESS  Type: REG_SZ, L...
3:11:36.7715890 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Voi...  SUCCESS  Type: REG_SZ, L...
3:11:37.2061089 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Cur...  SUCCESS  Type: REG_SZ, L...
3:11:37.2061567 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Cur...  SUCCESS  Type: REG_SZ, L...
3:11:37.4343603 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Cur...  SUCCESS  Type: REG_SZ, L...
3:11:37.4490489 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Cur...  SUCCESS  Type: REG_DWO...
3:11:37.5004986 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Ph...  SUCCESS  Type: REG_SZ, L...
3:11:41.0850204 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.0850960 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.0851392 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.0851746 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1311478 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1311891 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1441596 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1441969 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1442564 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1442860 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1443736 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1447461 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1559719 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1560089 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1560390 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1560688 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1561543 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1561833 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1565364 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1677290 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1677466 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
3:11:41.1677603 PM  2017-01-05-1st-run-pseudoDarkleech-Rig-V-payload-Cerber-rad7D3BE.tmp.exe  3060  RegSetValue  HKCU\Software\Microsoft\Speech\Au...  SUCCESS  Type: REG_SZ, L...
```

Figure 6.33: Procmon filter RegSetValue results

Sample 3: 2017-01-12-EITest-Rig-V-sends-CryptoMix-malware-and-artifacts

The third ransomware sample named Cryptomix has been run in a controlled environment on a virtual machine. Shortly after executing the malware presented with a notification screen as in **Figure 6.34**.

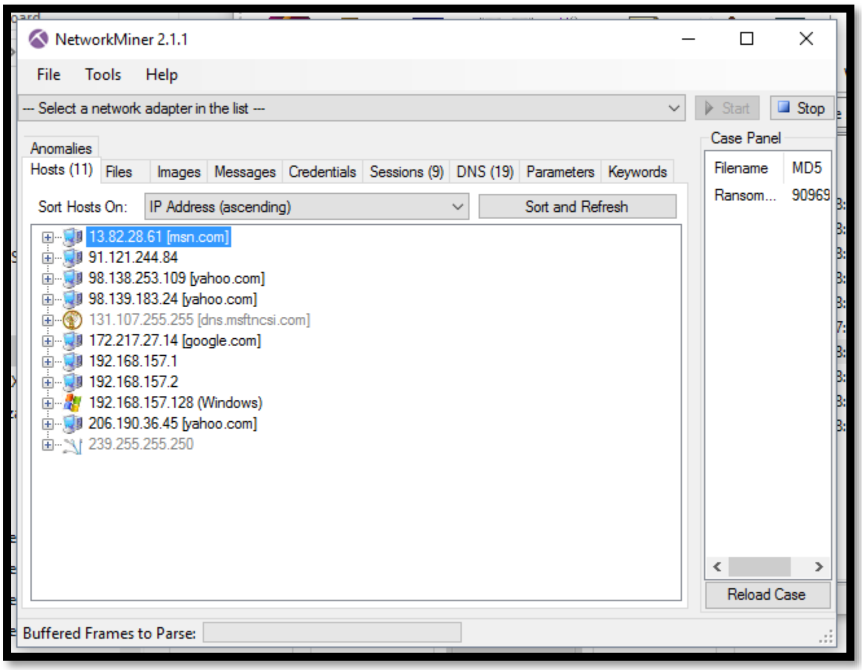

INSTRUCTION RESTORE FILE - Notepad
File Edit Format View Help
3:32 PM
5/17/2017

```
<--- INSTRUCTION RESTORE FILE --->

All of you files are encrypted with RSA-2048.
More information about the RSA can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)

Decrypting of  files is only possible with the private key and decrypt program, which is on our serv

To receive your private key:
Contact us by email , send us an email your (personal identification) ID number and wait for further
Our specialist will contact you within 24 hours.

E-MAILS:
 supl@post.com - SUPPORT;
 supl@oath.com - SUPPORT RESERVE;

Please do not waste your time!  You have 72 hours only! After that  server  double your price!

Your personal identification ID: 6ed56ddea27781d


 ^_- LESLI SPYING ON YOU -_-
```

Figure 6.34: CryptoMix ransomware screen

NetworkMinor Analysis

Examining the third sample, it shows that our machine contacted only 11 different IP addresses and domains as in **Figure 6.35**. If you are new to network forensics, it is a good idea to use a command like ‘whois’ and see who owns each of these IP addresses. There are no suspicious host that were contacted in **Figure 6.35**. Different from the second sample where do not know the name of the domain.



```
13.82.28.61 [msn.com]
91.121.244.84
98.138.253.109 [yahoo.com]
98.139.183.24 [yahoo.com]
131.107.255.255 [dns.msftncsi.com]
172.217.27.14 [google.com]
192.168.157.1
192.168.157.2
192.168.157.128 (Windows)
206.190.36.45 [yahoo.com]
239.255.255.250
```

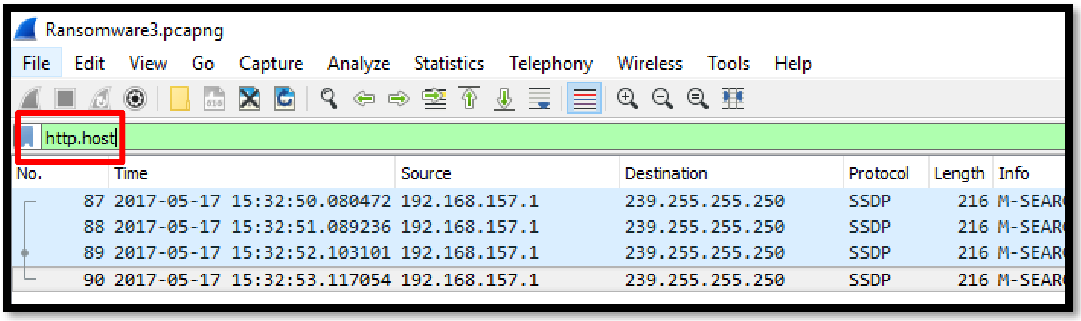
Ransom... 90969

Figure 6.35: NetworkMiner Hosts tab

Typically, if an IP address or domain belong to a well-known company such as Microsoft, Akamai, or Globalsign, it can reasonably ignore these requests. This analysis assume this third ransomware sample do not have to make any outbound connection by continue the further analysis.

Wireshark Analysis

Same as Wireshark Analysis on first and second sample: Locky ransomware. Open the .pcapng file that saved during the execution of CryptoMix ransomware in Wireshark, and search for "**http.host**" as shows in results in **Figure 6.36**.



Ransomware3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.host

```
No.   Time                          Source          Destination      Protocol  Length Info
   87 2017-05-17 15:32:50.080472 192.168.157.1   239.255.255.250  SSDP       216 M-SEAR
   88 2017-05-17 15:32:51.089236 192.168.157.1   239.255.255.250  SSDP       216 M-SEAR
   89 2017-05-17 15:32:52.103101 192.168.157.1   239.255.255.250  SSDP       216 M-SEAR
   90 2017-05-17 15:32:53.117054 192.168.157.1   239.255.255.250  SSDP       216 M-SEAR
```

Figure 6.36: Wireshark http.host filter

After entering in the filter, only the packets matching “**http.host**” are displayed. Next, right click one of the entries and select **Follow - UDP Stream** as in **Figure 6.37**. This will show the raw packet details allowing for further analysis.

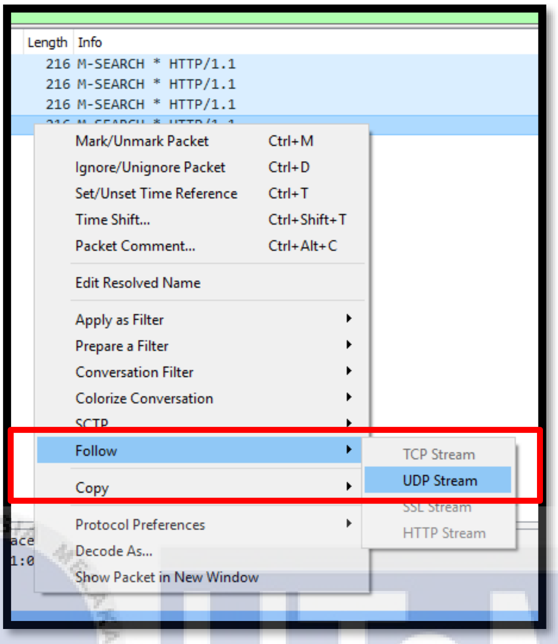
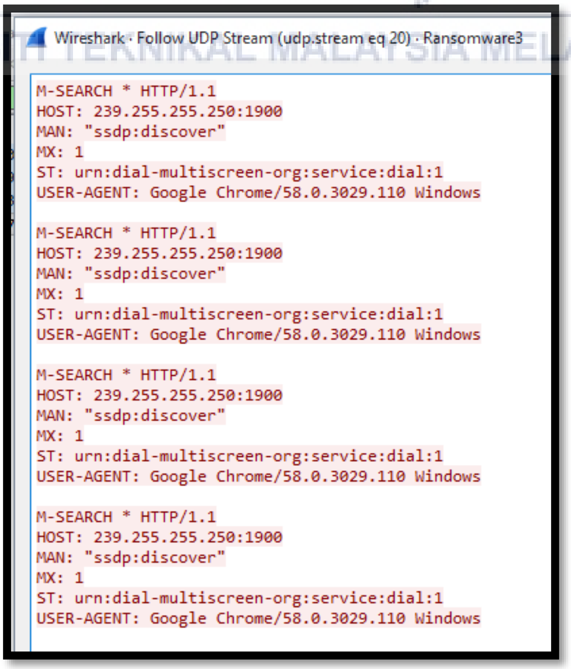


Figure 6.37: Wireshark Follow UDP Stream

From the resulting screen **Figure 6.38**, there are no suspicious information shows up. In **UDP Stream** since it only state about the **Google Chrome.**


Wireshark · Follow UDP Stream (udp.stream eq 20) · Ransomware3

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/58.0.3029.110 Windows
```

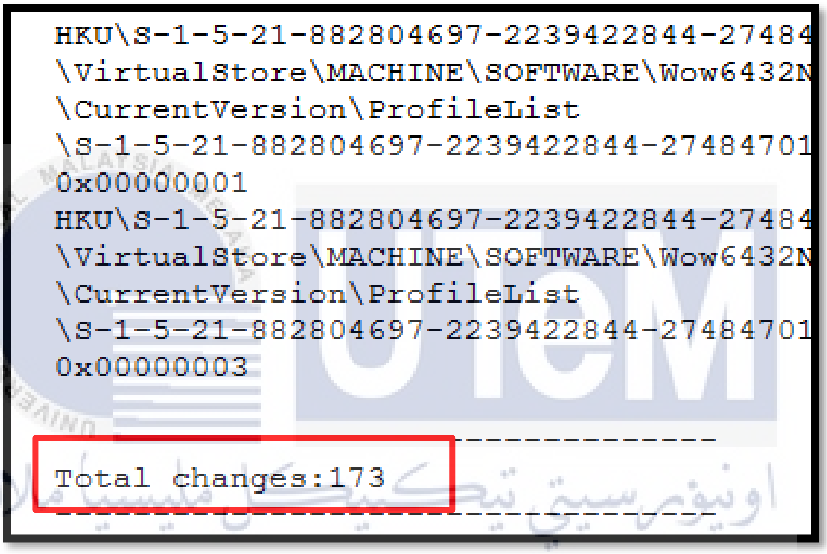
Figure 6.38: Wireshark TCP Stream details

The details of Follow UDP Stream, it shows about the **Host: "239.255.255.250"** that this analysis assume there is no bad outbound network connection occurs. It just belongs **Google Chrome**.

File System Analysis

Regshot findings

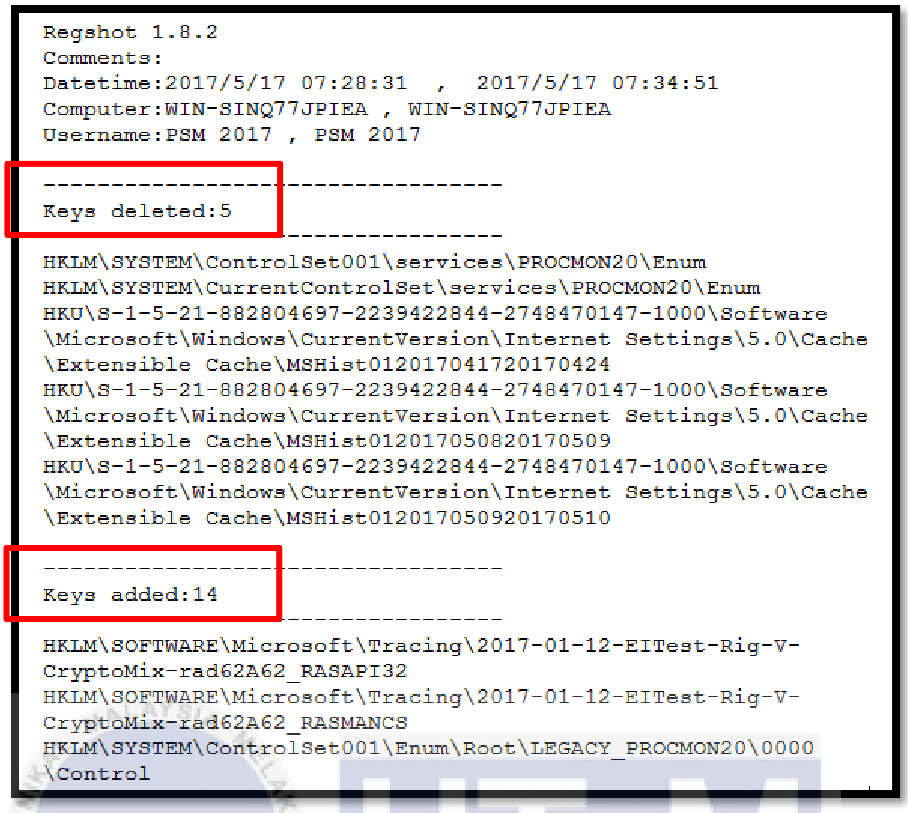
Regshot shows that over 100 changes were made to the Registry from the time the first and second snapshots were taken as in **Figure 6.39** below.



```
HKU\S-1-5-21-882804697-2239422844-27484
\VirtualStore\MACHINE\SOFTWARE\Wow6432N
\CurrentVersion\ProfileList
\S-1-5-21-882804697-2239422844-27484701
0x00000001
HKU\S-1-5-21-882804697-2239422844-27484
\VirtualStore\MACHINE\SOFTWARE\Wow6432N
\CurrentVersion\ProfileList
\S-1-5-21-882804697-2239422844-27484701
0x00000003

-----------------------------------------
Total changes:173
-----------------------------------------
```

Figure 6.39: Regshot total changes

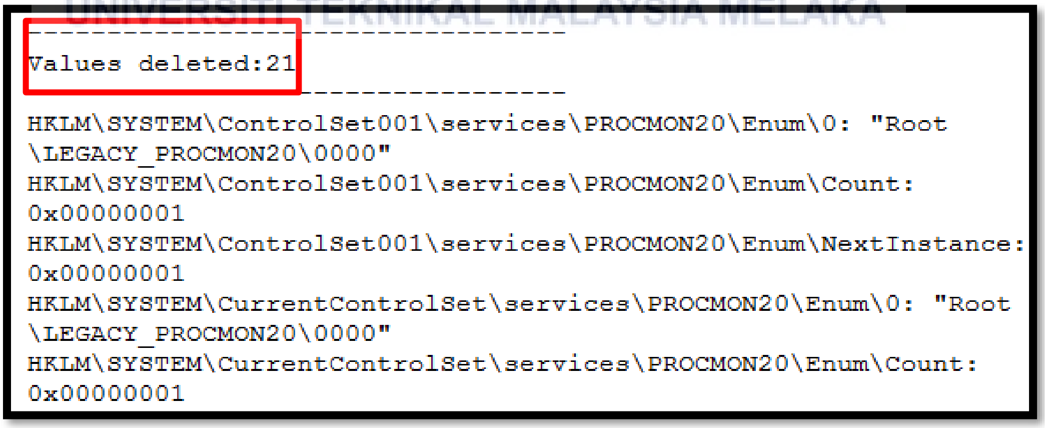
If continue to scroll down the document, we will see that it outlines several different aspects including the following. Remember that the numbers will vary based on the computer as **Total changes:173, Keys deleted: 5, Keys added: 14,** and **Values deleted: 21**. It shows which Registry keys were added or deleted in **Figure 6.40** and which values were deleted **Figure 6.41**.



```
Regshot 1.8.2
Comments:
Datetime:2017/5/17 07:28:31  ,  2017/5/17 07:34:51
Computer:WIN-SINQ77JPIEA , WIN-SINQ77JPIEA
Username:PSM 2017 , PSM 2017

----------------------------------
Keys deleted:5
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017041720170424
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017050820170509
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\Extensible Cache\MSHist012017050920170510

----------------------------------
Keys added:14
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\2017-01-12-EITest-Rig-V-
CryptoMix-rad62A62_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\2017-01-12-EITest-Rig-V-
CryptoMix-rad62A62_RASMANCS
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON20\0000
\Control
```

Figure 6.40: Regshot keys added

In addition to listing the changes, it provides in-depth details about which keys were altered by changing happen in the registry. This can be useful in case the researcher want to manipulate those keys manually.



```
----------------------------------
Values deleted:21
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\0: "Root
\LEGACY_PROCMON20\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\Count:
0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\NextInstance:
0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum\0: "Root
\LEGACY_PROCMON20\0000"
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum\Count:
0x00000001
```

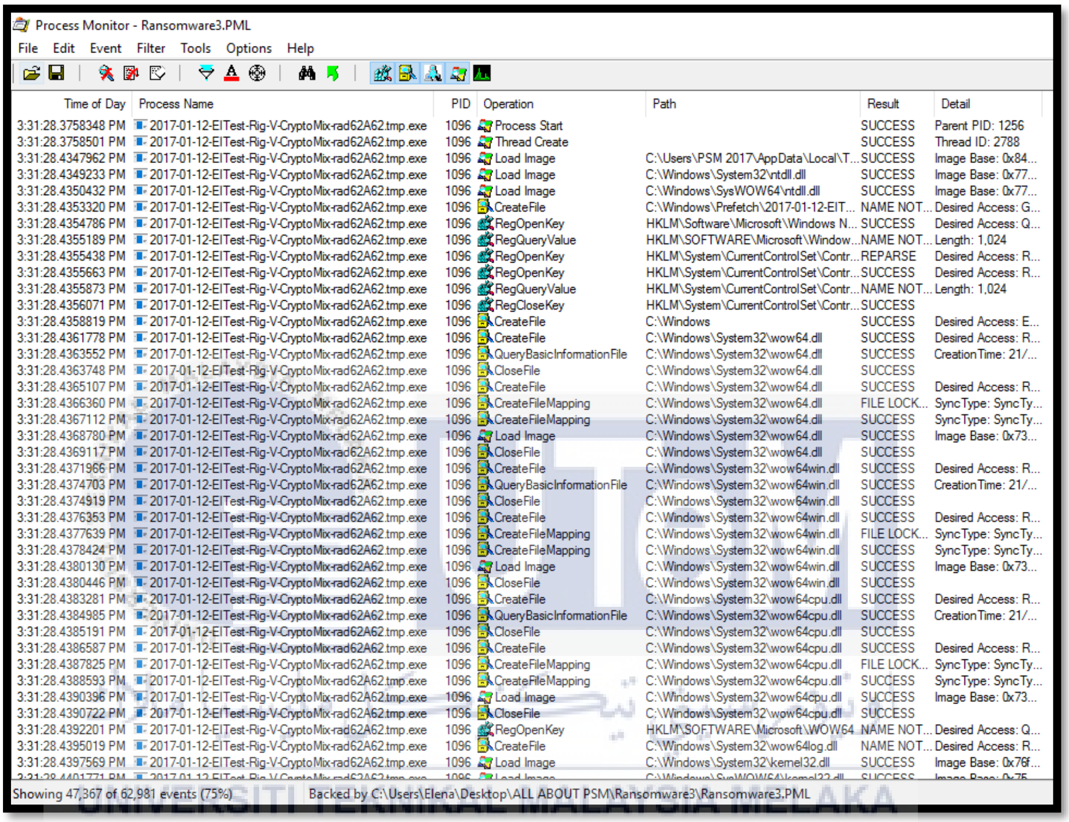
Figure 6.41: Regshot values deleted

Both ransomware not showing much of differences for the registry changes. But two more sample are not reveals yet to see the general changes in registry if this malware infected the computer.

Process Monitor Analysis

Process Monitor also shows changes made to the Registry but it only captures those made by the API call, and may not show everything that occurred.

However, Process Monitor captures a whole lot more information. When viewing the saved output from Process monitor in **Figure 6.42**, the results can be staggering

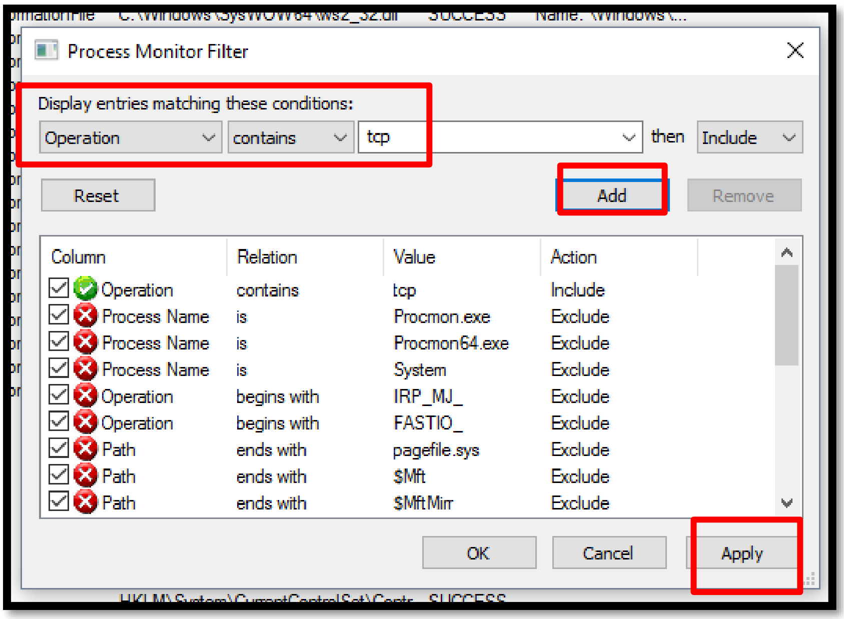

Process Monitor - Ransomware3.PML
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:31:28.3758348 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Process Start		SUCCESS	Parent PID: 1256
3:31:28.3758501 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Thread Create		SUCCESS	Thread ID: 2788
3:31:28.4347962 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Load Image	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Image Base: 0x84...
3:31:28.4349233 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77...
3:31:28.4350432 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77...
3:31:28.4353320 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\Prefetch\2017-01-12-EIT...	NAME NOT...	Desired Access: G...
3:31:28.4354786 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
3:31:28.4355189 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT...	Length: 1,024
3:31:28.4355438 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
3:31:28.4355663 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
3:31:28.4355873 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT...	Length: 1,024
3:31:28.4356071 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
3:31:28.4358819 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
3:31:28.4361778 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
3:31:28.4363552 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	QueryBasicInformationFile	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 21/...
3:31:28.4363748 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
3:31:28.4365107 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
3:31:28.4366360 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFileMapping	C:\Windows\System32\wow64.dll	FILE LOCK...	SyncType: SyncTy...
3:31:28.4367112 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFileMapping	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
3:31:28.4368780 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73...
3:31:28.4369117 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
3:31:28.4371966 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
3:31:28.4374703 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	QueryBasicInformationFile	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 21/...
3:31:28.4374919 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
3:31:28.4376353 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
3:31:28.4377639 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFileMapping	C:\Windows\System32\wow64win.dll	FILE LOCK...	SyncType: SyncTy...
3:31:28.4378424 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFileMapping	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
3:31:28.4380130 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x73...
3:31:28.4380446 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
3:31:28.4383281 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
3:31:28.4384985 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	QueryBasicInformationFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 21/...
3:31:28.4385191 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
3:31:28.4386587 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
3:31:28.4387825 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	FILE LOCK...	SyncType: SyncTy...
3:31:28.4388593 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
3:31:28.4390396 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73...
3:31:28.4390722 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
3:31:28.4392201 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT...	Desired Access: Q...
3:31:28.4395019 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT...	Desired Access: R...
3:31:28.4397569 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76f...

Showing 47,367 of 62,981 events (75%)　Backed by C:\Users\Elena\Desktop\ALL ABOUT PSM\Ransomware3\Ransomware3.PML

Figure 6.42: Process Monitor initial screen

To use a filter, click on the Filter at the top of the screen and then select Operation in the drop-down box on the left. In the next box, select Contains and, in the final field, enter “tcp” **Figure 6.42**. This will display any TCP connections that were attempted by the malware. The results can differ from what Wireshark packet capture detected.



Process Monitor Filter

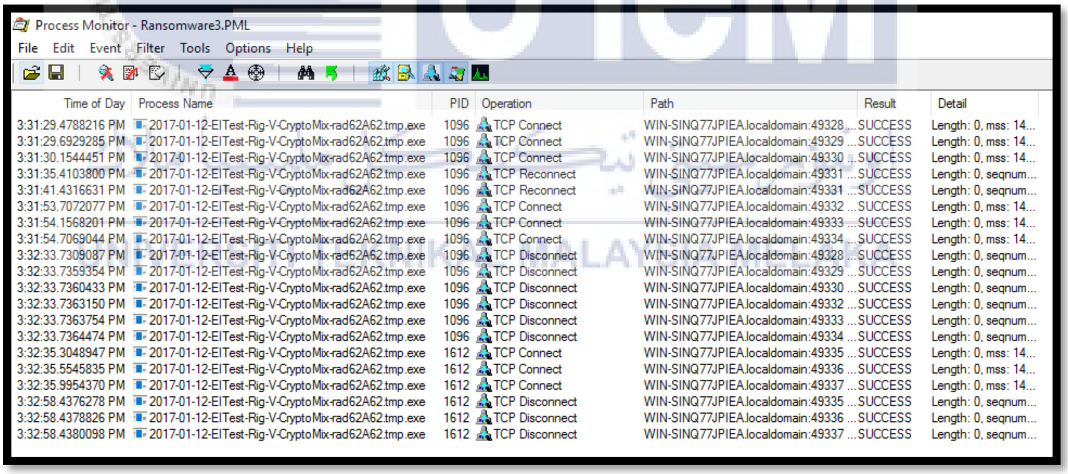
Display entries matching these conditions:

Operation | contains | tcp | then Include

Column	Relation	Value	Action
☑ Operation	contains	tcp	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Path	ends with	pagefile.sys	Exclude
☑ Path	ends with	$Mft	Exclude
☑ Path	ends with	$MftMirr	Exclude

Figure 6.43: Procmon filter TCP

After filtering, the results of **Operation** contain **TCP** in **Figure 6.44** do not showed up, this is means no TCP connection when this sample infected the computer.

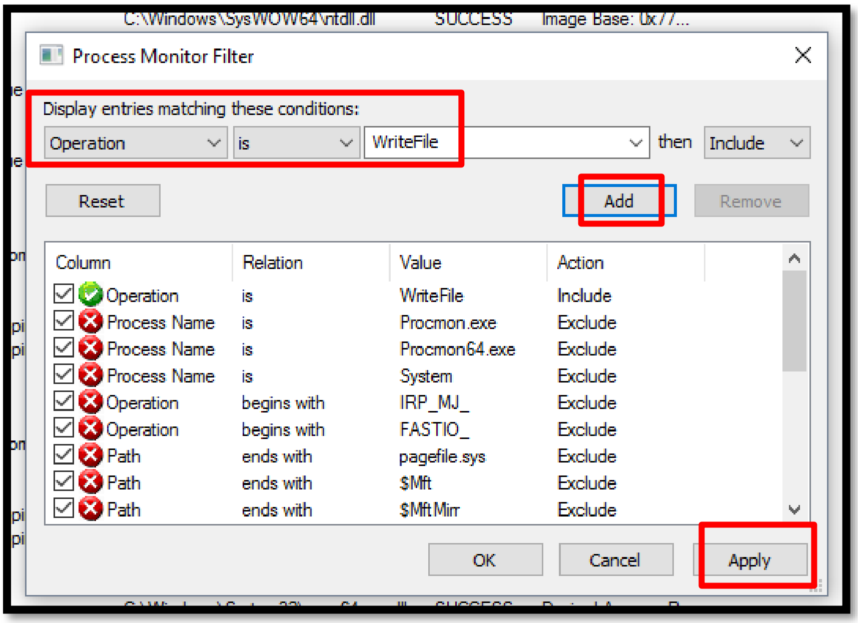


Process Monitor - Ransomware3.PML

Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:31:29.4788216 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Connect	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 0, mss: 14...
3:31:29.6929285 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Connect	WIN-SINQ77JPIEA.localdomain:49329 ...	SUCCESS	Length: 0, mss: 14...
3:31:30.1544451 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Connect	WIN-SINQ77JPIEA.localdomain:49330 ...	SUCCESS	Length: 0, mss: 14...
3:31:35.4103800 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49331 ...	SUCCESS	Length: 0, seqnum...
3:31:41.4316631 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Reconnect	WIN-SINQ77JPIEA.localdomain:49331 ...	SUCCESS	Length: 0, seqnum...
3:31:53.7072077 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Connect	WIN-SINQ77JPIEA.localdomain:49332 ...	SUCCESS	Length: 0, mss: 14...
3:31:54.1568201 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Connect	WIN-SINQ77JPIEA.localdomain:49333 ...	SUCCESS	Length: 0, mss: 14...
3:31:54.7069044 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Connect	WIN-SINQ77JPIEA.localdomain:49334 ...	SUCCESS	Length: 0, mss: 14...
3:32:33.7309087 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49328 ...	SUCCESS	Length: 0, seqnum...
3:32:33.7359354 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49329 ...	SUCCESS	Length: 0, seqnum...
3:32:33.7360433 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49330 ...	SUCCESS	Length: 0, seqnum...
3:32:33.7363150 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49332 ...	SUCCESS	Length: 0, seqnum...
3:32:33.7363754 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49333 ...	SUCCESS	Length: 0, seqnum...
3:32:33.7364474 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49334 ...	SUCCESS	Length: 0, seqnum...
3:32:35.3048947 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1612	TCP Connect	WIN-SINQ77JPIEA.localdomain:49335 ...	SUCCESS	Length: 0, mss: 14...
3:32:35.5545835 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1612	TCP Connect	WIN-SINQ77JPIEA.localdomain:49336 ...	SUCCESS	Length: 0, mss: 14...
3:32:35.9954370 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1612	TCP Connect	WIN-SINQ77JPIEA.localdomain:49337 ...	SUCCESS	Length: 0, mss: 14...
3:32:58.4376278 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1612	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49335 ...	SUCCESS	Length: 0, seqnum...
3:32:58.4378826 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1612	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49336 ...	SUCCESS	Length: 0, seqnum...
3:32:58.4380098 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1612	TCP Disconnect	WIN-SINQ77JPIEA.localdomain:49337 ...	SUCCESS	Length: 0, seqnum...

Figure 6.44: Procmon filter results

Process Monitor can also use a display filter to show any files that were written to the drive by the malware. It will filter for any Operation matching “WriteFile” to display this in **Figure 6.45**. Knowing what files are created on the system can help us identify additional malware that was downloaded, as well as help build out a list of identifiers can search for later.



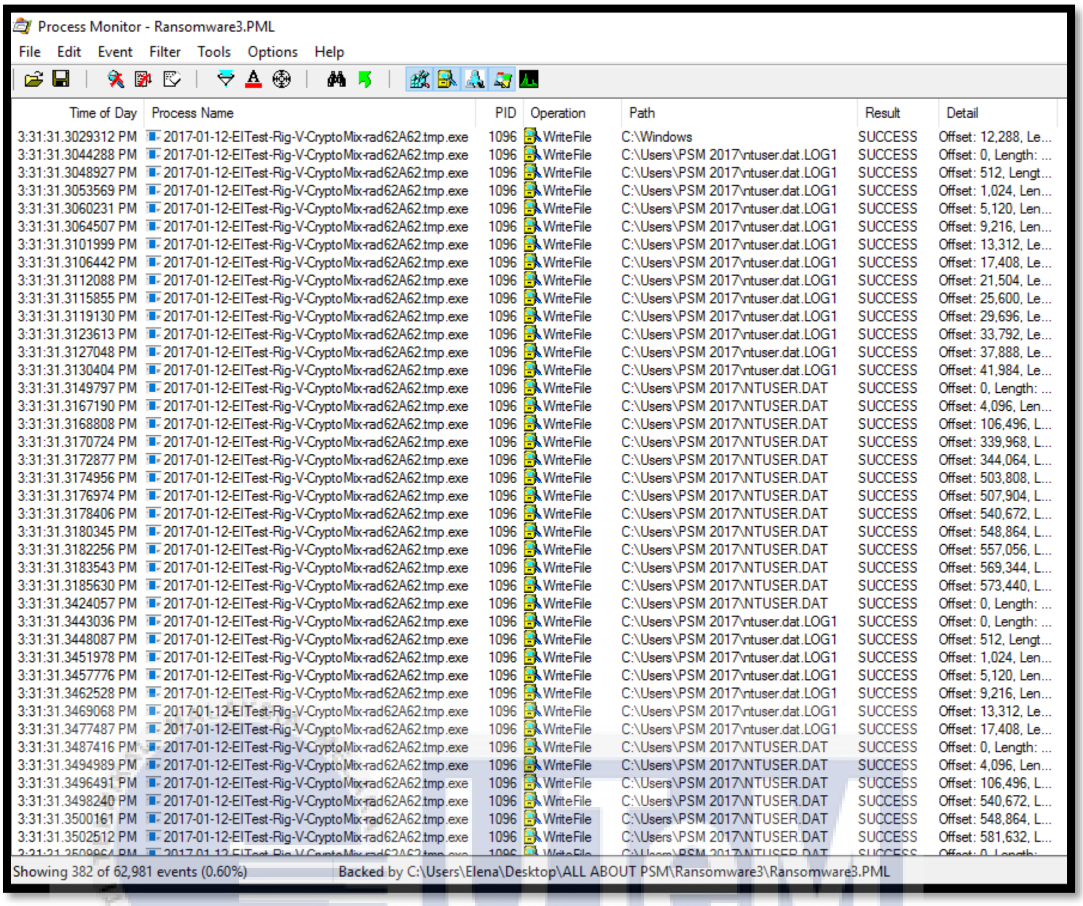
Display entries matching these conditions:

Operation is WriteFile then Include

Column	Relation	Value	Action
☑ ✓ Operation	is	WriteFile	Include
☑ ✗ Process Name	is	Procmon.exe	Exclude
☑ ✗ Process Name	is	Procmon64.exe	Exclude
☑ ✗ Process Name	is	System	Exclude
☑ ✗ Operation	begins with	IRP_MJ_	Exclude
☑ ✗ Operation	begins with	FASTIO_	Exclude
☑ ✗ Path	ends with	pagefile.sys	Exclude
☑ ✗ Path	ends with	$Mft	Exclude
☑ ✗ Path	ends with	$MftMirr	Exclude

Figure 6.45: Procmon filter Writefile

From these filtered results in **Figure 6.46**, it shows that our malware sample, 2017-01-12-EITest-Rig-V-sends-CryptoMix-malware-and-artifacts.exe, created several files on the system.



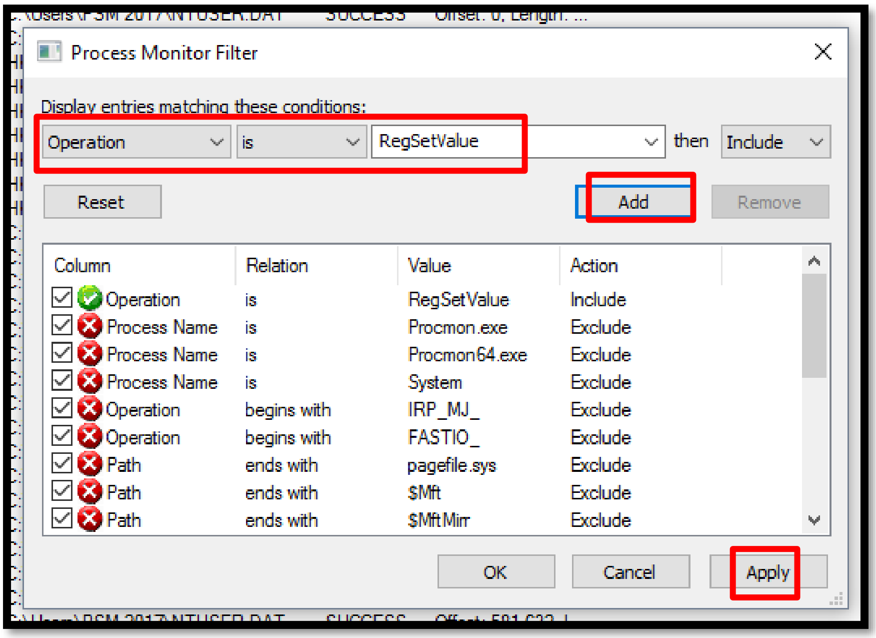
Process Monitor - Ransomware3.PML

Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:31:31.3029312 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Windows	SUCCESS	Offset: 12,288, Le...
3:31:31.3044288 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 0, Length: ...
3:31:31.3048927 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 512, Lengt...
3:31:31.3053569 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 1,024, Len...
3:31:31.3060231 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 5,120, Len...
3:31:31.3064507 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 9,216, Len...
3:31:31.3101999 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 13,312, Le...
3:31:31.3106442 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 17,408, Le...
3:31:31.3112088 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 21,504, Le...
3:31:31.3115855 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 25,600, Le...
3:31:31.3119130 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 29,696, Le...
3:31:31.3123613 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 33,792, Le...
3:31:31.3127048 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 37,888, Le...
3:31:31.3130404 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 41,984, Le...
3:31:31.3149797 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 0, Length: ...
3:31:31.3167190 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 4,096, Len...
3:31:31.3168808 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 106,496, L...
3:31:31.3170724 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 339,968, L...
3:31:31.3172877 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 344,064, L...
3:31:31.3174956 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 503,808, L...
3:31:31.3176974 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 507,904, L...
3:31:31.3178406 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 540,672, L...
3:31:31.3180345 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 548,864, L...
3:31:31.3182256 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 557,056, L...
3:31:31.3183543 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 569,344, L...
3:31:31.3185630 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 573,440, L...
3:31:31.3424057 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 0, Length: ...
3:31:31.3443036 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 0, Length: ...
3:31:31.3448087 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 512, Lengt...
3:31:31.3451978 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 1,024, Len...
3:31:31.3457776 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 5,120, Len...
3:31:31.3462528 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 9,216, Len...
3:31:31.3469068 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 13,312, Le...
3:31:31.3477487 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\ntuser.dat.LOG1	SUCCESS	Offset: 17,408, Le...
3:31:31.3487416 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 0, Length: ...
3:31:31.3494989 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 4,096, Len...
3:31:31.3496491 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 106,496, L...
3:31:31.3498240 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 540,672, L...
3:31:31.3500161 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 548,864, L...
3:31:31.3502512 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 581,632, L...
3:31:31.3509964 PM	2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe	1096	WriteFile	C:\Users\PSM 2017\NTUSER.DAT	SUCCESS	Offset: 0, Length:

Showing 382 of 62,981 events (0.60%) Backed by C:\Users\Elena\Desktop\ALL ABOUT PSM\Ransomware3\Ransomware3.PML

Figure 6.46: Procmon filter WriteFile results

Procmon can also display any changes 2017-01-12-EITest-Rig-V-sends-CryptoMix-malware-and-artifacts.exe made to the Windows Registry. For this, it will look for the value named RegSetValue in **Figure 6.47** below.



Process Monitor Filter

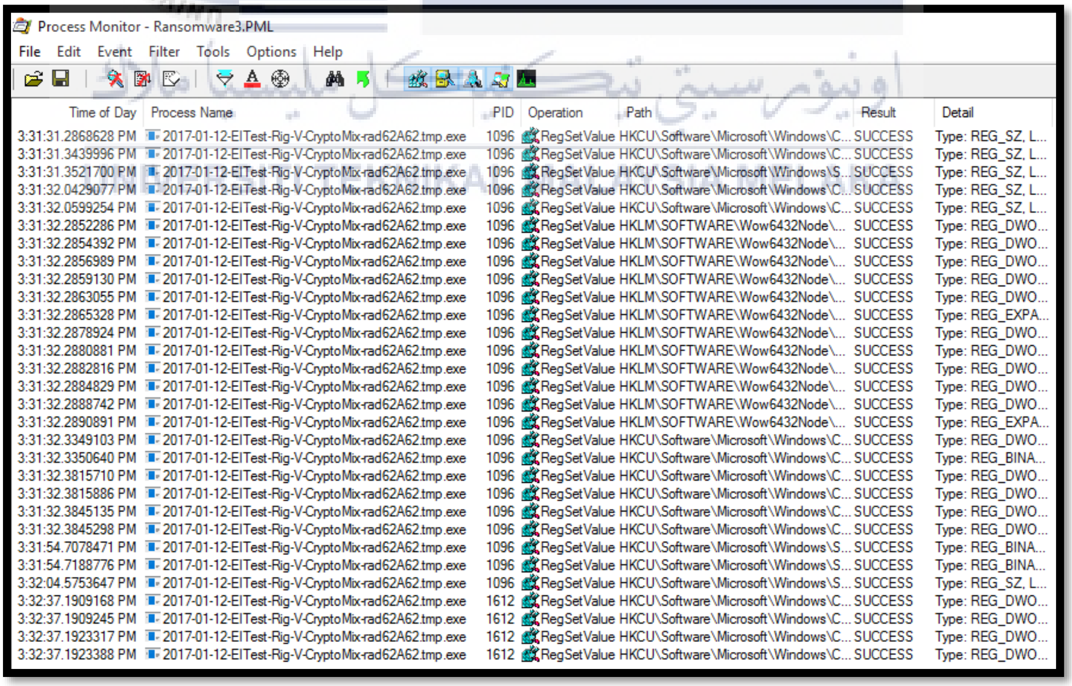
Display entries matching these conditions:

Operation | is | RegSetValue | then | Include

Column	Relation	Value	Action
☑ Operation	is	RegSetValue	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Path	ends with	pagefile.sys	Exclude
☑ Path	ends with	$Mft	Exclude
☑ Path	ends with	$MftMirr	Exclude

Figure 6.47: Procmon filter RegSetValue

After applying our filter, it shows that 2017-01-12-EITest-Rig-V-sends-CryptoMix-malware-and-artifacts.exe made several changes to the registry when it executed in **Figure 6.48**.



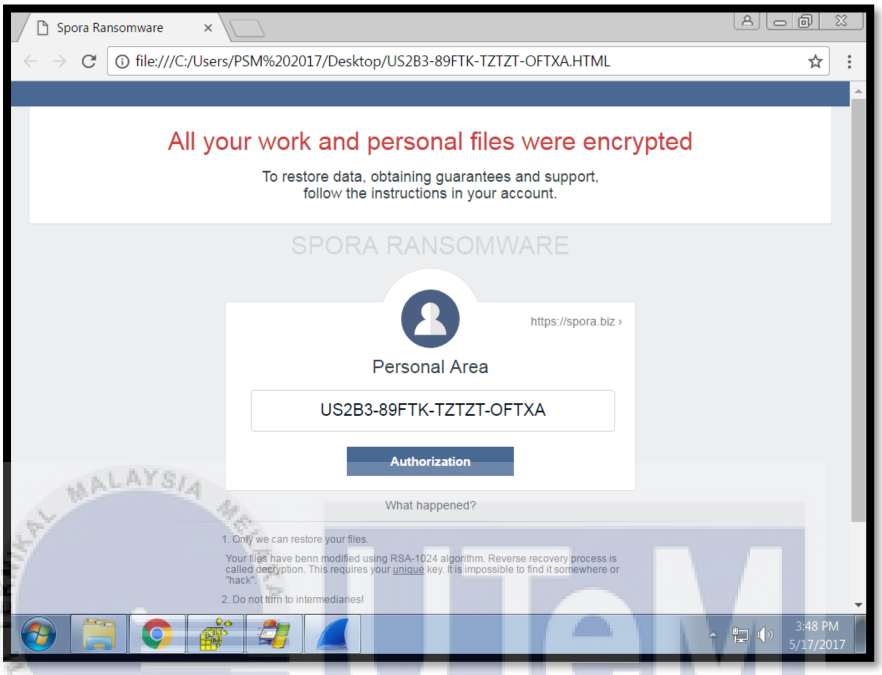
Process Monitor - Ransomware3.PML

```
     Time of Day  Process Name                                         PID  Operation   Path                                      Result   Detail
3:31:31.2868628 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_SZ, L...
3:31:31.3439996 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_SZ, L...
3:31:31.3521700 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\S... SUCCESS  Type: REG_SZ, L...
3:31:32.0429077 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_SZ, L...
3:31:32.0599254 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_SZ, L...
3:31:32.2852286 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2854392 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2856989 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2859130 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2863055 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2865328 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_EXPA...
3:31:32.2878924 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2880881 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2882816 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2884829 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2888742 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_DWO...
3:31:32.2890891 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKLM\SOFTWARE\Wow6432Node\...  SUCCESS  Type: REG_EXPA...
3:31:32.3349103 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:31:32.3350640 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_BINA...
3:31:32.3815710 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:31:32.3815886 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:31:32.3845135 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:31:32.3845298 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:31:54.7078471 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\S... SUCCESS  Type: REG_BINA...
3:31:54.7188776 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\S... SUCCESS  Type: REG_BINA...
3:32:04.5753647 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1096 RegSetValue HKCU\Software\Microsoft\Windows\S... SUCCESS  Type: REG_SZ, L...
3:32:37.1909168 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1612 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:32:37.1909245 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1612 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:32:37.1923317 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1612 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
3:32:37.1923388 PM 2017-01-12-EITest-Rig-V-CryptoMix-rad62A62.tmp.exe  1612 RegSetValue HKCU\Software\Microsoft\Windows\C... SUCCESS  Type: REG_DWO...
```

Figure 6.48: Procmon filter RegSetValue results

Sample 4: 2017-01-30-EITest-fake-Chrome-popup-sends-Spora-malware-and-artifacts

The last sample of ransomware named Spora ransomware in a controlled environment on a virtual machine. Shortly after executing the malware I was presented with a Chrome Web Browser screen as shown in **Figure 6.49**.


Spora Ransomware
file:///C:/Users/PSM%202017/Desktop/US2B3-89FTK-TZTZT-OFTXA.HTML

All your work and personal files were encrypted

To restore data, obtaining guarantees and support,
follow the instructions in your account.

SPORA RANSOMWARE

https://spora.biz ›

Personal Area

US2B3-89FTK-TZTZT-OFTXA

Authorization

What happened?

1. Only we can restore your files.

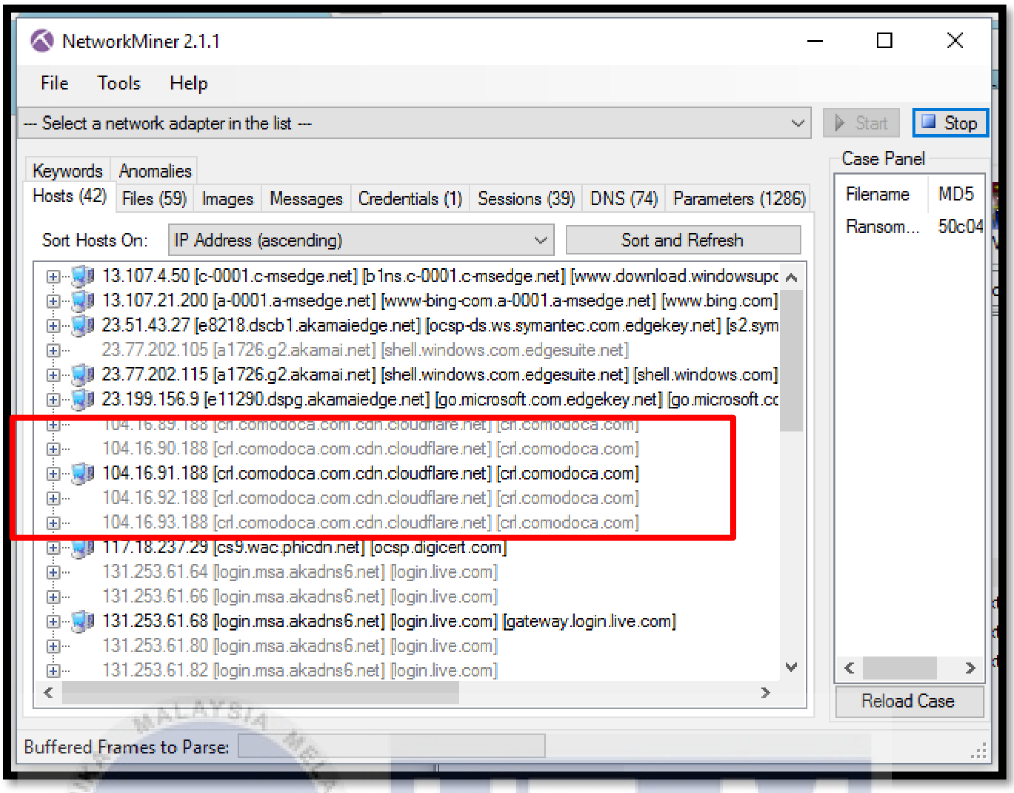
Your files have benn modified using RSA-1024 algorithm. Reverse recovery process is called decryption. This requires your unique key. It is impossible to find it somewhere or "hack".

2. Do not turn to intermediaries!

Figure 6.49: Spora ransomware screen

NetworkMinor Analysis

Examining the last sample, it shows that our machine contacted over 40 different IP addresses and domains as in **Figure 6.50**. If you are new to network forensics, it is a good idea to use a command like 'whois' and see who owns each of these IP addresses.



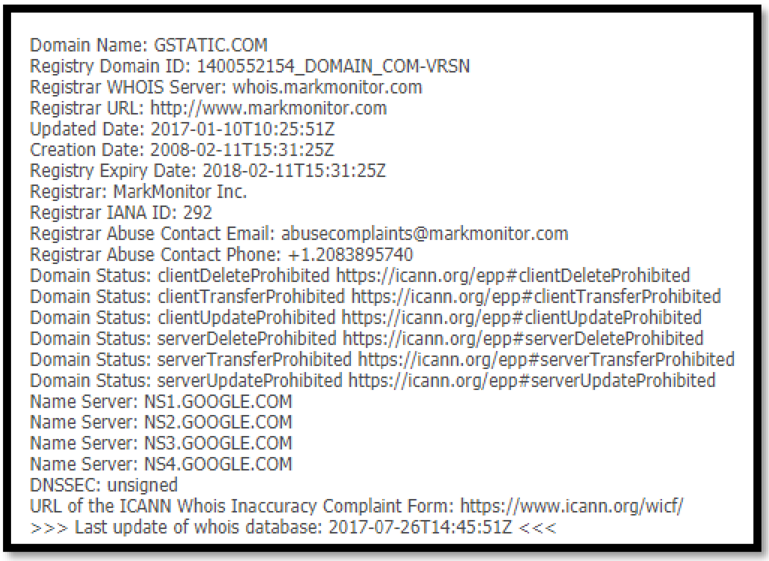
Sort Hosts On: IP Address (ascending)

```
13.107.4.50 [c-0001.c-msedge.net] [b1ns.c-0001.c-msedge.net] [www.download.windowsupc
13.107.21.200 [a-0001.a-msedge.net] [www-bing-com.a-0001.a-msedge.net] [www.bing.com]
23.51.43.27 [e8218.dscb1.akamaiedge.net] [ocsp-ds.ws.symantec.com.edgekey.net] [s2.sym
23.77.202.105 [a1726.g2.akamai.net] [shell.windows.com.edgesuite.net]
23.77.202.115 [a1726.g2.akamai.net] [shell.windows.com.edgesuite.net] [shell.windows.com]
23.199.156.9 [e11290.dspg.akamaiedge.net] [go.microsoft.com.edgekey.net] [go.microsoft.cc
104.16.89.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.90.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.91.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.92.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
104.16.93.188 [crl.comodoca.com.cdn.cloudflare.net] [crl.comodoca.com]
117.18.237.29 [cs9.wac.phicdn.net] [ocsp.digicert.com]
131.253.61.64 [login.msa.akadns6.net] [login.live.com]
131.253.61.66 [login.msa.akadns6.net] [login.live.com]
131.253.61.68 [login.msa.akadns6.net] [login.live.com] [gateway.login.live.com]
131.253.61.80 [login.msa.akadns6.net] [login.live.com]
131.253.61.82 [login.msa.akadns6.net] [login.live.com]
```

Filename	MD5
Ransom...	50c04

Figure 6.50: NetworkMiner Hosts tab

The **Figure 6.50** above show a suspicious host: **crl.comodoca.com.cdn.cloudflare.net** that used as baselined for the further analysis that is Wireshark Analysis. Typically, if an IP address or domain belong to a well-known company such as Microsoft, Akamai, or Globalsign, it can reasonably ignore these requests. For example, if it run the ‘whois’ command on the gstatic.com domain, it shows that it is owned by Google **Figure 6.51**.



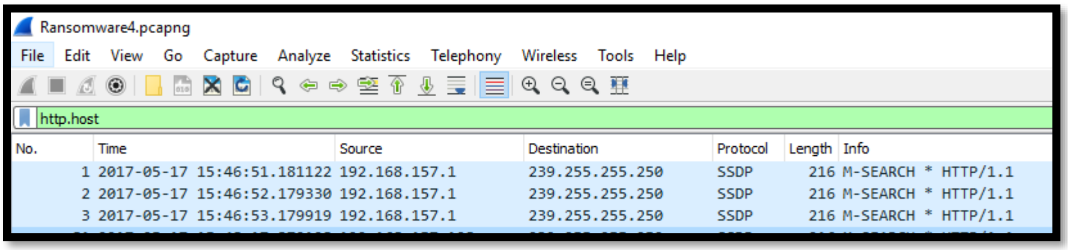
```
Domain Name: GSTATIC.COM
Registry Domain ID: 1400552154_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2017-01-10T10:25:51Z
Creation Date: 2008-02-11T15:31:25Z
Registry Expiry Date: 2018-02-11T15:31:25Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2017-07-26T14:45:51Z <<<
```

Figure 6.51: gstatic.com belongs to Google

Figure 6.51 above shows the results from 'whois' with IP Address **104.16.93.188** where the domain name belongs to **GSTATIC.COM** which it owned by **Google**. **crl.comodoca.com.cdn.cloudflare.net** in **Figure 6.50** is used as baselined for the further analysis in Wireshark Analysis.

Wireshark Analysis

Same case as sample 1: Cerber ransomware, **crl.comodoca.com.cdn.cloudflare.net** domain searched in Wireshark as identified in NetworkMiner analysis.

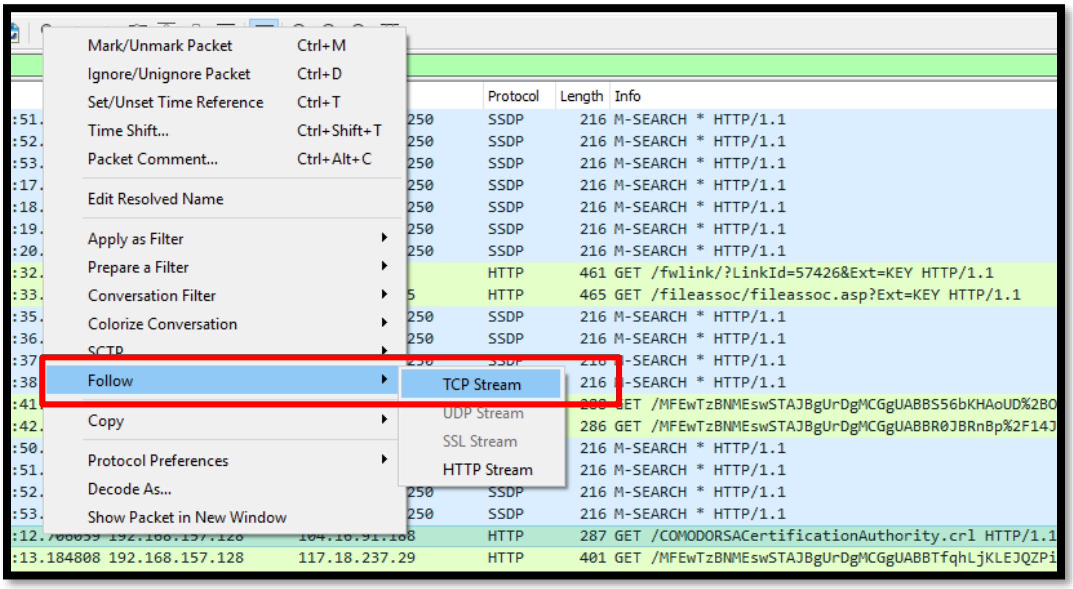


http.host

```
No.   Time                        Source          Destination      Protocol  Length Info
    1 2017-05-17 15:46:51.181122 192.168.157.1   239.255.255.250  SSDP       216 M-SEARCH * HTTP/1.1
    2 2017-05-17 15:46:52.179330 192.168.157.1   239.255.255.250  SSDP       216 M-SEARCH * HTTP/1.1
    3 2017-05-17 15:46:53.179919 192.168.157.1   239.255.255.250  SSDP       216 M-SEARCH * HTTP/1.1
```

Figure 6.52: Wireshark http.host filter

After entering in the filter, only the packets matching "**http.host**" are displayed. Next, right click one of the entries and select **Follow - TCP Stream** as in **Figure 6.53**. This will show the raw packet details allowing for further analysis.

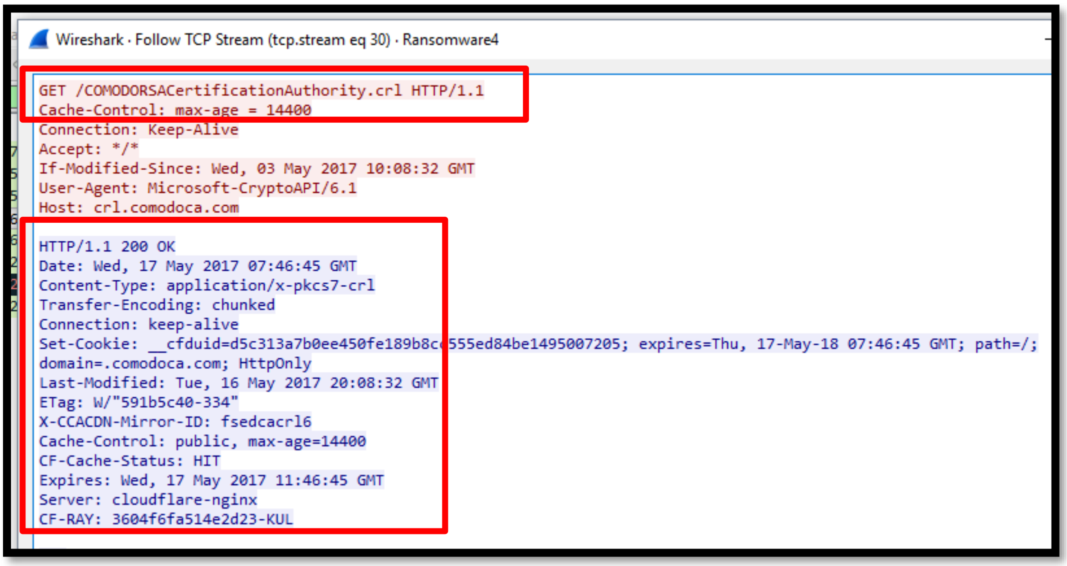


```
                                          Protocol  Length Info
:51.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:52.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:53.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:17.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:18.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:19.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:20.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:32.                                      HTTP         461 GET /fwlink/?LinkId=57426&Ext=KEY HTTP/1.1
:33.                             5        HTTP         465 GET /fileassoc/fileassoc.asp?Ext=KEY HTTP/1.1
:35.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:36.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:37                                                         -SEARCH * HTTP/1.1
:38                                                    216  -SEARCH * HTTP/1.1
:41                                                         ET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BO
:42.                                                   286 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR0JBRnBp%2F14J
:50.                                                   216 M-SEARCH * HTTP/1.1
:51.                                                   216 M-SEARCH * HTTP/1.1
:52.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:53.                             250      SSDP         216 M-SEARCH * HTTP/1.1
:12.                                      HTTP         287 GET /COMODORSACertificationAuthority.crl HTTP/1.1
:13.184808 192.168.157.128  117.18.237.29  HTTP        401 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPi
```

Figure 6.53: Wireshark Follow TCP Stream

From the resulting screen **Figure 6.54**, several interesting things shows up. Starting at the top, it shows that this was an **HTTP GET request**. This means that our machine made a request (GET) to the remote site crl.comodoca.com.cdn.cloudflare.net. The remote site responded with an **HTTP/1.1 200 OK**, which shows that the server accepted our request.

This analysis is also presented with the date of the request and information about the server. It shows the version of PHP that is running, as well as an indication of where the site is hosted. Our example shows **Cloudflare**, which is a content delivery network in the United States.

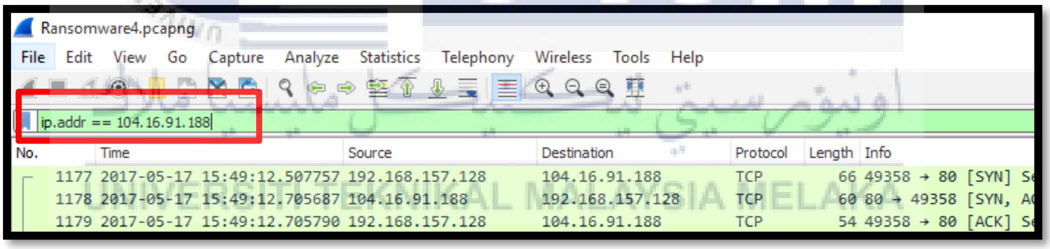


Wireshark · Follow TCP Stream (tcp.stream eq 30) · Ransomware4

```
GET /COMODORSACertificationAuthority.crl HTTP/1.1
Cache-Control: max-age = 14400
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Wed, 03 May 2017 10:08:32 GMT
User-Agent: Microsoft-CryptoAPI/6.1
Host: crl.comodoca.com

HTTP/1.1 200 OK
Date: Wed, 17 May 2017 07:46:45 GMT
Content-Type: application/x-pkcs7-crl
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=d5c313a7b0ee450fe189b8c555ed84be1495007205; expires=Thu, 17-May-18 07:46:45 GMT; path=/;
domain=.comodoca.com; HttpOnly
Last-Modified: Tue, 16 May 2017 20:08:32 GMT
ETag: W/"591b5c40-334"
X-CCACDN-Mirror-ID: fsedcacrl6
Cache-Control: public, max-age=14400
CF-Cache-Status: HIT
Expires: Wed, 17 May 2017 11:46:45 GMT
Server: cloudflare-nginx
CF-RAY: 3604f6fa514e2d23-KUL
```

Figure 6.54: Wireshark TCP Stream details

Like the **http.host** filter, this Wireshark can also display activity from a specific IP address with the **ip.addr** filter in **Figure 6.55**. In this case, put in the filter of **ip.addr == 104.16.91.188**. This IP address is the one identified in NetworkMiner that belongs to the crl.comodoca.com.cdn.cloudflare.net.



ip.addr == 104.16.91.188

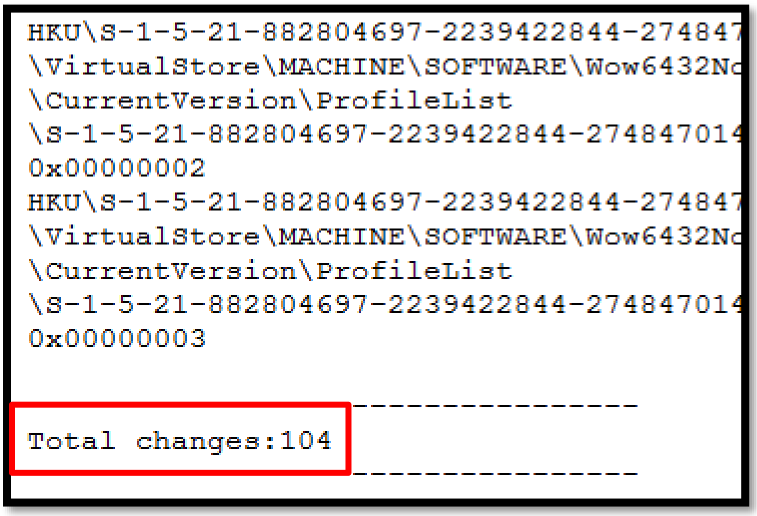
```
No.   Time                       Source            Destination       Protocol  Length  Info
 1177 2017-05-17 15:49:12.507757 192.168.157.128   104.16.91.188     TCP       66 49358 → 80 [SYN] Se
 1178 2017-05-17 15:49:12.705687 104.16.91.188     192.168.157.128   TCP       60 80 → 49358 [SYN, AC
 1179 2017-05-17 15:49:12.705790 192.168.157.128   104.16.91.188     TCP       54 49358 → 80 [ACK] Se
```

Figure 6.55: Wireshark TCP Stream details

File System Analysis

Regshot findings

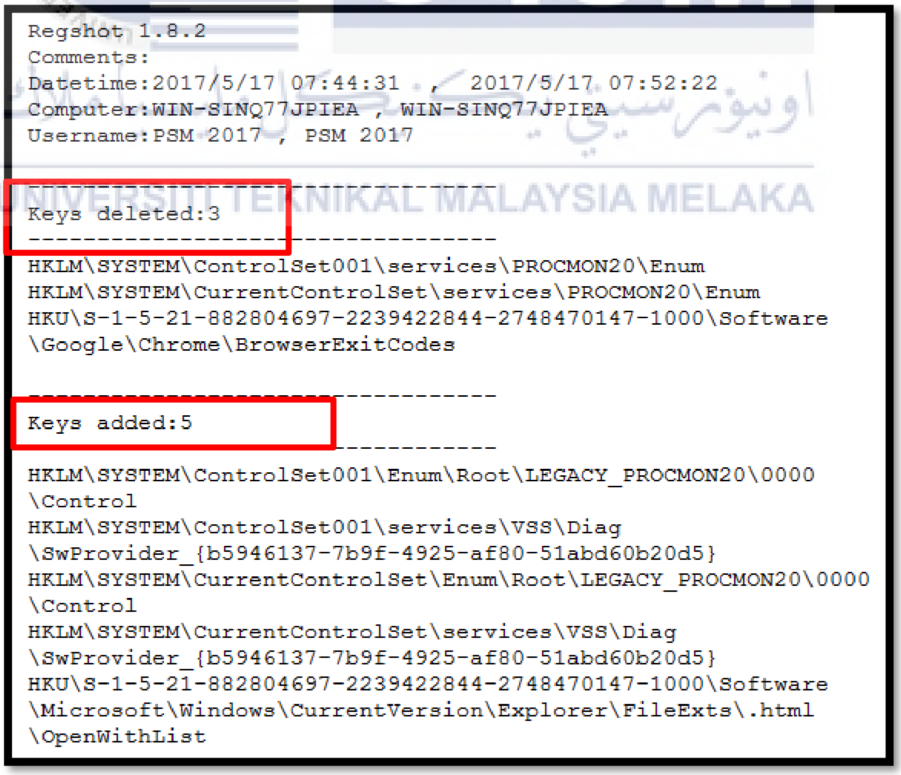
Regshot shows that over 100 changes were made to the Registry from the time the first and second snapshots were taken as in **Figure 6.56** below.



```
HKU\S-1-5-21-882804697-2239422844-274847
\VirtualStore\MACHINE\SOFTWARE\Wow6432Nc
\CurrentVersion\ProfileList
\S-1-5-21-882804697-2239422844-274847014
0x00000002
HKU\S-1-5-21-882804697-2239422844-274847
\VirtualStore\MACHINE\SOFTWARE\Wow6432Nc
\CurrentVersion\ProfileList
\S-1-5-21-882804697-2239422844-274847014
0x00000003

----------------------------------
Total changes:104
----------------------------------
```

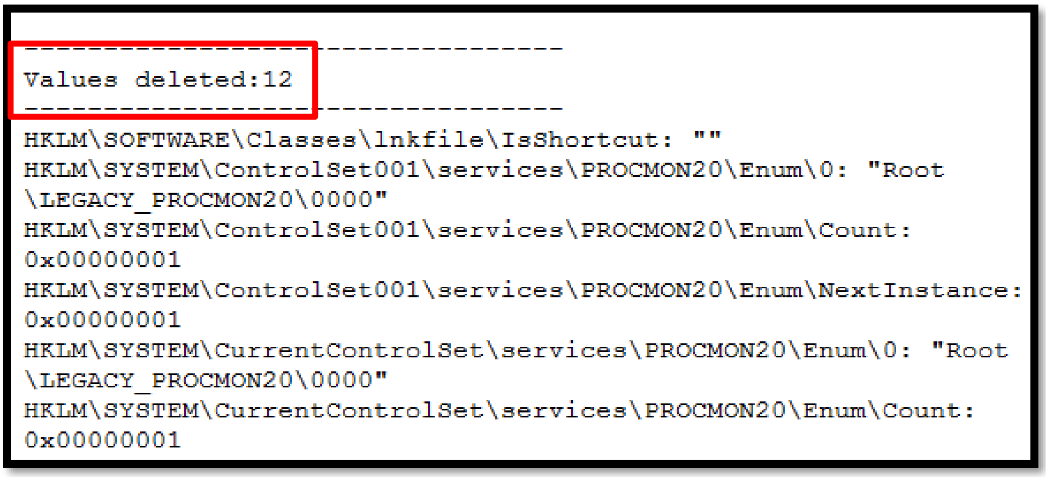
Figure 6.57: Regshot total changes

If continue to scroll down the document, it shows see that it outlines several different aspects including the following. Remember that the numbers will vary based on the computer as **Total changes:104, Keys deleted: 3, Keys added: 5**, and **Values deleted: 12**. It shows which Registry keys were added or deleted in **Figure 6.58** and which values were deleted **Figure 6.59.**



```
Regshot 1.8.2
Comments:
Datetime:2017/5/17 07:44:31 , 2017/5/17 07:52:22
Computer:WIN-SINQ77JPIEA , WIN-SINQ77JPIEA
Username:PSM 2017 , PSM 2017

----------------------------------
Keys deleted:3
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Google\Chrome\BrowserExitCodes

----------------------------------
Keys added:5
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON20\0000
\Control
HKLM\SYSTEM\ControlSet001\services\VSS\Diag
\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON20\0000
\Control
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag
\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
HKU\S-1-5-21-882804697-2239422844-2748470147-1000\Software
\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.html
\OpenWithList
```

Figure 6.58: Regshot keys added



```
---------------------------------
Values deleted:12
---------------------------------
HKLM\SOFTWARE\Classes\lnkfile\IsShortcut: ""
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\0: "Root
\LEGACY_PROCMON20\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\Count:
0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON20\Enum\NextInstance:
0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum\0: "Root
\LEGACY_PROCMON20\0000"
HKLM\SYSTEM\CurrentControlSet\services\PROCMON20\Enum\Count:
0x00000001
```

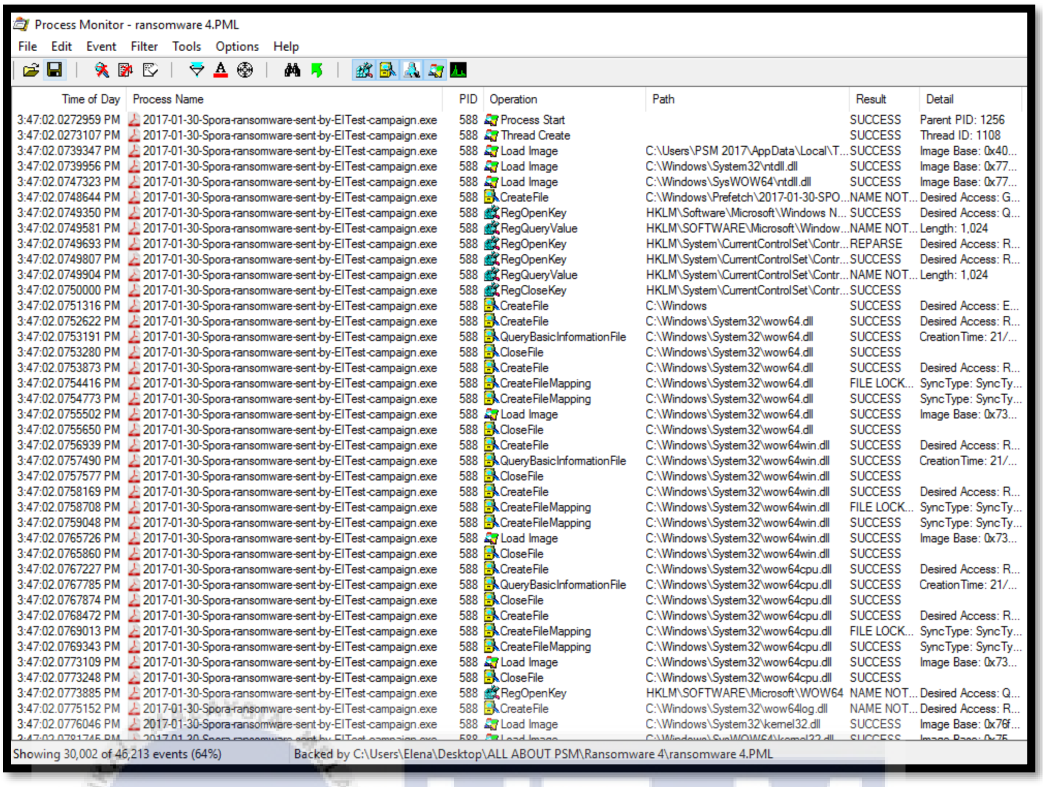
Figure 6.59: Regshot values deleted

It’s important to remember that Regshot not only captures the changes that the malware made, it also captures the changes made by any other application, including the operating system. Because of this, it can be difficult to identify changes made by the malware when you rely on this tool alone.

Process Monitor Analysis

Process Monitor also shows changes made to the Registry but it only captures those made by the API call, and may not show everything that occurred.

However, Process Monitor captures a whole lot more information. When viewing the saved output from Process monitor in **Figure 6.60**, the results can be staggering.



Process Monitor - ransomware 4.PML

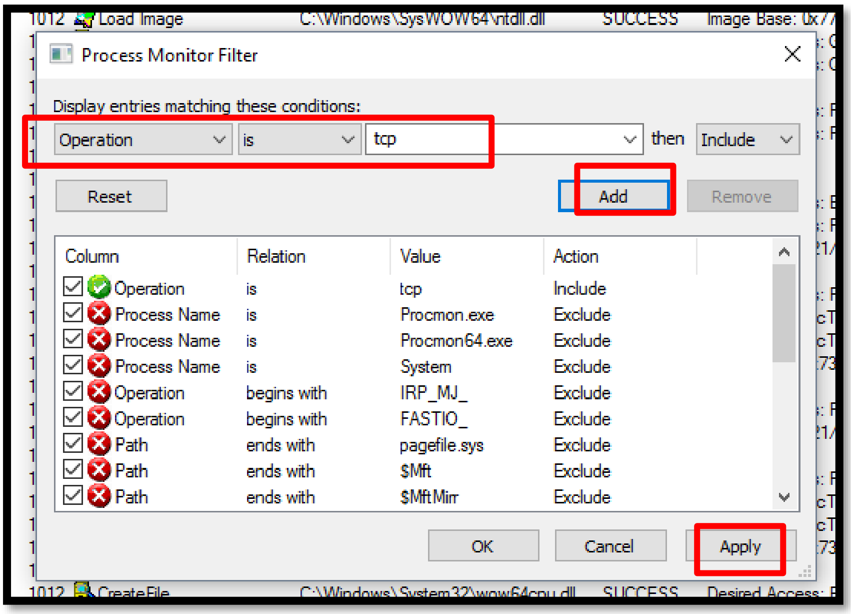
Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:47:02.0272959 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Process Start		SUCCESS	Parent PID: 1256
3:47:02.0273107 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Thread Create		SUCCESS	Thread ID: 1108
3:47:02.0739347 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Load Image	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Image Base: 0x40...
3:47:02.0739956 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77...
3:47:02.0747323 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77...
3:47:02.0748644 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\Prefetch\2017-01-30-SPO...	NAME NOT...	Desired Access: G...
3:47:02.0749350 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
3:47:02.0749581 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT...	Length: 1,024
3:47:02.0749693 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
3:47:02.0749807 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
3:47:02.0749904 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT...	Length: 1,024
3:47:02.0750000 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
3:47:02.0751316 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
3:47:02.0752622 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
3:47:02.0753191 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	QueryBasicInformationFile	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 21/...
3:47:02.0753280 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
3:47:02.0753873 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
3:47:02.0754416 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFileMapping	C:\Windows\System32\wow64.dll	FILE LOCK...	SyncType: SyncTy...
3:47:02.0754773 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFileMapping	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
3:47:02.0755502 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73...
3:47:02.0755650 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
3:47:02.0756939 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
3:47:02.0757490 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	QueryBasicInformationFile	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 21/...
3:47:02.0757577 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
3:47:02.0758169 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
3:47:02.0758708 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFileMapping	C:\Windows\System32\wow64win.dll	FILE LOCK...	SyncType: SyncTy...
3:47:02.0759048 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFileMapping	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
3:47:02.0765726 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x73...
3:47:02.0765860 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
3:47:02.0767227 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
3:47:02.0767785 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	QueryBasicInformationFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 21/...
3:47:02.0767874 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
3:47:02.0768472 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
3:47:02.0769013 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	FILE LOCK...	SyncType: SyncTy...
3:47:02.0769343 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
3:47:02.0773109 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73...
3:47:02.0773248 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
3:47:02.0773885 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT...	Desired Access: Q...
3:47:02.0775152 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT...	Desired Access: R...
3:47:02.0776046 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	588	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76f...

Showing 30,002 of 46,213 events (64%)   Backed by C:\Users\Elena\Desktop\ALL ABOUT PSM\Ransomware 4\ransomware 4.PML

Figure 6.60: Process Monitor initial screen

Again, an easy way to cut through the noise and find interesting artifacts from the malware is to use display filters. These filters function much like those in Wireshark, where it can search on specific keywords and ignore the rest of the data.

To use a filter, click on the Filter at the top of the screen and then select **Operation** in the drop-down box on the left. In the next box, select **Contains** and, in the final field, enter "**tcp**" **Figure 6.61**. This will display any TCP connections that were attempted by the malware. The results can differ from what Wireshark packet capture detected.



```
1012  Load Image    C:\Windows\SysWOW64\ntdll.dll        SUCCESS   Image Base: 0x7
1012  CreateFile    C:\Windows\System32\wow64cpu.dll     SUCCESS   Desired Access: F
```

Process Monitor Filter

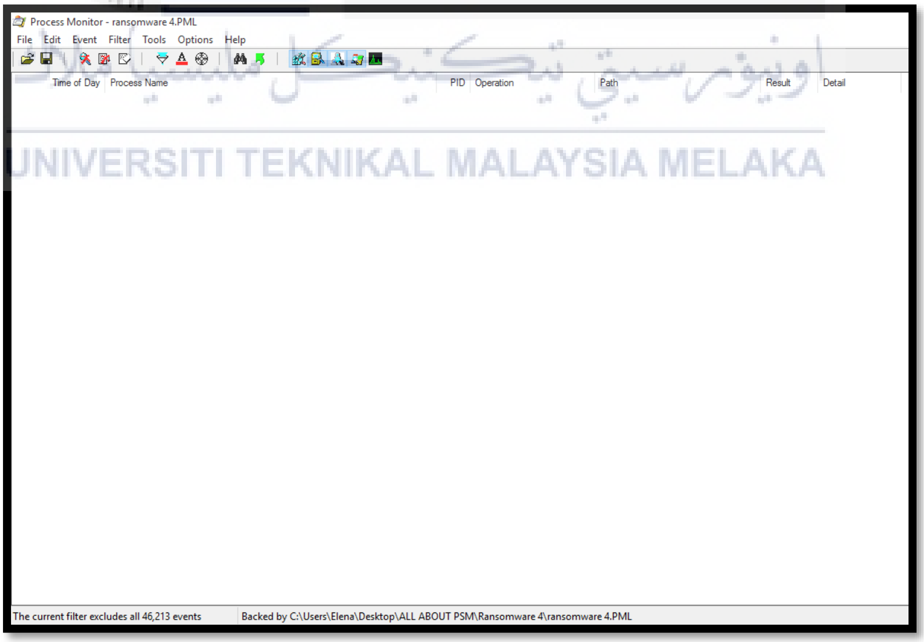
Display entries matching these conditions:

Operation | is | tcp | then Include

Column	Relation	Value	Action
☑ ✓ Operation	is	tcp	Include
☑ ✗ Process Name	is	Procmon.exe	Exclude
☑ ✗ Process Name	is	Procmon64.exe	Exclude
☑ ✗ Process Name	is	System	Exclude
☑ ✗ Operation	begins with	IRP_MJ_	Exclude
☑ ✗ Operation	begins with	FASTIO_	Exclude
☑ ✗ Path	ends with	pagefile.sys	Exclude
☑ ✗ Path	ends with	$Mft	Exclude
☑ ✗ Path	ends with	$MftMirr	Exclude

Figure 6.61: Procmon filter TCP

The filtered results in Process Monitor now show a new TCP host that wasn't easily identifiable in our NetworkMiner display in **Figure 6.62**. Therefore, it is important to use the output from multiple tools for our analysis. If hadn't checked this filter in Procmon, it's possible that could have missed this domain.



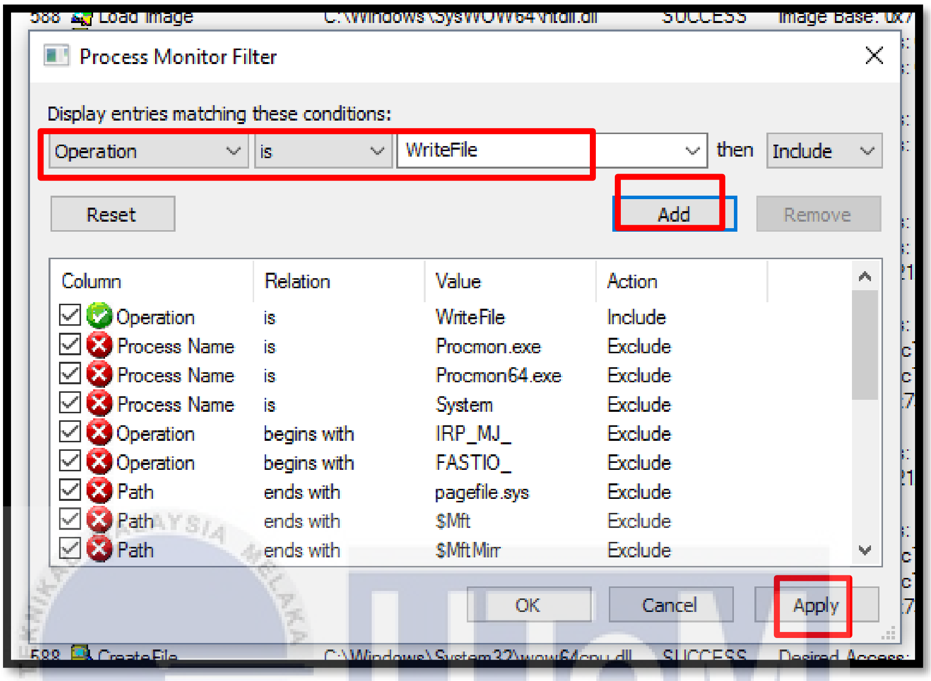
Process Monitor - ransomware 4.PML

The current filter excludes all 46,213 events

Backed by C:\Users\Elena\Desktop\ALL ABOUT PSM\Ransomware 4\ransomware 4.PML

Figure 6.62: Procmon filter results

Process Monitor can also use a display filter to show any files that were written to the drive by the malware. It will filter for any Operation matching "WriteFile" to display this in **Figure 6.63**. Knowing what files are created on the system can help us identify additional malware that was downloaded, as well as help build out a list of identifiers can search for later.



Process Monitor Filter

Display entries matching these conditions:

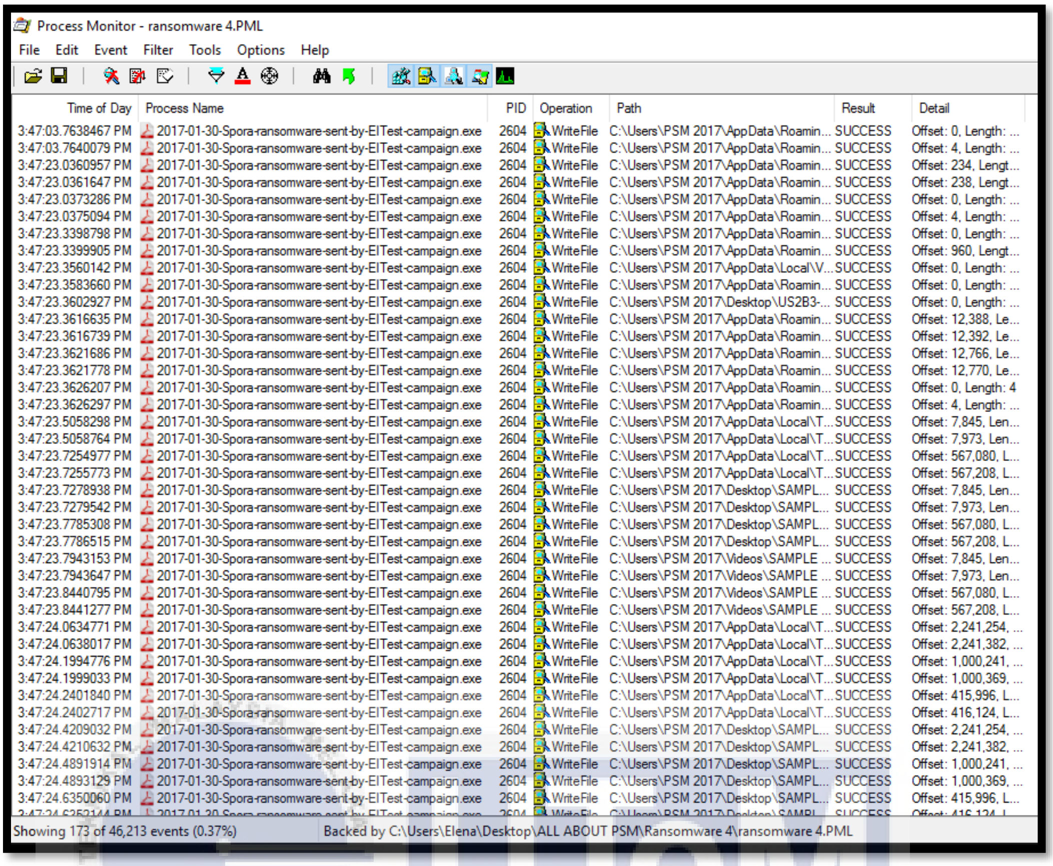
Operation is WriteFile then Include

Column	Relation	Value	Action
☑ ✓ Operation	is	WriteFile	Include
☑ ✗ Process Name	is	Procmon.exe	Exclude
☑ ✗ Process Name	is	Procmon64.exe	Exclude
☑ ✗ Process Name	is	System	Exclude
☑ ✗ Operation	begins with	IRP_MJ_	Exclude
☑ ✗ Operation	begins with	FASTIO_	Exclude
☑ ✗ Path	ends with	pagefile.sys	Exclude
☑ ✗ Path	ends with	$Mft	Exclude
☑ ✗ Path	ends with	$MftMirr	Exclude

588 Load Image C:\Windows\SysWOW64\ntdll.dll SUCCESS Image Base: 0x7
Reset
Add
Remove
OK
Cancel
Apply
588 CreateFile C:\Windows\System32\wow64cpu.dll SUCCESS Desired Access:

Figure 6.63: Procmon filter Writefile

From these filtered results in **Figure 6.64**, it shows that our malware sample, 2017-01-30-EITest-fake-Chrome-popup-sends-Spora-malware-and-artifacts.exe, created several files on the system.



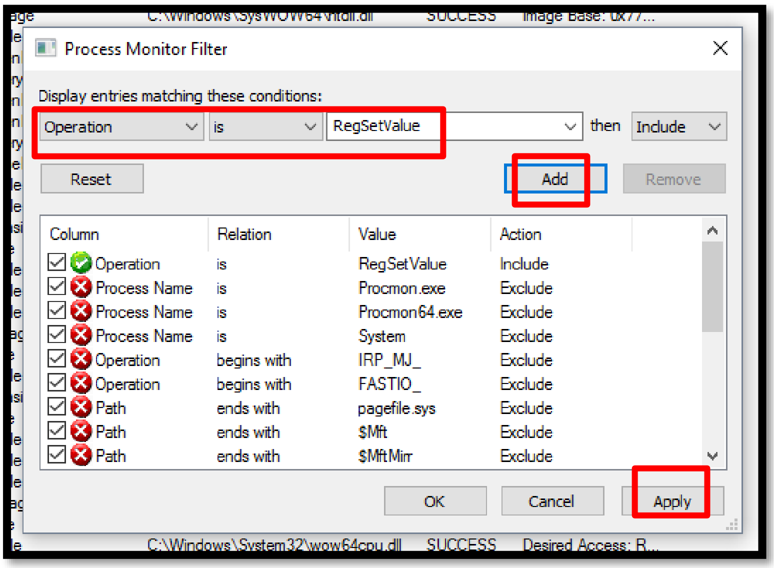
Process Monitor - ransomware 4.PML
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:47:03.7638467 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 0, Length: ...
3:47:03.7640079 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 4, Length: ...
3:47:23.0360957 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 234, Lengt...
3:47:23.0361647 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 238, Lengt...
3:47:23.0373286 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 0, Length: ...
3:47:23.0375094 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 4, Length: ...
3:47:23.3398798 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 0, Length: ...
3:47:23.3399905 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 960, Lengt...
3:47:23.3560142 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\V...	SUCCESS	Offset: 0, Length: ...
3:47:23.3583660 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 0, Length: ...
3:47:23.3602927 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\US2B3-...	SUCCESS	Offset: 0, Length: ...
3:47:23.3616635 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 12,388, Le...
3:47:23.3616739 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 12,392, Le...
3:47:23.3621686 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 12,766, Le...
3:47:23.3621778 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 12,770, Le...
3:47:23.3626207 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 0, Length: 4
3:47:23.3626297 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Roamin...	SUCCESS	Offset: 4, Length: ...
3:47:23.5058298 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 7,845, Len...
3:47:23.5058764 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 7,973, Len...
3:47:23.7254977 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 567,080, L...
3:47:23.7255773 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 567,208, L...
3:47:23.7278938 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 7,845, Len...
3:47:23.7279542 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 7,973, Len...
3:47:23.7785308 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 567,080, L...
3:47:23.7786515 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 567,208, L...
3:47:23.7943153 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Videos\SAMPLE ...	SUCCESS	Offset: 7,845, Len...
3:47:23.7943647 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Videos\SAMPLE ...	SUCCESS	Offset: 7,973, Len...
3:47:23.8440795 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Videos\SAMPLE ...	SUCCESS	Offset: 567,080, L...
3:47:23.8441277 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Videos\SAMPLE ...	SUCCESS	Offset: 567,208, L...
3:47:24.0634771 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 2,241,254, ...
3:47:24.0638017 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 2,241,382, ...
3:47:24.1994776 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 1,000,241, ...
3:47:24.1999033 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 1,000,369, ...
3:47:24.2401840 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 415,996, L...
3:47:24.2402717 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\AppData\Local\T...	SUCCESS	Offset: 416,124, L...
3:47:24.4209032 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 2,241,254, ...
3:47:24.4210632 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 2,241,382, ...
3:47:24.4891914 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 1,000,241, ...
3:47:24.4893129 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 1,000,369, ...
3:47:24.6350060 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	WriteFile	C:\Users\PSM 2017\Desktop\SAMPL...	SUCCESS	Offset: 415,996, L...

Showing 173 of 46,213 events (0.37%) Backed by C:\Users\Elena\Desktop\ALL ABOUT PSM\Ransomware 4\ransomware 4.PML

Figure 6.64: Procmon filter WriteFile results

It can also display any changes 2017-01-30-EITest-fake-Chrome-popup-sends-Spora-malware-and-artifacts.exe made to the Windows Registry. For this, it will look for the value named RegSetValue in **Figure 6.65** below.



C:\Windows\SysWOW64\ntdll.dll SUCCESS Image Base: 0x77...

Process Monitor Filter

Display entries matching these conditions:

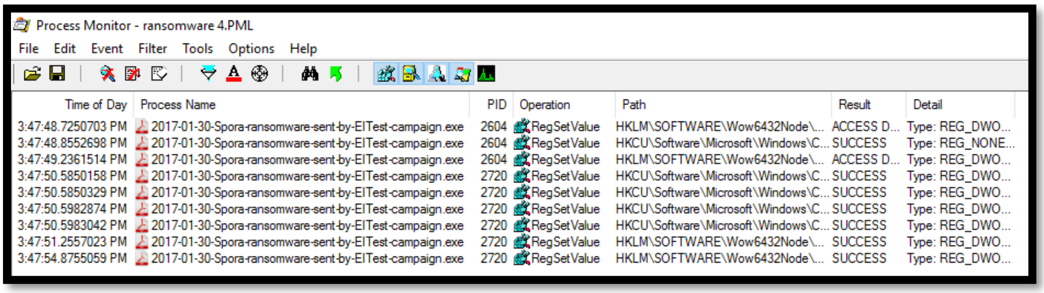
Operation is RegSetValue then Include

Column	Relation	Value	Action
☑ Operation	is	RegSetValue	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude
☑ Process Name	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Path	ends with	pagefile.sys	Exclude
☑ Path	ends with	$Mft	Exclude
☑ Path	ends with	$MftMirr	Exclude

C:\Windows\System32\wow64cpu.dll SUCCESS Desired Access: R...

Figure 6.65: Procmon filter RegSetValue

After applying our filter, it shows that 2017-01-30-EITest-fake-Chrome-popup-sends-Spora-malware-and-artifacts.exe made several changes to the registry when it executed in **Figure 6.66**.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:47:48.7250703 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	RegSetValue	HKLM\SOFTWARE\Wow6432Node\...	ACCESS D...	Type: REG_DWO...
3:47:48.8552698 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_NONE...
3:47:49.2361514 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2604	RegSetValue	HKLM\SOFTWARE\Wow6432Node\...	ACCESS D...	Type: REG_DWO...
3:47:50.5850158 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2720	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
3:47:50.5850329 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2720	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
3:47:50.5982874 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2720	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
3:47:50.5983042 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2720	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
3:47:51.2557023 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2720	RegSetValue	HKLM\SOFTWARE\Wow6432Node\...	SUCCESS	Type: REG_DWO...
3:47:54.8755059 PM	2017-01-30-Spora-ransomware-sent-by-EITest-campaign.exe	2720	RegSetValue	HKLM\SOFTWARE\Wow6432Node\...	SUCCESS	Type: REG_DWO...

Figure 6.66: Procmon filter RegSetValue results

The results of analysis ransomware samples summarize in the **Table 6.1** below.

Table 6.1 Comparison Results between Different Ransomware Sample

Ransomware/ Findings	**Sample 1**	**Sample 2**	**Sample 3**	**Sample 4**
PID (Procmon)	2060	3060	1612	2604
File Size	199KB	227KB	97KB	85KB
IP Address (Wireshark)	104.16.93.188	No Specific IP Address	No Specific IP Address	104.16.91.188
TCP Connection	YES	NO	YES	NO
Total Changes (Regshot)	192	128	173	104
Keys Added (Regshot)	6	5	5	3
Keys Deleted (Regshot)	18	20	14	5
Values Deleted (Regshot)	22	21	21	12

This research can conclude from a few analyses which include NetworkMiner Analysis, Wireshark Analysis, File System Analysis and Process Monitor Analysis, each of them have both the advantages and disadvantages. The data have been collected and looked at a great deal including Registry changes and network connections. This is where experience and knowledge become a factor.

This project does not want to assume every Registry change or outbound network connection is bad. It would have thousands of false alerts on our networks if it occurs. Instead, this project wants to take the known malicious activity generated by the ransomware and use this as a baseline to investigate other hosts. Known malicious activity is commonly called an “indicator of compromise” (IoC).

From all the packet capture analysis, this research project performed with Wireshark and Network Miner, the ransomware makes an outbound connection: **crl.comodoca.com.cdn.cloudflare.net**. Another indicator that can be use when analysing hosts is the Registry changes and file writes. These changes normally will occur again the next time ransomware is executed.

General Attack Flow of Ransomware

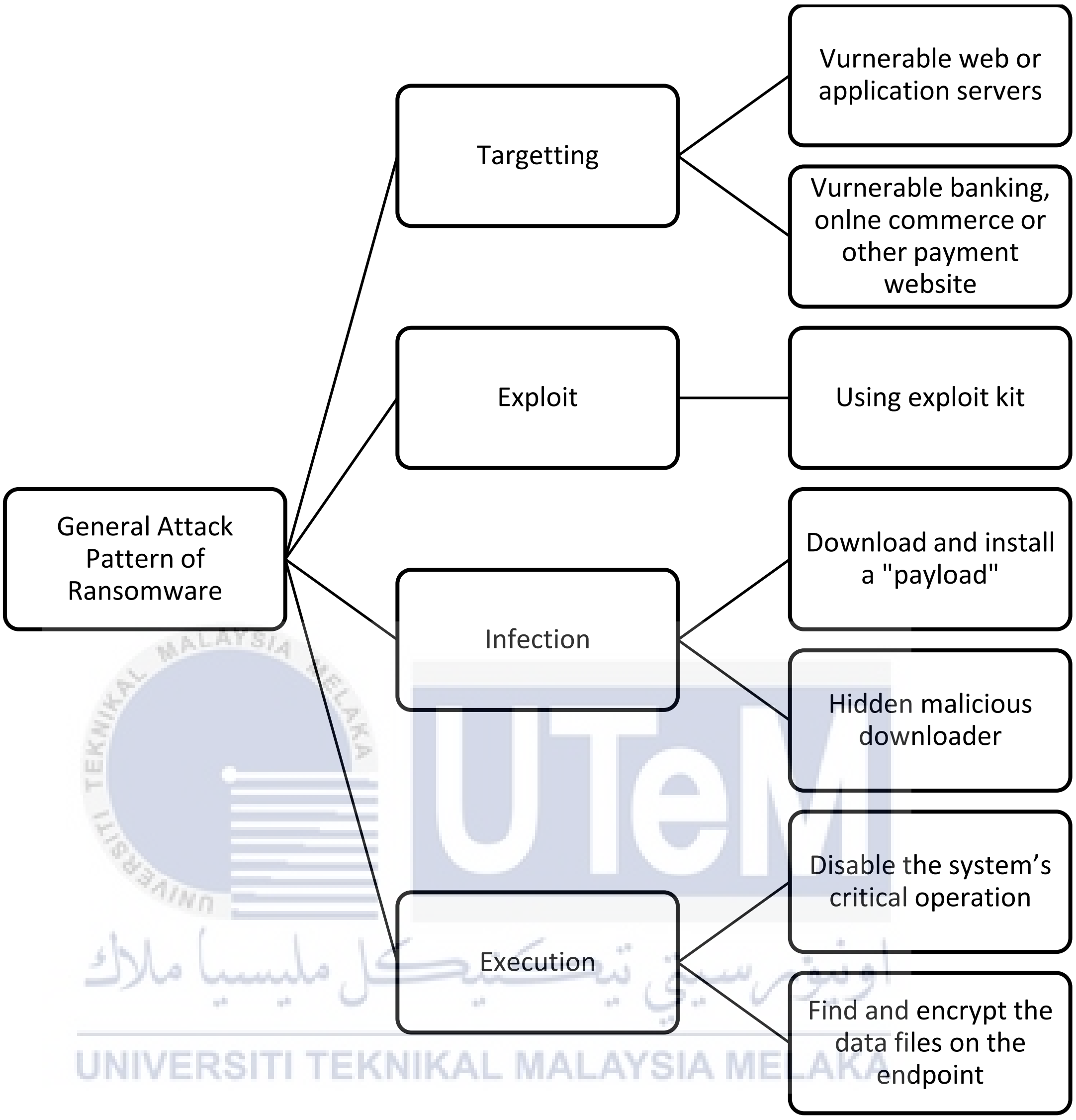

General Attack Pattern of Ransomware
Targetting
Exploit
Infection
Execution
Vurnerable web or application servers
Vurnerable banking, onlne commerce or other payment website
Using exploit kit
Download and install a "payload"
Hidden malicious downloader
Disable the system's critical operation
Find and encrypt the data files on the endpoint

Figure 6.67 General Attack Flow Ransomware

Targeting

Ransomware has primarily targeted endpoints running the Microsoft Windows operating system, although attacks targeting Mac operating system and mobile platforms are on the rise given their increasing, popularity. Users in specific geographic regions like Russia, Brazil and of course the US have seen the bulk of ransomware attacks. Because websites are a mechanism for the hackers to initiate the attack through hidden redirects and drive-by-downloads, hackers will also focus their attention on public websites running vulnerable web- or application-servers that they can leverage. This avenue is particularly dangerous if the hacker can find vulnerabilities in banking, online commerce or other payment websites.

Exploit

Many hackers today use malware packaged into exploit kits that they covertly place on legitimate websites, or host on fake websites designed to look like a legitimate site. When a potential victim’s browser lands on a website hosting such an exploit kit, the kit probes the visitor’s system and extracts information like OS, browser type, version information and applications installed to find and exploit vulnerabilities. Once the exploit kit has found a security vulnerability that it can exploit, the attack proceeds to the next step.

Infection

In the infection stage, the previous steps are used to download and install a “payload” to the victim’s endpoint or mobile device. This payload could be the actual ransomware itself, or it could also be a hidden malicious downloader which then creates a backdoor through which multiple types of malware can be downloaded and many different attacks can be executed.

Execution

Once the ransomware has been installed on the victim’s endpoint, the actual execution of the malicious program starts doing what it is designed to do – which is disable the system’s critical operation or find and encrypt the data files on the endpoint. At this point the disruption directs the victim to the hacker’s monetization mechanisms with instructions on where to send the ransom, in what form to make the payment (usually BitCoin) and other details to ensure the victim complies with the hacker’s instructions.

6.3 Conclusion

In this testing and analysis chapter, the actual result of this project will be documented. This chapter also will briefly describe about the activity involved in the implementation phase of this project

CHAPTER VII

PROJECT CONCLUSION

7.1 Introduction

The result and analysis had been done in previous chapter. In this chapter, the project conclusion will be contributed. The research summarization, research contribution, constraint, limitation and further research will be included in this chapter.

7.2 Project Summarization

To summarize this report, I would like to recall the objective of this project. The first objective is to analyses the behavior of a malware known as Ransomware to specific parameter or application and what the effect after the infection occurs. By using dynamic analysis approach to see the behavior of ransomware through virtual machine software (VMware) and through monitoring software as example by using *Wireshark* and *Process Monitor*. The ransomaware installed into the virtual OS or application and then the behavior will be observed and recorded. The behavior of the application before and after the ransomware infection also will be compared and analyzed.

7.3 Project Contribution

There are several expected contributions of this project to the community.

1. Highlight the parameters that the Ransomware affected and compromise (stated in chapter 2)
2. Verify what the Ransomware do with the information that it bad gathers.
3. Highlight the attack traces of the Ransomware (stated in chapter 4)

7.4 Project Limitation

There are several constraints and limitation on this research project. This research did not use any script that can help the computer user to detect the ransomware. If this can be done, the user can prevent their computer from being attacked by this type of malware. Besides, this project only uses the tools for dynamics analysis and not included with tools for static analysis. If other future researcher investigate ransomware using static analysis, the new findings might be come out.

7.5 Future Works

The future work that can be done with the information from this project and overcome the limitations of this project are: -

1. To build a script that can automatically convert and scan the code, so that it can overcome the limitation of this project.
2. To do a research on how to detect this malware better and build a stronger antivirus system that can detect and block this malware.
3. To do research on how to avoid the malware infections from being embedded to an application easily.
4. To build a stronger application source code with high security features.

7.6 Conclusion

In summary, this research had reached all the objectives and scopes that defined in Chapter 1. The behavior of ransomware is identified including its parameters and general attack flow. Based on the results, the general attack flow is successfully generated. The contribution of this research is significant but more research needed to overcome the constraints and the limitation thus more future works is needed to improve current weakness of project. This chapter has concluded the research undertaken in this project and recommendation for the further research.

REFERENCES

CABAJ, K. (2015). Network activity analysis of CryptoWall ransomware. *Przegląd Elektrotechniczny*, *1*(11), 203–206. https://doi.org/10.15199/48.2015.11.48

Elekar, K. S. (2015). Combination of Data Mining Techniques for Intrusion Detection System.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9148*, 3–24. https://doi.org/10.1007/978-3319-20550-2_1

Gorman, G. O., & McDonald, G. (2012). Ransomware: A Growing Menace. *Symantec*, *1*, 16.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *Proceedings - International Conference on Distributed Computing Systems*, *2016–Augus*, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Kansagra, D., Kumhar, M., & Jha, D. (n.d.). Ransomware: A Threat to Cybersecurity, 224–227. https://doi.org/10.090592/IJCSC.2016.035

KS, C., TM, S., & DP, L. (2016). Ransomware Against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory. *International Journal of Forensic Science & Pathology*, *4*, 253–258. https://doi.org/10.19070/2332-287X-1600061

Analysis, A., & Ransomeware, L. (n.d.). CryptoWall CryptoWall Version.

Chaisamran, N., Okuda, T., & Yamaguchi, S. (2012). A proposal for anomaly traffic detection in the IP multimedia subsystem using Tanimoto distance and a modified moving average. *Proceedings - 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, SAINT 2012*, 278–283. https://doi.org/10.1109/SAINT.2012.78

Curriculum, L., & Cramton, R. C. (2014). The Current State of Ransomware, *1*(December).

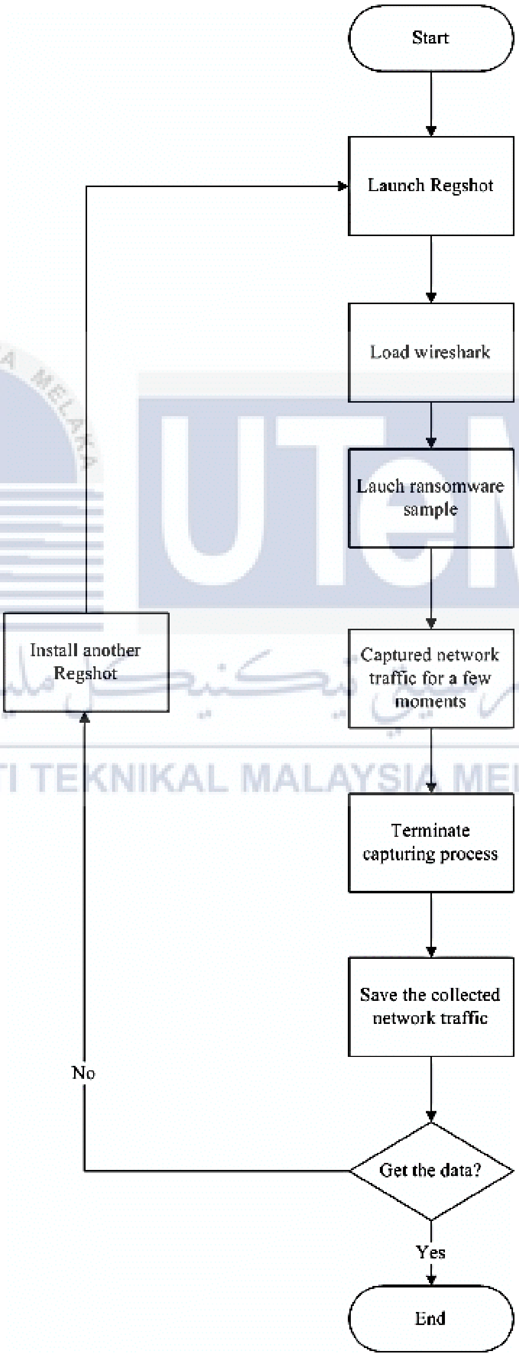
Aissa, N. B., & Guerroumi, M. (2015). A Genetic Clustering Technique for Anomaly-Based Intrusion Detection Systems.

Özçelik, İ., & Brooks, R. R. (2016). Cusum - Entropy: An efficient method for DDoS attack detection, 1–5.

Sharma, M. P., Zawar, S., & Patil, S. B. (2016). Ransomware Analysis: Internet of Things (Iot) Security Issues , Challenges and Open Problems Inthe Context of Worldwide Scenario of Security of Systems and Malware Attacks. *International Journal of Innovative Research N Science and Engineering*, *2*(3), 177–184. Retrieved from http://www.ijirse.com/wp-content/upload/2016/02/1089B.pdf

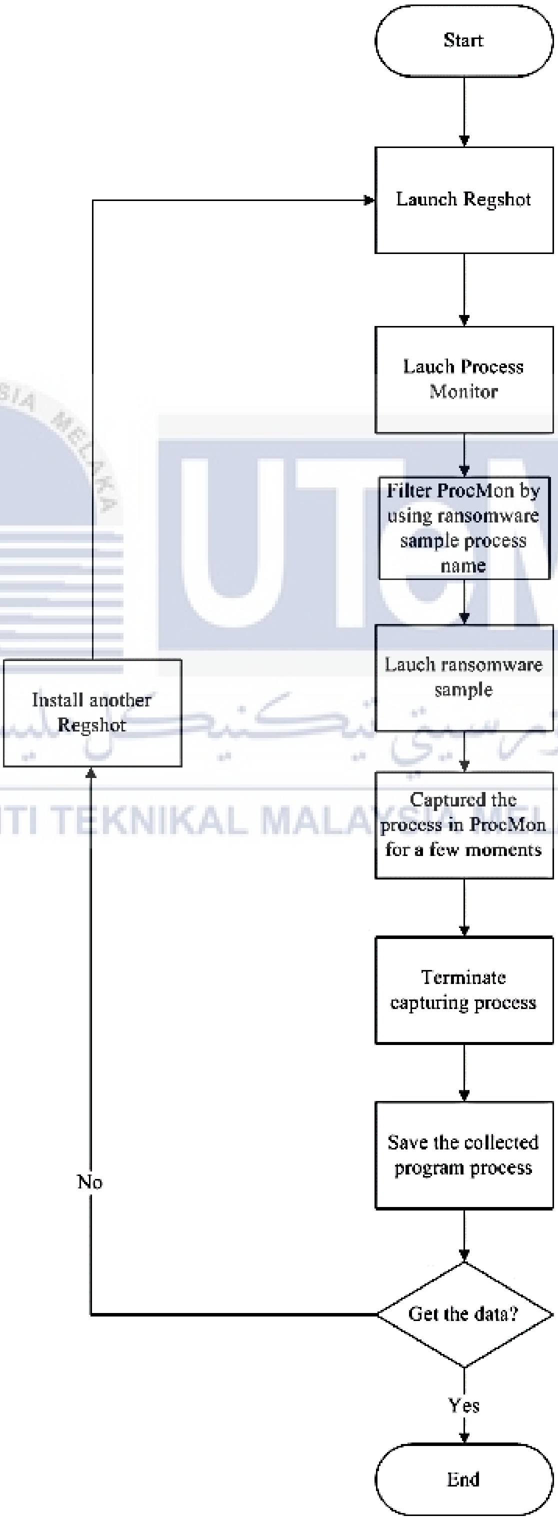
APPENDIX A

1. Process of Collect Network Traffic



Start
Launch Regshot
Load wireshark
Lauch ransomware sample
Captured network traffic for a few moments
Terminate capturing process
Save the collected network traffic
Get the data?
Yes
End
No
Install another Regshot

2. Process of Collect Program Process


Start
Launch Regshot
Lauch Process Monitor
Filter ProcMon by using ransomware sample process name
Lauch ransomware sample
Captured the process in ProcMon for a few moments
Terminate capturing process
Save the collected program process
Get the data?
Yes
End
No
Install another Regshot