

Digital Triage In Forensics Investigation

Nikolaos Bakirtzis

SID: 3301120004

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

NOVEMBER 2013 THESSALONIKI – GREECE



Digital Triage In Forensics Investigation

Nikolaos Bakirtzis

SID: 3301120004

Supervisor:Prof. Vasilios KatosSupervising CommitteeAssoc. Prof.Members:Assist. Prof.

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

NOVEMBER 2013 THESSALONIKI – GREECE

Abstract

This dissertation was written as a part of the MSc in ICT Systems at the International Hellenic University.

The digital triage in forensics investigation can really make the digital investigation a success or a disaster depending on numerous factors. There are numerous triage tools freely available online but there is no mature framework for practically testing and evaluating them. In the following pages we will analyze four open source triage tools and identify the advantages and drawbacks of each of them. We will also test their compliance to published forensic principles (ACPO).

The results prove that due to high complexity and variety of system configurations, triage tools should become more adaptable, in dynamic and manual manner, depending on the case and context, instead of sustaining a monolithic functionality.

After identifying the problem, an effort was made to create a program, that has the ability to search a whole computer, or any partition or file chosen, for files with any possible extension, that are installed or created by the user. This was possible by comparing the MD5 hashes of the files. In this way the investigator can search, in a very short time, the computer under examination, for installed and created files or programs, altered programs, possible malware and harmful programs.

This program can have even greater usability if it is incorporated into other digital triage programs or if it is enhanced with more advanced functionality.

Special thanks is given to my supervisor Prof. Vasilios Katos that showed me the way to where address my research and solved any issues raised giving insightful feedback.

Nikolaos Bakirtzis 05-11-2013

Contents

A	BSTR	ACT		[
С	ONTE	NTS	IV	7
1	INT	RODUG	CTION	L
2	LITE	ERATU	RE REVIEW	7
	2.1	DIGITA	L FORENSIC PROCESS	3
		2.1.1	Techniques	1
		2.1.2	Volatile data	!
		2.1.3	Analysis tools	?
		2.1.4	Certifications	?
	2.2	DIGITA	L TRIAGE IN FORENSICS INVESTIGATION	<u>)</u>
	2.3	TESTIN	IG TRIAGE TOOLS	7
	2.4	BULK I	EXTRACTOR	7
		2.4.1	Advantages	3
		2.4.2	Drawbacks	3
	2.5	Triag	EIR v.0.79)
		2.5.1	Advantages)
		2.5.2	Drawbacks)
	2.6	TR3S	ECURE)
		2.6.1	Advantages	!
		2.6.2	Drawbacks	[
	2.7	KLUDO	E 3.20110223	
		2.7.1	Advantages	2
		2.7.2	Drawbacks	2
	2.8	SYNOF	23 23	3
		2.8.1	Bulk Extractor	3
		2.8.2	TriageIR, TR3Secure and Kludge25	5
	2.9	Suggi	ESTIONS	3
		2.9.1	Bulk Extractor)

	2.9.2	TriageIR 0.79	29
	2.9.3	TR3Secure	29
	2.9.4	Kludge 3.20110223	29
2.10	Futur	E WORK ON THE FOUR TOOLS	30
PRO	BLEM	DEFINITION	31
3.1	BULK E	EXTRACTOR	32
3.2	Triage	EIR v.0.79	32
3.3	TR3S	ECURE	32
3.4	Kludg	ie 3.20110223	33
CON	TRIBL	JTION	35
4.1	FIRST	THOUGHTS	35
4.2	THE NE	EW TARGET	37
4.3	The de	EVELOPING PROCESS	38
4.4	THE SC	CANNER PROGRAM - HOW IT WORKS	39
	4.4.1	Help mode	40
	4.4.2	Scan mode with no parameters	42
	4.4.3	Scan mode with parameters	47
	4.4.4	Compare mode with parameters	52
4.5	THE SC	CANNER_VERSION_2 PROGRAM	62
4.6	THE SC	CANNER_VERSION_3 PROGRAM	63
4.7	Advan	ITAGES	70
4.8	Draw	BACKS	71
4.9	EVALU	ATION	71
4.10	Sugge	ESTIONS	71
4.11	Futur	E WORK – ENHANCEMENTS	72
4.12		LUSION	73
PER	SONA	L REFLECTION	75
CON	CLUS	IONS	78
6.1	DIGITA	L FORENSICS IS DIFFERENT	78
	6.1.1	The challenge of data diversity	79
	6.1.2	Data scale	79
	610	Temporal diversity: the never-ending upgrade cycle	70
	2.10 PRO 3.1 3.2 3.3 3.4 CON 4.1 4.2 4.3 4.4 4.3 4.4 4.5 4.4 4.5 4.6 4.7 4.8 4.9 4.10 4.11 4.12 PERS CON	2.9.3 2.9.4 2.9.4 2.10 FUTUR PROBLEM 1.1 BULK B 3.2 TRIAGE 3.2 TRIAGE 3.3 TR3SE 3.4 KLUDE 1.3 TR3SE 3.4 KLUDE 1.4 FIRST 4.2 THE NE 4.2 THE NE 4.3 THE SE 4.4 T	2.9.3 TR3Secure. 2.9.4 Kludge 3.20110223

	6.1.4	Human capital demands and limitations	. 80
	6.1.5	The CSI effect	. 80
	6.1.6	The cost of development and the role of government	. 80
6.2	LESSO	NS LEARNED DEVELOPING DIGITAL FORENSICS TOOLS	. 81
	6.2.1	Platform and language	. 81
	6.2.2	Parallelism and high performance computing	. 81
	6.2.3	All-in-one tools vs. single-use tools	. 81
	6.2.4	Evidence container file formats	. 82
6.3	CONCI	_USION	. 82
REFER	ENCES	S	85
APPEN	DIX		91

1 Introduction

Computers and computing devices are more and more a part of our lives. Not only most of us have a computer, such as desktops and laptops but we also have smart phones, tablets and GPSs in our cars. If we don't have a phone available, we can use our laptop or tablet and communicate with others using instant messaging, email, Twitter, or Skype applications. Furthermore computers become more and more a part of our lives, so does crime involving those devices. Whether it's "cyberbullying" or "cyberstalking," identity theft, or intrusions and data breaches, all result in some form of data theft. A wide number of real-world physical crimes are now being committed through the use of computers, and as such, get renamed by prepending "cyber" to the description. As we transfer lot of the things that we did in the real world to the online world, we became targets of cybercrime. [19]

What makes this activity even more insidious and sophisticated is that we don't recognize it for what it is, because conceptually, the online world is simply so foreign to us. If someone breaks a storefront window to steal a television, there's noise, alarm, broken glass, and someone running away with the stolen goods. Cybercrime isn't like this; something isn't stolen and then absent, but is also copied. Additionally, the crime does result in something that is stolen and removed from us, but we may not understand that immediately, because we're talking about 1s and 0s in cyberspace, not for example a car in our garage. These malicious activities also increase in complexity. In many cases, the fact that a crime has happened is not obvious until someone notices a significant decrease in a bank account, which shows that the perpetrator has already gained access to systems, gathered the data needed, accessed that bank account, and left with the money. The incidents are not detected until well after they've occurred. In other cases, the malicious activity continues and even escalates after we become aware of it, because we're unable to defend from the attack. [19]

Computers, as mentioned above, can be used for committing a crime, contain evidence of a crime or be targets of the crime. Specifying the role and nature of the electronic evidence, how to analyze a crime scene that contains electronic evidence and how the responder should act to these circumstances is important. [1]

Triage is a term deriving from medicine. It is defined as "the sorting and allocation of treatment to patients and victims in battle and disaster according to priorities that target to maximize the number of survivors". [52] In incident response the term triage is specified as the step where an analyst when receiving a report about an incident, assesses the danger, prioritizes the incident, relates it to other incidents and decides whether this report is true. [9] Triage is a way of prioritizing tasks and allocating the resources which are limited. [23]

Digital triage give to us: The knowledge what items to be taken from the scene. This helps us manage the flow of items that will be examined. This speeds the whole process. [23] This is done by executing triage software in the suspect system.

From the above definition it is obvious that the success of the investigation depends on the first actions and triage of the first responder. Correct priorities and handling of the live system may reveal an encrypted partition or a remote IP. [77]

Historically, the computer related crime concerned only a small number of victims and investigators. Nowadays this situation is changing and the impact of digital evidence within conventional investigations is very common. In addition, any investigation in the public or private sector usually involves the seizure, preservation and examination of electronic evidence. [1]

The former pull-the-plug approach is obsolete and overlooks the volatile data that will be lost. Today, investigators face the fact of sophisticated data encryption, hacking tools and malicious software that exist only in memory. [1]

The most widespread strategies to collect potential evidence are two: a) use personnel with limited forensic training and seize everything or b) use skilled experts with selective acquisition. In the first approach, there will be potential damage of digital evidence during the process. The second approach has advantages in serious crime or major incidents, but removes valuable skills from the forensic staff which reduces the throughput and capacity respond in the laboratory. [37]

Examiners need to constantly upgrade their skills, tools, and knowledge to keep up with the new technologies. The solution is not just to unplug the computer and evaluate it later. Examiners must know how to capture an image of the running memory and perform volatile memory analysis using various tools. [93] In figure 1 there is a compari-

son between live response with Sys-Internal tools vs. memory analysis on a static memory dump. [93]

Sys-Internal vs. Memory Analysis Tools	Ner	One Const	Run Ports and thomas and the sections	Hier Proceed	Ter Runnises	Load De De De Ces	Ope DILS Cresses	OS. Files	Aron Marine Marine	Series Ourner	200 200 DS	r Logoer Ch
Live Response												
PsList			X									1
ListDLLs						Х						
Handle							Х					
Netstat	Х	Х										
Fport		Х]
Userdump									Х]
Strings										X		
PsLoggedOn											X]
Memory Analysis]
Volatility	X	Х	X	X	Х	Х	X	X			X]
PTFinder			X	Х	Х]

Figure 1: Live response with Sys-Internal tools vs. memory analysis on a static memory dump. [93]

Electronic evidence is very fragile. It can be altered, damaged, or destroyed by wrong handling and improper examination. This is why special actions should be taken to document, collect, preserve and examine the digital evidence. Failure to do so can make it useless or drive to a faulty conclusion. [1]

A usual forensic lifecycle for a hard drive can be the following:

- Remove the disk from the computer.
- Connect this disk to the examiners computer with a writeblocker that prevents any alterations.
- Make an image of the disk that represents all the contents of the disk.
- Make cryptographic hash values for each and every digital object and for the disk.
- Search for malware.
- View files.

- Search metadata.
- Extract metadata.
- Identify and bookmark privacy concerns.
- Create replicates and examine them in an emulator.
- Convert digital replicates to interoperable files known as digital facsimiles.
- Analyze metadata.
- Create log files during the examination process.
- Make a forensic report as documentation. [48]

All the above were given me the incentive for this dissertation which contains the following: In the Literature Review there is an explanation and analysis of what digital triage in forensics investigation is about and what is the current picture. Digital triage categories, characteristics, scopes, goals, objectives and achievements till nowadays. References to four existing tools that are free and things to consider when choosing the right tool. There is research for these four open source triage tools to help us understand and study the most important issues concerning these digital triage processes. There is description of the effort needed and the practical challenges an analyst may encounter when employing them. Also these tools are evaluated depending on the requirements of the ACPO principles, a practice guide developed for digital forensics. [77] In bibliography they analyzed and they also proposed ways of improving these tools.

In the Problem Definition there is an analysis of what existing tools provide, what they don't offer and why this is important. Why the lack of a proper and advanced tool is so important. There is gap analysis and drawbacks of the presented tools. Also possible contributions of a new tool.

In the Contribution is presented the thought to make a program that could search the computer targeted and find added files, altered files, infected files or even malware constructed by the suspect. As a start the target was to make a program that would search the computer under investigation for the files we want to find. To have the ability to choose the type of files we want, the domain of the computer to search in, the file the results would be saved in. The results would show the name and the path of the files found. The next target was to find all the MD5 hashes of the files we want. This could help to find which files were modified in comparison to the original ones. This could be achieved by producing the MD5 hashes [50] of the files found and comparing them with the MD5 hashes of the original files. In the next stage all the above was necessary not to

be hard coded but to offer the examiner the ability to insert the desired values as parameters during the execution. During the development many features were added and the program was upgraded and became more complicated until it reached its final form. My target was to easy the forensics analyst and provide him an overview of the hard disc with a glimpse. Demonstrate and present the contents of the hard disc in a way that helps the investigator have a more concrete image of the contents of the disc. Help him take the right decisions fast.

In the Personal Reflection there is the personal opinion about the subjects analyzed, the problems, the solutions and the contribution offered. What went wrong, what to avoid the next time, where to improve and upgrade in the future.

In the Conclusions there is the summary of the work of the dissertation. Evaluation of achievements and final thoughts.

This dissertation is structured as follows:

Chapter 2 contains the literature review. An extensive research of what has been published by accredited scholars and researchers on the topic has been made. In chapter 2.1 digital forensic process is analyzed including techniques, volatile data, analysis tools and certifications that can be obtained. In chapter 2.2 digital triage in forensics investigation is explained. In chapter 2.3 we talk about testing triage tools. In chapter 2.4 the tool Bulk Extractor is tested retrieving its advantages and drawbacks. In chapter 2.5 the tool TriageIR is tested highlighting its advantages and drawbacks. In chapter 2.6 the tool TR3Secure is tested mentioning its advantages and drawbacks. In chapter 2.7 the tool Kludge is tested acknowledging its advantages and drawbacks. In chapter 2.8 there is a synopsis of the testing process and in chapter 2.9 there are suggestions for each tool. In chapter 2.10 there are some proposals on future work on the four tools.

Chapter 3 contains the definition of the problem in digital forensics. In chapters 3.1, 3.2, 3.3, 3.4 problems are specified for each and every one of the four tools.

Chapter 4 contains the contribution that this dissertation has made to the topic. In chapter 4.1 there are the first thoughts about what program to develop. In chapter 4.2 the new target chosen is analyzed. In chapter 4.3 the developing process of the program is explained. In chapter 4.4 the functionality of the scanner program is described. In chapter 4.5 the functionality of the scanner_version_2 program is described. In chapter 4.6 the functionality of the scanner_version_3 program is described. In chapter 4.7 there are the advantages of the program. In chapter 4.8 there are the drawbacks of the pro-

gram. In chapter 4.9 there is the evaluation of the program. In chapter 4.10 some suggestions are made for better use of the program. In chapter 4.11 future work and enhancements for the program are included. In chapter 4.12 there is the conclusion about the program.

Chapter 5 contains the personal reflection and the personal thoughts about the topic of the dissertation.

Chapter 6 contains the conclusions after ending this dissertation and creating the scanner program. In chapter 6.1 is explained why digital forensics is different from any other topic. In chapter 6.2 are mentioned the lessons learned from developing digital forensics tools. In chapter 6.3 there are the overall conclusions and the final thoughts.

In the appendix there is the source code of the scanner.php, scanner_version_2.php and scanner_version_3.php programs.

2 Literature Review

A technical definition for digital forensics is the following: the tools and techniques that are used to preserve, recover and analyze digital evidence and data on digital devices or being transmitted by them. [3]

Digital forensics is a part of forensic science including the recovery and examination of evidence found in digital devices that are related to computer crime. [71] [18] Digital forensics investigations apply in many cases. The most usual is to check a hypothesis before the criminal or civil courts. Forensics are also used in the private sector; for example during internal investigations or intrusion cases. [24] There are many types of forensics: computer forensics, network forensics, forensic data analysis and mobile device forensics. [24]

Digital forensics are also used to verify evidence of the suspects, check alibis or statements, determine intent, identify sources, or authenticate documents. [85] Investigations have a wider scope of the other forensic analysis also including complex time-lines or hypotheses. [17]

Digital forensic process begins with the collection, duplication, and authentication of all the data before the examination begins. These first three phases have the biggest costs. Duplication is a standard practice for all laboratories but it takes great time which has become a big problem. One solution is the pre-examination techniques known as digital triage. These techniques help the prioritization and lead the examination. [16]

Digital triage in forensics investigation is a rapid growing sector with serious purpose, numerous implementations, multiple objectives and many achievements. There are many tools free and licensed and in the following paragraphs we are going to analyze four well known free tools Bulk Extractor [12], TriageIR [90], TR3Secure [89] and Kludge [46].

Computer forensics, also known as computer forensic science [60] is a branch of digital forensic science that refers to legal evidence stored in computers and other digital media. The aim of computer forensics is to analyze digital data forensically with the

target to identify, preserve, recover, analyze and present important information about these data. [21]

Since 1980 the computer crime has developed and grown radically. [49] Nowadays computer forensics investigates a great range of crimes, such as child pornography, fraud, cyber stalking, murder and rape. Computer forensics is also used in civil proceedings for information gathering. [21]

These techniques and knowledge are used to extract useful conclusions from a digital artifact; like a computer system, storage medium and electronic document. [99] The target of forensic examination can be from simple information extraction to rebuilding a timeline of events. [39]

In court the computer forensic evidence are required to have information that are authentic, reliably obtained, and admissible. [2] Many countries have developed guidelines and practices for evidence recovery. In United Kingdom, analysts use the Association of Chief Police Officers (ACPO) guidelines which help ensure the authenticity and integrity of evidence. [21]

Computer forensics process usually include four stages:

- Acquisition.
- Analysis.
- Evaluation.
- Presentation. [22]

Mobile device forensics is a branch of digital forensics, used in the recovery of digital evidence or data from a mobile device, PDA devices, GPS devices and tablet computers. [54]

The forensic examination of mobile devices is a relatively new field, starting from the early 2000s. The big spread of phones caused a bottleneck in the forensic examination of the mobile devices. [80]

2.1 Digital forensic process

Computer forensic examination most times uses the process of standard digital examination. [27] Examinations are executed basically on static data and not so much on "live" systems. This has changed from the way early forensic practices used to do. In that time the lack of special programs drove the examiners to work mainly on live data. In figure 2 we see the traditional process models. In figure 3 we see the computer forensics field triage process model (CFFTPM). [74]

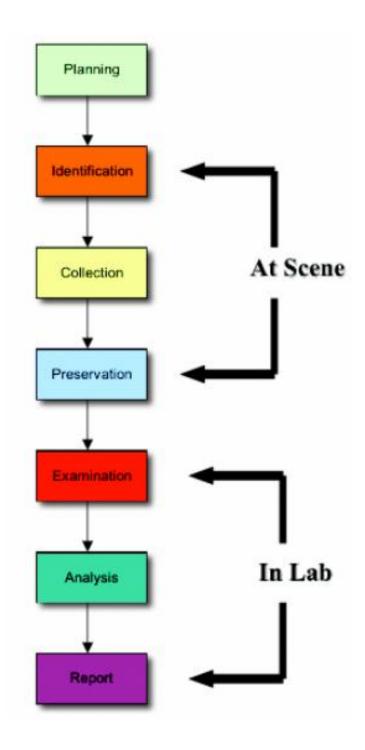


Figure 2 – Traditional Process Models [74]

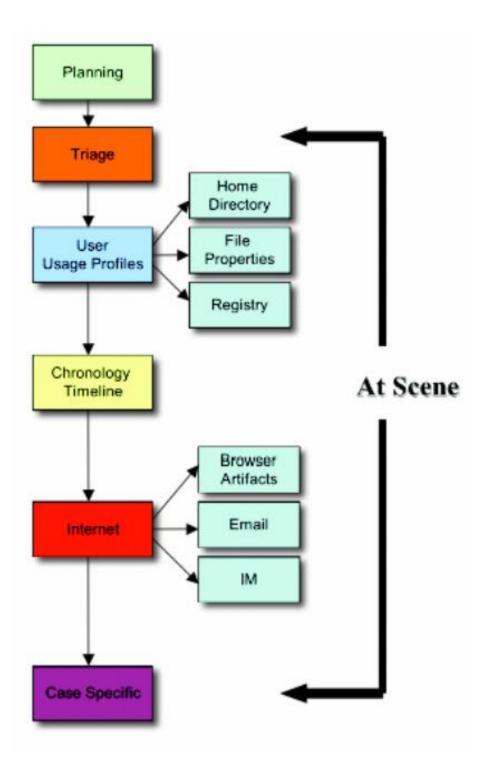


Figure 3 - CFFTPM Phases

2.1.1 Techniques

The techniques that are used in a computer forensics examination are the following:

1) Cross-drive analysis: Correlation of data being on different hard drives. [35] [98]

2) Live analysis: Examination of computers by using the installed operating system. This is achieved with custom forensics or sysadmin tools to gather all the information needed. This is crucial when we face encrypting file systems. [21]

3) Deleted files: The recovery of deleted archives. [64] Operating systems don't erase the physical data written on the hard drives. So analysts can reconstruct the information thought to be deleted. [21]

4) Stochastic forensics: This technique exploits stochastic properties of the computer to search for activities that don't have digital artifacts. The main use is to distinguish data theft.

5) Steganography: A method to hide information is by using steganography. This is the technique of hiding information inside a digital image or picture. This is mainly being used by criminals to hide pornographic content. Examiners by comparing hash values can understand if the image is the original. [26]

2.1.2 Volatile data

During the forensic process, when we shut down a computer, the data that are stored in RAM are disappeared. This is why we have to save them first. [20] Between other practices "live analysis" includes recovering RAM information before seizing a computer. [21]

After the seizure of the computer, RAM retains some electric current and this can help the examiner by using cold boot attack to regain some information. RAM retains this electric current for more time in very low temperatures. For example storing the RAM below -60 °C helps to achieve a successful recovery. But this is quite difficult to achieve while being at the scene. [41]

In order to extract volatile data correct, we must be at the lab, so as to take notice of the chain of evidence and to make our work easier. Some additional techniques to transfer a live computer is the mouse jiggler and the uninterruptible power supply (UPS) that provides the power. [21]

An easy way to save the data stored in RAM is to copy these data to a disc. [36]

2.1.3 Analysis tools

There is a wide number of open source and commercial tools for computer forensics examination. The forensic investigation gathers information from the media and the Windows registry. In addition tries to crack passwords and searches for keywords that have a relation to the crime under investigation. Finally retrieves e-mail addresses and texts and also pictures and video. [27]

2.1.4 Certifications

To achieve a forensics certification there is the ISFCE Certified Computer Examiner and the IACRB Certified Computer Forensics Examiner.

IACIS, the International Association of Computer Investigative Specialists, provides the Certified Computer Forensic Examiner, CFCE, course.

Nowadays most forensic software companies provide certifications on the programs they offer. An example is the Guardiancesoftware offering "EnCE" certification and AcCessdata offering "ACE" certification. [21]

2.2 Digital triage in forensics investigation

When an incident occurs, digital forensics processes are used to examine the incident, to collect and examine the digital evidence so as to evaluate the incident, identify a perpetrator and prove if a cyber-crime has been committed. [77] An incident can be caused by a human penetrator or by something irrelevant. Traces could be left anywhere. Here come the digital forensics investigation to search the digital crime scene and retrieve the aforementioned traces and evidence. [77]

Organizations nowadays have a specific IT security strategy to cover all the IT security and the other activities taking place in the organization. Until recently only law enforcement agencies were using computer forensics. But now many organizations use computer forensics to be protect by or examine cases for fraud, money laundering, pornography and harassment. [40]

A model depicting the forensic lifecycle could be the following:

- Identification.
- Authorization.
- Preparation.
- Securing and Evaluating the Scene.
- Documenting the Scene.
- Evidence Collection.
- Packaging, Transportation and Storage.
- Initial Inspection.
- Forensic Imaging and Copying.
- Forensic Examination and Analysis.
- Presentation and Report. [48]

In figure 4 we depict the IT Security fundamentals and in figure 5 we depict the Digital Forensics Investigation Fundamentals.

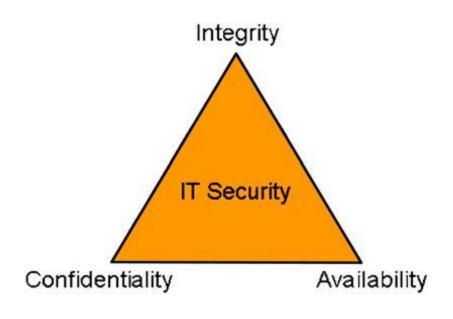


Fig. 4 – IT Security fundamentals. [73]

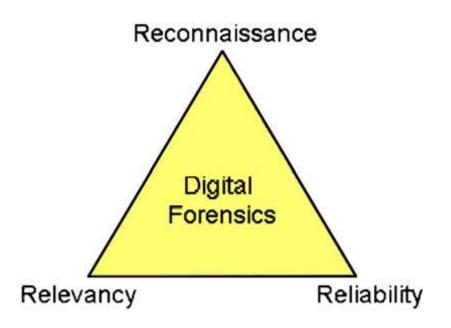


Fig. 5 – Digital Forensics Investigation Fundamentals. [73]

Digital Triage Forensics includes processes for examination of traditional crime scenes, digital crime scenes and battlefield crime scenes. [63] Digital triage collects digital evidence and processes in the first steps of investigation in order to identify what is useful and what not while being at the crime scene so as to lead the research to other possible and hidden evidence. All those evidence are meant to be used in a court of law so it is necessary to find them before they are lost or altered. So the triage tools, processes and scripts used must obey to all forensic principles to ensure the admissibility of the collected information and evidence. [77] The Association of Chief Police Officers, ACPO, has published a guide with the basic forensic principles under the name of Good Practice Guide for Computer Based Electronic Evidence. [1]

Since criminals use information and technologies from all around the world the examiners cannot work in the opposite way. The examination team must have collaboration of numerous and different members. [6] But this makes investigation even more complex and challenging. [8] These different nationalities, cosmopolitan backgrounds, socio cultural backgrounds, legal frameworks multiply the difficulties and makes the decision-making processes highly demanding. [80]

Many organizations don't take seriously the digital forensics [81]. But they have to understand that linking an attacker to a crime isn't something easy to achieve. Organizations must be prepared for digital forensic investigations and be sure that they have taken all the measures to be ready for such examinations. [38]

Internet has developed a great need for digital investigations. Computers are now used to commit company policy violations, e-mail harassment, murder, leaks of proprietary information, embezzlement, and even terrorism. [57]

In computer forensics most professionals have been self-taught. Computer forensics investigators examine mainly hard drives, CDs, DVDs, Flash memory devices, floppies, and tapes but they must also have deep knowledge of all the computer systems. [14]

ACPO Good Practice Guide has four principles. The number is small so as to be able every investigator to understand and remember them. The Principle 1 is: no change of data must take place. [1] The Principle 2 is: the examiner to be really competent and explain his actions. [1] The Principle 3 is: that an archive of all the actions made must be recorded. [1] The Principle 4 is; that the person in charge has all the responsibility. [1] The important aspect is to show to the court that the evidence collected from the digital crime scene is exactly the same as found from the first person reaching the crime scene. If there are alterations, augmentation or decrement to the digital evidence collected data. [1] The problem with the programs used nowadays is that they often alter the data and it is crucial for the investigator to find and monitor all the alterations. Objectivity, continuity and integrity when possessing the evidence is a high priority. The tools applied must collect evidence starting from the volatile to the less volatile. [7]

In the ForensicArtifacts.com database the investigator can find potential forensic artifacts so he knows what to look for. [28] There is also the SANS resources such as the Sans Digital Forensics and Incident Response Poster-2012 or Sans forensic cheat sheets that include such information. [47] For example if we have a child pornography crime the browsing history, favorites and browsing information is the place to look for. It is important for the investigator to put some priorities before he starts collecting the data. Proper prioritization can save time, help him find evidence before they are lost, avoid mistakes and make a concrete and well monitored investigation. Data with small life time like processes, routing tables and temporary files should be a priority. [74]

In incident response there is a choice to be made. Whether to perform a complete memory acquisition or a live response. Complete memory acquisition is the analysis of the computer's physical memory with a number of tools. Some memory imaging tools are Crash Dumps, LiveKd Dumps, Hibernation Files, Firewire and Virtual Machine Imaging. [96]

Live incident response collects evidence from a computer so as to prove if an incident took place. Live incident response includes the gathering of volatile and nonvolatile data. Volatile data is data that would be lost if we cut the power off from the computer. Nonvolatile data is don't get easily lost and include useful information for digital forensic collection such as system event logs, user logons, and patch levels, among many others. Live incident response further includes the collection of information such as current network connections, running processes, and information about open files. To collect live incident response data we run commands that produce data that are send to a different storage device than the console. [72]

Memory acquisition is slow. [1] The modern hardware has big memory that includes data of past and completed processes. These data cannot be collected by the live response tools. [4]

The first responder will find live response useful if he is well prepared for the case under examination. [93] For best results both practices need to be applied.

From all the above we understand that a triage tool must comply with a number of requirements, have performance, low complexity but great adaptability.

In the following chapters we analyze, evaluate and compare four open-source triage tools used in digital forensics and incident response, assess their behavior and conclude telling if they fulfill the purpose of the forensics analyst and remark any needed enhancements.

2.3 Testing triage tools

In the next paragraphs we test four open-source triage tools, to evaluate their behavior, their validity and conclude how useful they are for the first responder.

The four triage/incident response tools that we are going to analyze are Bulk Extractor [12], TriageIR [90], TR3Secure [89] and Kludge [46]. We tested their abilities in Microsoft Windows operating systems because based on statistics they are the most widespread operating systems for both examiners, users and criminals. [58].

To help us test TriageIR, TR3Secure and Kludge we used Windows 7 with VMware Player 8 installed including 8 different Windows OS systems. [77] Also Sandboxie 3.74, was installed. [15] [76]

We copied TriageIR v.79, Kludge-3.20110223 and TR3Secure on "E: disk" so as to use and simulate this partition as an external USB drive, as a forensic examiner would do. [77]

The tools were executed with all their options enabled in a sandboxed environment and normal environment. [77] The sandboxed environment was necessary to help us see which files are created or altered in the users system. [77]

2.4 Bulk Extractor

Bulk Extractor [12] is written in C++. It scans a file, a disk image, or a directory without parsing the file system. In addition Bulk Extractor makes histograms of features because features that are more common are more important. [10] This tool is useful for law enforcement, defense, intelligence, and cyber-investigation applications. [11]

Bulk Extractor is also usefull for digital archivists. [13] Bulk Extractor has a GUI interface, the Bulk Extractor Viewer utility. Process of the results can be achieved by using the digital forensics tools in the Bit Curator environment. [13]

2.4.1 Advantages

Bulk Extractor advantages are the high speed and thoroughness. This happens because it ignores file system structure. Bulk Extractor has the ability to examine different parts of the hard disk in parallel. Bulk Extractor is thorough because automatically detects, decompresses, and processes compressed data that have been compressed by numerous algorithms. [11] Another advantage is that Bulk Extractor can process any digital media. It can process hard drives, SSDs, optical media, camera cards, cell phones, network packet dumps, and other kinds of digital information. [11] Also it can recover more high-value forensic information than other tools. [31] Bulk Extractor is easy to use and this is why it has been used by numerous law enforcement organizations, and its acceptance spreads. [30]

2.4.2 Drawbacks

When using Bulk Extractor every media that will be examined is connected to a write-blocker of an investigator workstation and then it is processed with the Bulk Extractor tool. To start all this examination there is some time needed. Around 5 min per media. The Bulk Extractor is executed recursively without needing the attendance of the investigator, but the time needed to complete all its operations is big. [30] So Bulk Extractor works additionally to the traditional forensic procedures and its target is not to replace them. [30]

2.5 TriagelR v.0.79

When we read the manual of the TriageIR tool we see that it needs some tools added in a folder named tools which is located in the program's folder. The tools needed are: a) DumpItmemory utility [25], b) Sysinternals Suite [87], c) RegRipper [70], d) MD5deep and sha1deep [51], e) 7Zip Command Line [100]. TriageIR has 6 tabs – pages that contain all the options, see Fig. 6. In most cases the tool worked fine. [77]

The modifications that the tool makes to the computer under examination are justifiable and thus can be explained which helps to be defended in court. [77]

File Help														
System Information	Network Information	Registry	Disk Information	Evidence Collection	Options									
System Informatio	n													
Capture Processe	S													
Capture Services														
 Associated Services Scheduled Tasks Information Hostname Information AutoRun Information 														
									Account Settings					

Fig. 6. TriageIR v.79 GUI.

2.5.1 Advantages

TriageIR can collect information about the startup process of the computer that is useful for malware examination. [78] Also TriageIR creates MD5 and SHA-1 hashes of evidence files. [77] This is crucial because it can prove the integrity of the evidence information.

2.5.2 Drawbacks

TriageIR during execution produced some errors that are due to programming faults or incompatibility of the utilities with the operating systems. TriageIR does not gather any Netbios evidence and has a problem in collecting all the event log information. [77] TriageIR has also problem collecting the security registry hive, the hard disk's directory structure and other information from the examined computer.

2.6 TR3Secure

TR3Secure data collection script uses Windows tools and tools that must be downloaded from the internet. Furthermore a .txt file with commands must be inserted in the tools folder of the program.

We chose option 4 from the tool's menu, see Fig. 7, so as to exploit all its abilities. [77] The tool did what expected in all operating systems. [77]

Like TriageIR the changes made are justifiable, they can be explained and so to be defended in the court. [77]

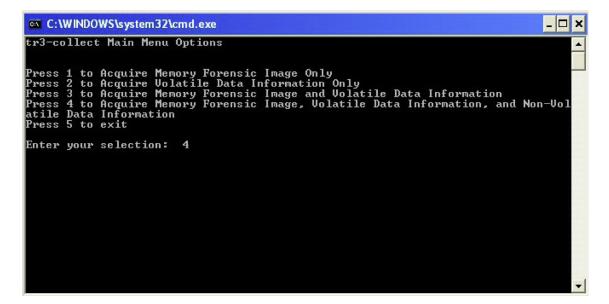


Fig. 7. TR3Secure Main Menu.

2.6.1 Advantages

TR3Secure from a forensics view has all the functions needed including the choice to insert the case name, the examiners information, the path for storage and the execution date and time. Furthermore it records all the triage process so as to help the investigator find any errors produced.

2.6.2 Drawbacks

When we run the tool many errors occurred. The most important is that it fails on 64-bit operating systems. [77] In Windows 7 64-bit was not able to find the tools folder. [77] Also when it was executed in operating systems that used different codepage the results created needed a specific viewer to be read. [77]

2.7 Kludge 3.20110223

Kludge in the startup screen provide us 3 options (figure 8). The first is to perform simple analysis. The second is to perform a detailed analysis including timeline and registry analysis. The third is to perform the above and memory and process captures and file hashes.

Kludge was originally developed to be executed remotely by a network. This would be achieved by exploiting the administrative shares of the computer under examination. So Kludge copies all the information needed in the target computer and then it executes them. This is not a very good forensics practice because the changes to the target computer are massive. Also the administrative shares must be enabled. [77] Another option is to execute Kludge from a USB drive and save all the reports in the USB drive. [77]

When we run the Kludge by using the network the alterations to the target computer are explainable but not justifiable and so they cannot be accepted in a court. [77] But the new altered version of Kludge that was executed from a USB drive don't have this major disadvantage.

🖬 [#] C:\Windows\system32\cmd.exe [#]
<pre>[#] C:\Windows\system32\cmd.exe [#] Running Kludge Analysis version 3.1 Please enter the following information An Option Level (1-Simple Analysis, 2-Detailed including Timeline and Registr y Analysis, 3-Includes Memory and Process captures and file Hashes) An associated Ticket Number. If there is no ticket number associated, please enter 0 or none The Analyst's name (e.g. john) The Targeted Remote Machine Name (files will be copied to c:\Windows\Temp\ana lysis Your Admin Account Username (You will be prompted for your password twice) A Local folder name on this machine where you want the final report to be cop ied to. Quote directories with spaces (e.g. "c:\Documents and Settings" or simp ly put a period for current directory) Enter 'yes' or 'no' for GPG encryption. If 'yes', you will need your GPG Pub lic key in a file called "pubkey.txt". The script can decrypt the Report if the Private Key is already installed on the current machine or exported to an ascii text file called "privkey.txt" Enter 'yes' to have the script query a remote text file for previous incident s If Querying a share enter the share's path (e.g. \\192.168.1.2\Reports\incide </pre>
Enter an Option Level (e.g. 2): 3 Enter the Remote Machine Name:

Fig. 8. Kludge script execution.

2.7.1 Advantages

Kludge is able to collect useful information that TR3Secure and TriageIR cannot. Something important for the investigator is that it collects internet history from Mozilla Firefox and Internet Explorer browsers. This is helpful in cases like grooming, bullying, spam, and other. [77] In addition it collects antivirus logs, firewall state, process dumps and memory information of running processes. [77] By creating timelines of running processes as being executed adheres to ACPO principles. [79] Furthermore the report is concentrated in a well organized html file from where the examiner can have an overview of the collected evidence. And in his way simplifying and speeding up the triage work.

2.7.2 Drawbacks

Kludge when executed produced out-of-the-box errors, programming faults and incompatibility of the utilities. It also collects only specific antivirus logs. [77] Symantec and McAffee antivirus programs share only 15% of the market. [61] It also does not collect event logs in Windows Vista, 7 and 8 operating systems. [77] Since Kludge doesn't record an analytic log of all the processes executed it is hard to make checks and comparisons. [77] Like TriageIR does not remove added registry keys.

2.8 Synopsis

After running and testing the four tools and having found their advantages and drawbacks we come up to a synopsis about their performance.

2.8.1 Bulk Extractor

Bulk Extractor collects credit card numbers, email addresses, URLs, and other kind of information from any digital media. The tool can be executed on different data formats and collects much evidence concerning internet. Also it can detect and decompress data that have been compressed by using many different algorithms. [86] Bulk Extractor also uses GNU flex. [88] When all the evidence have been collected Bulk Extractor creates a histogram of useful features. Stop lists can also be applied. [30] In figure 9 there is an overview of the tools architecture. A graphical user interface helps the investigator to view the reports created. [30]

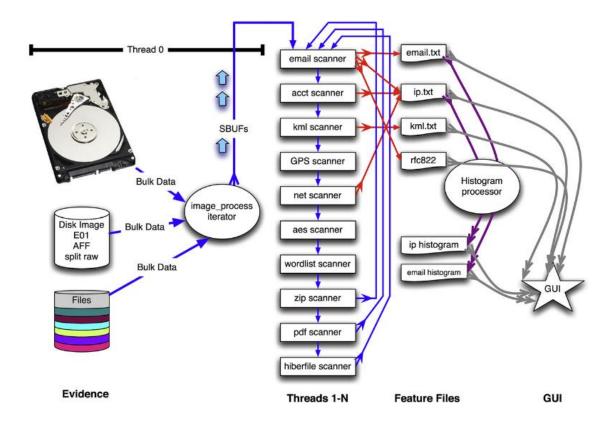


Fig. 9 Diagram showing overview of the Bulk Extractor architecture. [30]

Bulk Extractor constructs a report that have: [11]

- Credit card information.
- IP addresses found.
- Ethernet MAC addresses found.
- EXIFs from JPEGs and video segments.
- Credit card numbers.
- US and international phone numbers.
- URLs from browsers and emails.
- Email addresses.
- A histogram of terms used for internet searches.
- A list with words for password cracking.
- The wordlist in a form to be used by password-cracking programs.
- Internet domains found.
- Information about ZIP files.

• Results of specific search requests.

For all the above, two files are also created: [11]

- A stop list or a list of information not to be shown to the user.
- Histograms of features with appearance frequency.

Bulk Extractor additionally creates a report. An XML report with information concerning the source data, the compilation and execution of the tool, time used for processing and additionally includes all the evidence found. [11] Bulk Extractor is very helpful for triage. It aids to put priorities before the thorough examination begins. [30]

2.8.2 TriageIR, TR3Secure and Kludge

None of the triage tools TriageIR, TR3Secure and Kludge inform the user that has to run the tools as administrator in Windows Vista, 7 and 8 operating systems in order to work properly. [77]

In Table 1, Table 2 and Table 3 we see a picture of the incident data that the above three tools were able to collect when they were executed during the triage process. [77] The column headers of the table indicate the order of volatility scale, and the row headers show the tools tested.

Table 1 Collected forensic artifacts [77]

Tested tools - collected forensic artifacts vs. order of volatility scale.

der of volatility (from more v	volatile to less volatile) \downarrow	TriageIR 0.79	TR3 Secure	Kludge 3
gisters and Cache	No data collected	Х	Х	Х
uting table, arp cache,	Network-related data \rightarrow ARP cache	Х	Х	х
process table, kernel	Network-related data \rightarrow Routing table		Х	Х
statistics, memory	Network-related data \rightarrow DNS cache and resolution		Х	
	Network-related data \rightarrow DNS Information	Х		Х
	Network-related data \rightarrow A records			Х
	Network-related data \rightarrow Host file			х
	Network-related data \rightarrow Netbios routing table	Х		Х
	Network-related data \rightarrow Netbios information (sessions,	Х	Х	х
	connections, file transfer over netbios)			
	Network-related data \rightarrow Port to process mapping		Х	
	Network-related data \rightarrow TCP/UDP active connections	Х	Х	х
	Network-related data \rightarrow TTL			х
	Network-related data \rightarrow Firewall (info, status)			х
	Process data \rightarrow Process File Handles	Х	х	х
	Process data \rightarrow Running Processes-DLLs	х	х	х
	Process data \rightarrow Services			х
	Process data \rightarrow Process to exe mapping		х	
	Process data \rightarrow Process to user mapping		х	
	Process data \rightarrow Child processes		Х	
	Process data \rightarrow Process dependencies		х	
	Process data \rightarrow Process dumps			х
	Process data \rightarrow Process memory			х
	User's activity → Active logon sessions		х	
	User's activity \rightarrow Logged on users	Х	х	х
	User's activity \rightarrow Recent files	Х		
	User's activity \rightarrow Internet browsers history			х
	User's activity \rightarrow Jump lists Files	Х		
	User's activity \rightarrow Clipboard-contents		х	x
	Registry hives \rightarrow Sam	Х		х
	Registry hives \rightarrow Security	Х		х
	Registry hives \rightarrow System	X		x
	Registry hives \rightarrow Software	х		х
	Registry hives \rightarrow HKCU	х		x
	Registry hives \rightarrow NTUSER.dat	Х		х
	Registry hives \rightarrow USRCLASS.dat	Х		x
	Various timelines \rightarrow IE Timeline			x
	Various timelines \rightarrow FF Timeline			х
	Various timelines \rightarrow Hard disk timeline			x
	Various timelines \rightarrow Prefetch info			x
	Various timelines → Recycle Bin timeline and contents			x
	Memory image			x
	System configuration \rightarrow VSS service status			Х
	Prefetch files	Х	X	
	NTFS data streams		X	Х
	UnSigned-executables \rightarrow Uptime		Х	
	Table 2 Collected forensic artifa	cts [77]		
Temporary file systems	System event logs \rightarrow evt files System event logs \rightarrow evtx files	x x		х
	Processed event logs \rightarrow System	x		Х
	Processed event logs \rightarrow Security	X		x
	Processed event logs \rightarrow Application event logs	x		x
	Antivirus logs			х
	No data collected		х	
Disk Remote logging and	Not applicable	х	x	х
monitoring data that	Network-related data \rightarrow Open shared files	x		
is relevant to the	User's activity \rightarrow Remotely logged on users		х	
system in question	User's activity \rightarrow Remote users IP-addresses		x	
	No data collected			Х
Physical configuration,	Network-related data \rightarrow Network configuration	х	х	~
network topology	Network-related data \rightarrow Network Adapter info			х
in the second	Network-related data \rightarrow Routing table	х		X
	Network-related data \rightarrow Host File	x		x
	Network-related data \rightarrow Enabled network protocols		х	

	riocessed event logs - security	~		
	Processed event logs → Application event logs	х		
	Antivirus logs			
	No data collected		Х	
isk Remote logging and	Not applicable	Х	Х	
monitoring data that	Network-related data → Open shared files	Х		
is relevant to the	User's activity → Remotely logged on users		Х	
system in question	User's activity → Remote users IP-addresses		Х	
	No data collected			
hysical configuration,	Network-related data \rightarrow Network configuration	Х	Х	
network topology	Network-related data → Network Adapter info			
	Network-related data \rightarrow Routing table	Х		
	Network-related data \rightarrow Host File	Х		
	Network-related data → Enabled network protocols		Х	
	Network-related data \rightarrow Promiscuous adapters		Х	
	User's activity \rightarrow Logged on users	Х		
	System configuration \rightarrow User accounts policy	х		
	System configuration \rightarrow User groups		Х	
	System configuration \rightarrow Startup information	Х	Х	
	System configuration \rightarrow Directory structure	х		

Table 3 Collected	forensic	artifacts	[77]
-------------------	----------	-----------	------

order of volatility (from	more volatile to less volatile) \downarrow	TriageIR 0.79	TR3Secure	Kludge 3
	System configuration \rightarrow Mounted disks information	Х		
	System configuration \rightarrow Hostname	Х		
	System configuration \rightarrow Local shares	Х		х
	System configuration \rightarrow Schedule tasks	Х		х
	System configuration \rightarrow Kernel build	Х		
	System configuration \rightarrow Register organization	Х		
	and owner			
	System configuration \rightarrow OS-version		Х	
	System configuration \rightarrow Group policy listing and RSOP		Х	
	System configuration \rightarrow Installed software		Х	
	System configuration \rightarrow Security settings		Х	
	System configuration → Hardware devices		Х	
	System configuration \rightarrow Number of processors	х		
	and their type			
	System configuration \rightarrow Amount of physical memory	х		
	System configuration \rightarrow System's install date	х		
	System configuration \rightarrow System variables	X		
	System configuration \rightarrow System configuration			х
	System configuration \rightarrow Firewall configuration	х		
	System configuration \rightarrow Services	X		
	System configuration \rightarrow Type of installation	х		
	System configuration \rightarrow NTFS partition info	X		
	Certain applications \rightarrow Version and Signing			х
	info for Acrobat			
	Certain applications \rightarrow Acrobat Reader			х
	Certain applications \rightarrow Flash			x
	Certain applications \rightarrow Java			x
	Certain applications \rightarrow Firefox			x
	Certain folders structure \rightarrow Program Files			x
	Certain folders structure \rightarrow Documents and Settings			x
	Certain folders structure \rightarrow Windows			x
	UnSigned-Executables \rightarrow Computer name			x
	UnSigned-Executables \rightarrow Autoruns			x
	UnSigned-Executables \rightarrow Startup apps			x
	UnSigned-Executables \rightarrow BHO's			x
	UnSigned-Executables \rightarrow Hotfixes and service packs			x
	UnSigned-Executables \rightarrow Environment Variables			x
	UnSigned-Executables \rightarrow Uptime			x
	UnSigned-Executables \rightarrow Operating			x
	System Information			^
				х
	UnSigned-Executables \rightarrow Drive Information UnSigned-Executables \rightarrow Partition info			x
				x
	UnSigned-Executables → Users			
	UnSigned-Executables \rightarrow USB device history			X
- the second	Registry files	V	N	X
rchival media	Not applicable	х	Х	Х

The contents of a hard disc usually are examined in the lab so there is no use to analyze them in the triage process. [77] In Table 4 we see how effective each tool is in different operating systems. [77]

Table 4 Tool effectiveness [77]

Tool	Win XP SP3 32 bit	Win XP SP2 64 bit	Win 7 32 bit	Win 7 SP1 32 bit	Win 7 64 bit	Win 7 SP1 64 bit	Win 8 32 bit	Win 8 64 bit
TriagelR 0.79	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium
	effective	effective	effective	effective	effective	effective	effective	effective
TR3Secure	Medium effective	Ineffective	Medium effective	Medium effective	Ineffective	Ineffective	Medium effective	Ineffective
Kludge 3.20110223	Medium	Less	Less	Less	Less	Less	Less	Less
	effective	effective	effective	effective	effective	effective	effective	effective

In Table 5 we see the alterations caused by TriageIR, TR3Secure and Kludge on the registry and file system of every operating system. These alterations were captured with the help of Buster Sandbox Analyzer 1.87 and Sandboxie. [77] The version of the Kludge tool, that was changed to be used by a USB drive, was the most forensically correct of all the above triage tools. [77]

Table 5 Modifications produced [77]

OS	Tool		
	TriageIR	TR3Secure	Kludge (modified version
Win XP SP3	FM ^a : 39 (mainly prefetch and /system32/CatRoot)	FM: 13 (one in /system32/)	FM: 0
	RC: 33	RC: 21	RC: 4
Win 7 64 b	FM: 84 (mainly prefetch and logfiles)	FM: 4 (mainly logfiles)	FM: 1 (temp appdata)
	RC: 379	RC: 71	RC: 6
Win 7	FM: 39 (prefetch and user appdata)	FM: 26 (mostly in prefetch, one in /system32/)	FM: 1 (temp appdata)
	RC: 134	RC: 131	RC: 14
Win 8 64 b	FM: 138 (prefetch and user appdata)	FM: 45 (mostly in /INF folder)	FM: 0
	RC: 354	RC: 73	RC: 6
Win 8	FM: 29 (prefetch and user appdata)	FM: 19 (2 in /system32/)	FM: 1 (temp appdata)
	RC: 131	RC: 127	RC: 8

^a FM: File creations/modifications – RC: Registry changes.

Summing up all the above we see that it is obvious that a triage tool have to be balanced in numerous requirements, including performance, complexity and adaptability so as to be effective and successful during the triage evaluation.

2.9 Suggestions

The four triage tools analyzed before could be adjustable in two ways: First before the execution to avoid as many errors as possible and second during the acquisition to achieve the maximum effectiveness. [77]

If we disable Prefetch on Windows the modifications created will be even less. [77] Furthermore the tools should record all the actions executed including errors and problems. [77] In addition it is advisable the tools to log and restore all registry modifications. Finally it is important that the tools enhance the collection of all history and internet activity information of all widely used browsers.

2.9.1 Bulk Extractor

Bulk Extractor is a command line tool. [31] An advanced GUI could be used for easier and faster use, even from people with little experience and a GUI for the results found. With the current version it is possible to run multiple copies of Bulk Extractor on different machines but there is no way to easily recombine the results. [31] A good direction would be to solve this problem and improve the combined functionality. Also we can extend Bulk Extractor with numerous plug-ins.

2.9.2 TriagelR 0.79

This tool must overcome problems that are encountered when it is used in different operating systems. It seems to work properly only in Windows XP and faces problems in the other releases. [97]

2.9.3 TR3Secure

This tool has compatibility problems with Windows 64bit operating systems so modifications must be made to overcome this problem. In addition it must be enhanced with capabilities such as collection of scheduled tasks, registry files, installed printers, peripherals, user logons and internet activity information. [77]

2.9.4 Kludge 3.20110223

This tool was created having in mind specific antivirus and security products. But it must broaden its use and target machines. Some other enhancements are to run from a USB stick or an external drive and save the reports there. Additionally some functions have to be altered in order to be able to execute in Windows 7 and 8 operating systems. [77]

2.10 Future work on the four tools

As it is understood from the above analysis there is no tool to cover all the purposes, be very effective and be the best for triage process. This result was obvious because there is high variety and complexity on modern media and systems. The complexity and the variety in the needs, the software and processes are increased radically so the examiner must have a wide portfolio of different tools to manage and handle every different case. [77]

In order to help the examiner choose the portfolio of tools we can put some qualitative and quantitative metrics. [77] After the examination of the four triage tools, we could apply these three metrics:

1) Effectiveness.

- 2) (Un)reliability.
- 3) Invariability. [77]

The use and the connection between these metrics could be a good field for future research.

Also in the future we could try to assess the tools in terms of usability, usefulness, exploitable results, validity and evaluation of reports and case-by-case analysis. [77] A future target would be to create an advanced triage tool based on the four tools mentioned above that would combine all their advantages , functions and options and none of the drawbacks.

An enhancement for Bulk Extractor would be to develop an algorithm, for distinguishing compressed data from encrypted data [33], and additionally present the percentage of encrypted data on the digital media that is under examination. [30]

The reports of Bulk Extractor can be useful when they are compared and contrasted to other data of forensic practices, for example, cross-drive analysis information. [59]

3 Problem Definition

Computer abilities and capabilities have grown radically since 1960, and they are going to develop exponentially in the future. Storage capacity has grown beyond any expectation and there is no limit for the future. [62] FBI's statistics state that the data for analysis per case have multiplied 6.65 times, from 84 GB to 559 GB, in eight years, from 2003 to 2011. [69] The expanded computing capabilities makes processing and storage cheaper. This makes the forensic examination even harder with more compute resources needed. Although this problem is known, little has been done to confront it. The blame is on both users and developers. [75]

In the triage process first we have to put priorities before starting the collection of data. Great importance must be given to the data that live for a short time like routing tables, temporary files and processes. Forensic analysts have to have a wide number of tools because no tool can apply to all the different cases. [74] So the triage tool must be flexible be able to change its functionality depending on the evidence. [77] The triage tool must collect data in very short time but this is many times overlooked. This disadvantage derives from the fact that triage tools come from traditional forensic tools which were designed to conduct the analysis at a future time. [44]

The processing speed of current digital forensic tools is not a match for the average cases because users don't have specific performance requirements and developers haven't put performance and latency to a top-level objective. [75]

SPEKTOR triage tool includes some automation, but this is done in order to be used by people who have no specific technical skills. [82] This is in violation to ACPO's second principle and this is why it is considered to be a poor practice. [77]

In the next chapters we are going to analyze the most important problems of the four tools tested before.

3.1 Bulk Extractor

Bulk data analysis has the limitation that compressed data that are fragmented into many locations are difficult to recover. However, most interesting files in forensic manner are not fragmented. The only exception is log files. [34].

Unicode and non-Latin characters create problems for bulk data analysis. One other complication is that there are many types of localized strings that are possible to be found. [30]

3.2 TriagelR v.0.79

The tool failed only in Windows 8 OS 64 bit. [77] When the tool runs its utilities create and change many files. These alterations are undesirable. [77]

By analyzing the execution and results we see that the tool violates a number of forensic principles. First of all some utilities of the tool need a hard disk partition letter as a parameter to execute properly. [77] Also when executed the tool adds registry keys but does not undo these registry alterations. Furthermore it does not record all executed commands in the created incident log file. In this way the analyst doesn't know which commands executed correctly, which failed and why. [77] Traceability is hard to achieve because the tool uses a separate command shell for each utility called. This ends after the execution and this makes the examiner not to acknowledge the errors that have been created. [77] The tool should create hashes of the reports, so as to have a complete and correct chain of custody for the data that have been either gathered or produced by the tool. Finally, when the compression ability of the tool is used, some data are not gathered. [77]

3.3 TR3Secure

Like TriageIR, the utilities used by TR3Secure alter some Windows OS files. This happens also with some temp and recent activity files. [77] In all operating systems

TR3Secure loads drivers in certain folders, alters or adds registry keys, creates or modifies folders. Finally when some utilities fail to execute the crash reports are created in specific folders. [59] [77]

3.4 Kludge 3.20110223

Kludge in all operating systems applied adds and alters registry keys, creates or modifies files, try to install drivers and changes Prefetch and the users' temp files and recent activity. [77]

Kludge uses the Hobocopy utility [43] to copy files. This utility crashed in Windows 7 and 8 OS, causing the registry files and event logs not been collected. Moreover many utilities used by Kludge in Windows 7 and 8 OS, crashed. Finally some utilities didn't execute at all in the above operating systems. [77]

4 Contribution

This paper contributes in both the theory and practice of digital forensics. The purpose is to study and analyze, the way four free triage tools work and respond during the process of installation and execution. Also highlight the advantages and drawbacks and make suggestions for improvements and better performance. Finally develop a program to help the first responder make the digital triage fast and in an easy, concrete and meaningful way.

4.1 First thoughts

The first thought was to use one or more existing tools and change the presentation of the results that they provide, when they are used for digital triage. The purpose would be to improve the results by making them more helpful and beneficial for the investigator. The target would be to ease the forensics analyst and provide him an overview with a glimpse. Help him take the right decisions fast. Demonstrate and present the contents of the hard disc in a way that helps the investigator have a more concrete image of the contents of the disc. Provide visualization, analysis and evaluation with the use of diagrams, bars, pies, percentages, images and other presentation tools.

The way to do all the above was the following: Find as many sources as possible and bibliography. Read papers, articles, published material by accredited scholars and researchers. Search the internet. Search for digital triage tools and how the presentation can be improved. Find for digital triage in forensics investigation definition, categories and characteristics, scopes, goals, objectives and achievements. Find the existing tools and what things to consider when choosing the right tool. Find regulations globally and in Greece. Find what existing tools provide, what they don't offer and why this lack is important. Why the lack of a proper and advanced presentation is so important. Make a gap analysis. Search for drawbacks and possible contribution. Improve the visualization, analysis and evaluation with the use of diagrams, bars, pies, percentages, images and other presentation tools.

The first thought was to help the child pornography examiner. After taking an image from the hard disk, the RAM and the volatile data, then provide him with the history from all the browsers that are installed on the computer. While he is at the scene it is crucial to recover everything that is related to the examined case. When a suspect searches for child pornography in the internet or stores digital files, containing this child pornography material, many traces are left behind. The most possible scenario is that the suspect won't have great programming skills and knowledge to create a script to delete, every time, the browsing history and the evidence from all the browsers in his computer. So during the triage process, the program that I would create, would be able to collect all the evidence from the web browsers, specify attributes that stand out and present them in a useful and easy to understand way, to help the examiner.

One first approach was to use a widely available open source tool, Kludge, that collects digital evidence that the other two tools TR3Secure and TriageIR do not. It can collect internet browsers history from Mozilla Firefox and Internet Explorer. Some modifications could be made to be more focused on the latest versions of the browsers. And this because the browsers pop up often messages, to the users, to download the latest versions available. It is rare for a user to decline these prompts all the time and use a very old version of the browsers. Knowing the browsers history is crucial when the examiner searches for grooming, bullying, spam, and so on. But also Kludge can collect antivirus logs and reports of the firewall state. In addition it can collect process dumps and process-related memory for each running process. In the end Kludge produces an html file with a well organized menu which help the examiner navigate the collected digital evidence. This can simplify the work of the examiner and speed up the triage process. To enhance the usability and presentation of the tool one thought was to add statistics, diagrams, bars, pies and percentages to the reports, which could be navigated through the html file. Kludge produces .txt files for the reports. So the purpose of the new program would be to read these .txt files and produce more complicated reports with all the statistics, diagrams, bars, pies and percentages mentioned above.

However there was a major turn over in the development of the program. After reading all the sources cited in the bibliography and many more, the conclusion was that there are some tools freeware and licensed that present their results using visualization, analysis and evaluation including the use of diagrams, bars, pies, percentages, images and other presentation tools. Such a tool is Spektor. So the new thought was to develop a tool, that would be very simple and easy to use, for the first responder, to exploit it for digital triage in the crime scene but also helpful during the analysis at the lab.

4.2 The new target

After all the above the second thought was to make a program that could search the targeted computer and find the added files, altered files, infected files or even malware constructed by the suspect.

At start, the new target, was to make a program that would search the computer under investigation for the files we want to find. To have the ability to choose the type of files we want, the domain of the computer to search in, the file the results would be saved in. The results file would show the name and the path of the files found.

The next step was to find all the MD5 hashes of the files we wanted. This could help to find which files were modified (ex .exe files for windows) in comparison to the original ones. This could be done by producing the MD5 hashes [50] of the files found and compare them with the MD5 hashes of the original files (which are unaltered).

In the next stage the above program was necessary not to be hard coded (the parameters not to be fixed in the code) but to offer the examiner the ability to insert the desired values as parameters during the execution:

1. The path where the program to search in.

- 2. The type of files the program to search for.
- 3. The name of the file with the results.
- 4. The path of files to be compared.

5. Where the reports with the name of the files, the path found and the MD5 hash to be saved in.

During the development many features were added, the program was upgraded many times and became more complicated, until it reached its final form presented below. The final program has the following functionality: The user by using the command prompt can choose: a) to see the help guide of the program b) to scan a specific domain, retrieve the files chosen and create their MD5 values and c) compare the created MD5 values of the files chosen with a file containing the "clean" MD5 values of unaltered files that he wants to compare.

1. The user first inserts the option "help", "scan" or "compare".

2. In case of "help" the programs functionality is shown.

3. In case of "scan" without putting any parameters the default values are used.

4. In case of "scan" with parameters the inserted values are used to set a) the path for the program to search b) the extension of the files being searched and c) the path where the results file to be stored.

5. In case of "compare" the parameters are necessary. The values inserted are used a) to set the path for the file containing the MD5 of thescanned files b) the path for the file with the clean MD5 values and c) the path where the results file to be stored.

4.3 The developing process

The first attempt was to use the programming language VBscript for developing the program. [91] [92] Also there were thoughts to use the programming language Python because it is widely used for applications concerning security and digital triage. [67] [68] The final decision though was to use the programming language PHP because I had better knowledge of this language, I had use it extensively before, I knew its capabilities and the belief that I could accomplish the program till the end was strong. [65] [66]

The editor I used to write the PHP scripts was the Sublime-text editor. [84] [85] A server was used, the Wamp Server, to run the program locally and see the results, because the program doesn't have a web interface. [94] [95] So in order to run the PHP program there is a need to install PHP and a server on the examined computer. But in order to adhere to the ACPO principles there was a need to minimize the changes to the computer under investigation. To bypass this problem Bamcompile was used to convert the PHP application to standalone .exe application. [5] By transforming the *.php program into a *.exe file we give the ability to the investigator to run the program from a USB stick using only the command prompt of the computer. No need for php dlls and installations that alter the computer files system. Bamcompile is a freeware. To use Bamcompile you have to visit the site http://www.bambalam.se/bamcompile/ and download the win 32 zip. You extract this zip file wherever you want, for example at the desktop. In this folder you insert the scanner.php file. You open a command line prompt and write the following:

"cd C:\Users\nikos\Desktop\bamcompile1.21". After this you write in the cmd:

"bamcompile scanner.php" and in the same folder with the scanner.php the file scanner.exe is created and is therefore ready for use.

4.4 The scanner program - How it works

The program's name is scanner.php and the standalone .exe application is scanner.exe. If the examiner wants to run the scanner.php program, first he must install a server to run it locally at the computer, like the Wamp Server, and put the scanner.php program into the www folder of the directory of the server. Then in order to run it (this is for use with Wamp Server) he must open a command line prompt and open the folder of the server where php is located, for example: cd C:\wamp\bin\php\php5.4.16\. Then depending on what he intends to achieve he can type:

1) .\php.exe C:\WAMP\www\scanner.php

2) .\php.exe C:\WAMP\www\scanner.php help

3) .\php.exe C:\WAMP\www\scanner.php scan

4) .\php.exe C:\WAMP\www\scanner.php scan --path="C:\\" --extension="exe" -- log_file="C:\WindowsMD5\Cexe.txt"

5) .\php.exe C:\WAMP\www\scanner.php compare -log_file="C:\WindowsMD5\log.txt" --MD5_values_file="C:\WindowsMD5\clean.txt" --results_file="C:\WindowsMD5\results.txt"

The MD5_values_file must be a .txt file, with the created MD5 values from the scan option, from files that are clean and secure. The folder where the .txt file with the results will be stored must be created before the program is used.

If the analyst wants to run the program on the computer under examination by using a USB stick then he must place in the USB stick the scanner.exe program. Then in order to run it he must open a command line prompt and type the letter of the flash drive (e.x. F:) and this will move the working directory to the root of F. Then he must open the folder where the scanner.exe program is located in. For example: cd folder\. If the scanner.exe program is located just in the F and not in a folder the following commands will do. Then depending on what he intends to achieve he can type:

1) scanner.exe

2) scanner.exe help

- 3) scanner.exe scan
- 4) scanner.exe scan --path="C:\\" --extension="exe" --log_file="F:\Cexe.txt"

5) scanner.exe compare --log_file="F:\log.txt" --MD5_values_file="F:\clean.txt" -results_file="F:\results.txt"

4.4.1 Help mode

If we press as mentioned above:

- 1) .\php.exe C:\WAMP\www\scanner.php
- 2) .\php.exe C:\WAMP\www\scanner.php help
- 3) scanner.exe
- 4) scanner.exe help

Then we see the help screen of the program that shows us how it works, some instructions and what parameters to insert in each case. The help screen is appeared in the case the user doesn't know how the program works and runs the program with no parameters at all.

Figures 10, 11, 12 and 13 visualize this functionality of the program.

Γραμμή εντολών			×
Microsoft Windows [Version 6.2.9200] (c) 2012 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματο	5-		^
C:\Users\nikos>cd C:\wamp\bin\php\php5.4.16\			
C:\wamp\bin\php\php5.4.16>.\php.exe C:\WAMP\www\scanner.php SCAN MODE			
Usage: php scanner.php scanpath=path_to_checkextension=extension= log_file=path_and_name_of_log_file	on_to_f	filte	r
Example: php scanner.php scanpath="C:\myfolder\"extension="exe ="C:\mydocuments\md5_log.txt"	"log	g_fi∷	Le
Default values:path="C:\Windows"extension="exe"log_file="C: _log_file.txt"	\logfi]	le\ma	15
COMPARE MODE Usage: php scanner.php comparelog_file=path_and_name_of_log_file - _file=path_and_name_of_md5_values_fileresults_file=path_of_result:		value	25
Example: php scanner.php comparelog_file="C:\log_file_after_scan. alues_file="C:\file_with_clean_md5_values.txtresults_file="C:\fil ts.txt			
C:\wamp\bin\php\php5.4.16>			v

Fig. 10 Running the scanner.php program with no parameters.

🖬 Γραμμή εντολών 🗕 🗆 🗙
Microsoft Windows [Version 6.2.9200] (c) 2012 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.
C:\Users\nikos>cd C:\wamp\bin\php\php5.4.16\
C:\wamp\bin\php\php5.4.16>.\php.exe C:\WAMP\www\scanner.php help SCAN MODE Usage: php scanner.php scanpath=path_to_checkextension=extension_to_filter log_file=path_and_name_of_log_file
Example: php scanner.php scanpath="C:\myfolder\"extension="exe"log_file ="C:\mydocuments\md5_log.txt"
Default values:path="C:\Windows"extension="exe"log_file="C:\logfile\md5 _log_file.txt"
COMPARE MODE Usage: php scanner.php comparelog_file=path_and_name_of_log_filemd5_values _file=path_and_name_of_md5_values_fileresults_file=path_of_results_file
Example: php scanner.php comparelog_file="C:\log_file_after_scan.txt"md5_v alues_file="C:\file_with_clean_md5_values.txtresults_file="C:\file_with_resul ts.txt
C:\wamp\bin\php\php5.4.16>

Fig. 11 Running the scanner.php program in help mode.

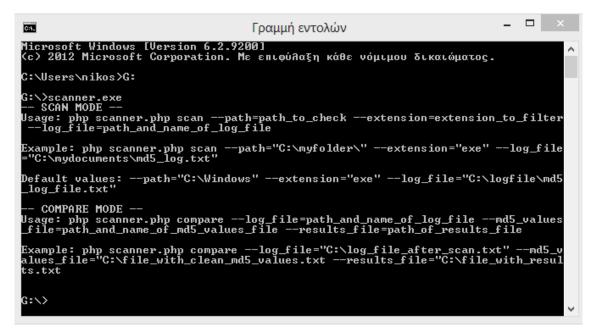


Fig. 12 Running the scanner.exe program from a USB drive with no parameters.

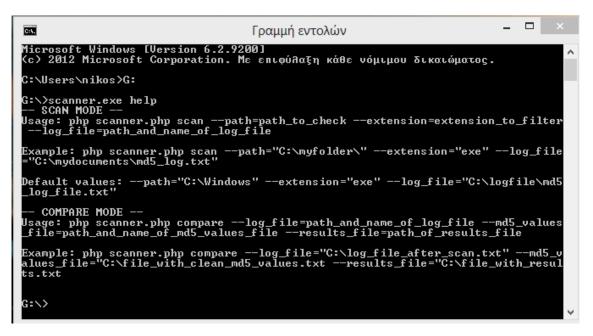


Fig. 13 Running the scanner.exe program from a USB drive in help mode.

In the above cases G drive is the USB stick.

4.4.2 Scan mode with no parameters

If we press as mentioned above:

1) .\php.exe C:\WAMP\www\scanner.php scan

2) scanner.exe scan

Then the program will use the scan mode with the default values (which the user can insert in the program using the Sublime-text editor) and are now set to be:

The path where the program to search in "C:\Windows".

The extension to search for "exe".

The path and the name of the .txt file to store the results "C:\logfile\md5_log_file.txt".

Figures 14, 15, 16, 17 and 18 visualize this functionality of the program.

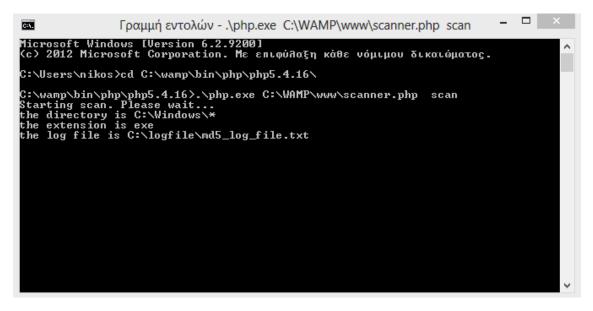


Fig. 14 Commands needed for running the scanner.php program in scan mode with no

parameters.

🖬 Γραμμή εντολών – 🗇	×
string(58) "C:\Windows\Microsoft.NET/Framework/v4.0.30319/ngentask.exe" [101] =>	^
string(53) "C:\Windows\Microsoft.NET/Framework/v4.0.30319/vbc.exe" [102] =>	
string(49) "C:\Windows\Microsoft.NET/Framework/NETFXSBS10.exe" [103] =>	
string(91) "C:\Windows\Microsoft.NET/assembly/GAC_32/MSBuild/v4.0_4.0.0.0_ f5f7f11d50a3a/MSBuild.exe" [104] =>	_Ъ03
string(103) "C:\Windows\Microsoft.NET/assembly/GAC_MSIL/ComSvcConfig/v4.0_4 0.0b03f5f7f11d50a3a/ComSvcConfig.exe" [105] =>	4.0.
string(111) "C:\Windows\Microsoft.NET/assembly/GAC_MSIL/InspectVhdDialog/v4 6.2.0.031bf3856ad364e35/InspectVhdDialog.exe"	4.0_
[106] => string(133) "C:\Windows\Microsoft.NET/assembly/GAC_MSIL/Microsoft.Workflow. piler/v4.0_4.0.0.031bf3856ad364e35/Microsoft.Workflow.Compiler.exe" [107] =>	. Com
string(97) "C:\Windows\Microsoft.NET/assembly/GAC_MSIL/SMSvcHost/v4.0_4.0.0 _b03f5f7f11d50a3a/SMSvcHost.exe" [108] =>	0.0_
string(99) "C:\Windows\Microsoft.NET/assembly/GAC_MSIL/WsatConfig/v4.0_4.0. b03f5f7f11d50a3a/WsatConfig.exe" [109] =>	.0.0
string(89) "C:\Windows\Microsoft.NET/assembly/GAC_MSIL/dfsvc/v4.0_4.0.0.0_ f5f7f11d50a3a/dfsvc.exe" [110] =>	_ЪØЗ
string(97) "C:\Windows\Microsoft.NET/assembly/GAC_MSIL/vmconnect/v4.0_6.2.0 _31bf3856ad364e35/vmconnect.exe" 	0.0_
string(36) "C:\Windows\Speech/Common/sapisvr.exe" [112] =>	
string(36) "C:\Windows\System32/Boot/winload.exe"	
[113] => string(38) "C:\Windows\System32/Boot/winresume.exe"	
[114] => string(36) "C:\Windows\System32/Com/MigRegDB.exe"	
[115] => string(35) "C:\Windows\System32/Com/comrepl.exe"	
[116] => string(37) "C:\Windows\System32/Dism/DismHost.exe"	
[117] => string(87) "C:\Windows\System32/DriverStore/FileRepository/bth.inf_x86_3033 09fb0d31a/fsquirt.exe"	3f54
[118] => string(87) "C:\Windows\System32/DriverStore/FileRepository/bth.inf_x86_594) bef3a1195/fsquirt.exe"	bba3
[119] => string(87) "C:\Windows\System32/DriverStore/FileRepository/bth.inf_x86_6510 33256645e/fsquirt.exe" [19] =>	cbbd
[120] => string(87) "C:\Windows\System32/DriverStore/FileRepository/bth.inf_x86_6d07 ab272b88f/fsquirt.exe"	733b
[121] => string(87) "C:\Windows\System32/DriverStore/FileRepository/bth.inf_x86_79a4 6ac1d2780/fsquirt.exe"	48b7
[122] => string(87) "C:\Windows\System32/DriverStore/FileRepository/bth.inf_x86_d5f8 9da72af83/fsquirt.exe"	3793
[123] => string(91) "C:\Windows\System32/DriverStore/FileRepository/cmazal.inf_x86_5 8a9147e94713/cmirmdrv.exe" [123] =>	552d
[124] => string(89) "C:\Windows\System32/DriverStore/FileRepository/hdart.inf_x86_ad 15ed112685b/AERTSrv.exe" f15ed112685b/AERTSrv.exe	ca1f
[125] => string(97) "C:\Windows\System32/DriverStore/FileRepository/hdart.inf_x86_ad 15ed112685b/DTSAudioService.exe" [126] =>	ca1f
[126] => string(95) "C:\Windows\System32/DriverStore/FileRepository/hdart.inf_x86_ad 15ed112685b/DTSU2PAuSrv32.exe" [127] =>	ca1f
[127] => string(87) "C:\Windows\System32/DriverStore/FileRepository/hdart.inf_x86_ad 15ed112685b/FMAPP.exe"	ca1f
<pre>(more elements)</pre>	
C:\wamp\bin\php\php5.4.16>	~

Fig. 15 Results after running the scanner.php program in scan mode with no parameters.

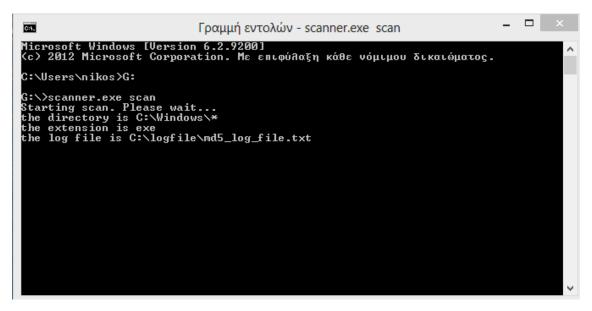


Fig. 16 Commands needed for running the scanner.exe program from a USB stick in scan mode with no parameters.

04.	Γραμμή εντολών 🦰	ō ×
[1740]=> string(32)	"C:\\indows\\$ystem32/yssadmin.exe"	^
[1741]=> string(29)		
[1742]=> string(31)	"C:\Windows\System32/waitfor.exe"	
[1743]=> string(31)		
[1744]=> string(32)	"C:\Windows\System32/wbengine.exe"	
[1745]=> string(31)	"C:\Windows\System32/wecutil.exe"	
[1746]=> string(30)	"C:\Windows\System32/wermgr.exe"	
[1747]=> string(32)	"C:\\indows\Sustem32/weututil.exe"	
[1748]=> string(32)		
[1749]=> string(29)	"C:\Windows\System32/where.exe"	
[1750]=> string(30)		
[1751]=> string(32)	"C:\\Vindows\System32/wiaacmgr.exe"	
[1752]=> string(31)		
[1753]=> string(31)	"C:\\indows\System32/wininit.exe"	
[1754]=> string(31)		
[1755]=> string(32)	"C:\Windows\System32/winload.cxe"	
[1756]=> string(33)	"C:\\indows\System32/winiogon.exe"	
[1757]=> string(29)	"C:\\indows\System32/wintesame.exe"	
[1758]=> string(33)	"C:\Windows\System32/winrshost.exe"	
[1759]=> string(30)	"C:\Windows\System32/winrsh5st.txt	
[1760]=> string(34)	"C:\Windows\System32/wkspbroker.exe"	
[1761]=> string(30)		
[1762]=> string(31)		
[1763]=> string(30)	-	
[1764]=>		
string(32) [1765]=>	"C:\Windows\System32/wpnpinst.exe"	
[1766]=>	"C:\Windows\System32/write.exe"	
string(31) [1767]=>		
[1768]=>	"C:\Windows\System32/wsmprovhost.exe"	
[1769]=>	"C:\Windows\System32/wsqmcons.exe"	
[1770]=>	"C:\Windows\System32/wuapp.exe"	
[1771]=>	"C:\Windows\System32/wuauclt.exe"	
string(28) [1772]=>		
string(29) [1773]=>		
string(32) [1774]=>		
[1775]=>	"C:\Windows\System32/xwizard.exe"	
[1776]=>	"C:\Windows\Temp/7za.exe"	
[1777]=>	"C:\Windows\WinStore/WSHost.exe"	
string(41)	"C:\Windows\servicing/TrustedInstaller.exe"	
G:\>		~

Fig. 17 Results after running the scanner.exe program from a USB stick in scan mode with no parameters.

In the above cases G drive is the USB stick.

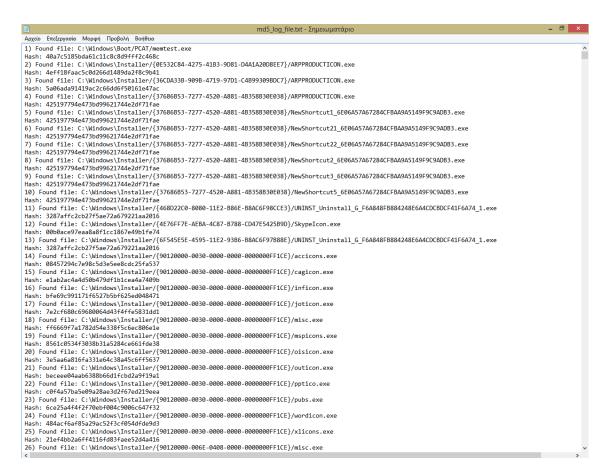


Fig. 18 The results md5_log_file.txt file after running the scanner.php or scanner.exe program in scan mode with no parameters.

4.4.3 Scan mode with parameters

We can use the scan mode with parameters if we want for example to use scanner.php program to search the entire C drive, for *.docx files and store the results in the Cdocx.txt file, which will be located in the WindowsMD5 file which we will have created in advance in the C drive. In this case we have to insert in the command line the following commands:

1) .\php.exe C:\WAMP\www\scanner.php scan --path="C:\\" --extension="docx" -log_file="C:\WindowsMD5\Cdocx.txt"

Then the program will use as values (which the user can insert from the command prompt) the following:

The path where the program to search "C:\\" (everything in C).

The extension to search for "docx".

The file to store the results "C:\WindowsMD5\Cdocx.txt".

If we want to use scanner.exe program from a USB stick to search all the D drive (partition of the hard disc) for *.txt files and store the results in the logDtxt.txt file which is located in the G drive (USB stick) we have to insert in the command line the following:

2) scanner.exe scan --path="D:\\" --extension="txt" --log_file="G:\logDtxt.txt"

Then the program will use as values (which the user can insert from the command prompt) the following:

The path where the program to search "D:\\" (everything in D).

The extension to search for "txt".

The file to store the results "G:\logDtxt.txt".

The program has the ability to search for any file extension we want .exe, .doc, .docx, .dll, .pdf, .log and so on. Also can search at any path we want, even USB sticks, and store the results wherever we want, including USB sticks, but in .txt only format.

Figures 19, 20, 21, 22, 23 and 24 visualize this functionality of the program.

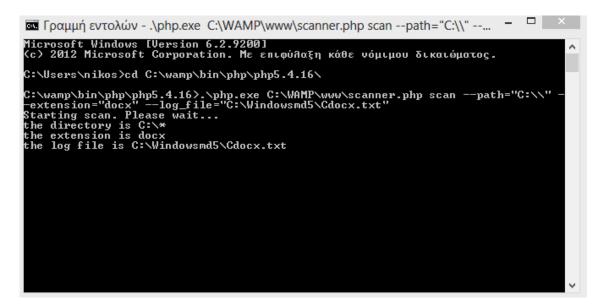


Fig. 19 Commands needed for running the scanner.php program in scan mode with the above mentioned parameters.

🔤 Γραμμή εντολών – 🗇	×
Microsoft Windows [Version 6.2.9200] (c) 2012 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.	^
C:\Users\nikos>cd C:\wamp\bin\php\php5.4.16\	
C:\wamp\bin\php\php5.4.16>.\php.exe C:\WAMP\www\scanner.php scanpath="C:\ -extension="docx"log_file="C:\Windowsmd5\Cdocx.txt" Starting scan. Please wait the directory is C:* the extension is docx	~" -
the log file is C:\Windowsmd5\Cdocx.txt array(24) { [0] =>	
string(75) "C:\\$Recycle.Bin/S-1-5-21-1123561945-1482476501-682003330-1004/ OFOH.docx" [1] =>	\$IXN
" """"""""""""""""""""""""""""""""""""	docx
[2] => string(55) "C:\Users/nikos/Desktop/bamcompile1.21/instructions.docx" [3] =>	
string(195) "C:\Users/nikos/Desktop/ $^{\mu}$ F $_{\Gamma}^{\mu}$ /All Chapters except from the lusions and the additional material 07-10-2013/Dissertation Nikolaos Bakirtz igital triage in forensics investigation 2013.docx" [4] =>	Conc is∕D
string(89) "C:\Users/nikos/Desktop/ ¹¹ Ffff ¹¹ ff/Dissertation Roadmap 15-07-201 ssertation Roadmap.docx"	3/Di
[5] => string(109) "C:\Users/nikos/Desktop/ ^{IL} F F ^{LI} /Interim report 22-08-2013/Dig triage in forensics investigation 2013.docx" [6] =>	ital
string(91) "C:\Users/nikos/Desktop/ ¹¹ Er ₁ -14 /Interim report 22-08-2013/Diss tion Roadmap Updated.docx"	erta
[7] => string(52) "C:\Users/nikos/Desktop/ ¹¹ EFHF ¹ 4 /TOOLS/Q±Yή±áHHá.docx" [8] =>	
string(56) "C:\Users/nikos/Desktop/ ¹¹ Ephr ¹¹ H/guidelines/appendix.docx" [9] =>	
string(58) "C:\Users/nikos/Desktop/ ¹¹ EFHF ¹¹ H/guidelines/submission.docx" [10] =>	
string(74) "C:\Users/nikos/Desktop/Digital triage in forensics investigati 013.docx" [11] =>	on 2
string(42) "C:\Users/nikos/Desktop/command prompt.docx" [12] =>	
string(38) "C:\Users/nikos/Desktop/references.docx" [13] =>	
string(38) "C:\Users/nikos/Desktop/~\$ferences.docx" [14] =>	
string(86) "C:\Users/nikos/Desktop/~\$gital triage in forensics investigati 013 - "IÏǿή±ά÷ I.docx" [15] =>	on 2
string(74) "C:\Users/nikos/Desktop/~\$gital triage in forensics investigati 013.docx"	on 2
[16] => string(42) "C:\Users/nikos/Desktop/~\$lk extractor.docx" [17] =>	
string(42) "C:\Users/nikos/Desktop/~\$mmand prompt.docx" [18] =>	
string(36) "C:\Users/nikos/Desktop/~\$@AYI(2.docx" [19] =>	
string(69) "C:\Users/nikos/Desktop/~\$Υ ξήή±ά÷Υ ΪΥΫ Microsoft Office Word (ocx"	2).d
[20] => string(65) "C:\Users/nikos/Desktop/~\$Υ ϡήή±ά÷Υ ΪΥΫ Microsoft Office Word.d	ocx"
[21] => string(36) "C:\Users/nikos/Desktop/~\$±ά°ώHY.docx" [22] ->	
[22] => string(35) "C:\Users/nikos/Desktop/⊥ H╥╓⊥.docx" [23] =>	
string(35) "C:\Users/nikos/Desktop/i@AYIi2.docx"	
- C:\wamp\bin\php\php5.4.16>	
	~

Fig. 20 Results after running the scanner.php program in scan mode with the above mentioned parameters.

🗖 Cdoox.txt - Σημειωματάριο – 🗖 💌
Αρχείο Επεξεργασία Μορφή Προβολή Βοήθεια
1) Found file: C:\\$Recycle.Bin/S-1-5-21-1123561945-1482476501-682003330-1004/\$IXNOFOH.docx Hash: eefed87b327bf64f7dec21b9d7bb9c5c
2) Found file: C:\Users/nikos/Desktop/Bike Built Buisness Plan - Contest/vpn.docx Hash: 33ba29278a20734c08648bb87c9073c1
3) Found file: C:\Users/nikos/Desktop/bamcompile1.21/instructions.docx Hash: 3210601801a9117a7121fd79857b6822
4) Found file: C:\Users/nikos/Desktop/ITYXIAKH/All Chapters except from the Conclusions and the additional material 07-10-2013/Dissertation Nikolaos Bakirtz: Hash: 4e7226536a70cc0e8ad792b95288359f
5) Found file: C:\Users/nikos/Desktop/NTYXIAKH/Dissertation Roadmap 15-07-2013/Dissertation Roadmap.docx
Hash: 94b16c4103a380f01c0a8944ba2ac3ad 6) Found file: C:\Users/nikos/Desktop/ITTYXIAKH/Interim report 22-08-2013/Digital triage in forensics investigation 2013.docx
Hash: 352d907cdcf60533ba0b95da5e2bdb14 7) Found file: C:\Users/nikos/Desktop/NTYXIAKH/Interim report 22-08-2013/Dissertation Roadmap Updated.docx
Hash: a2f64aee2257158028d2235e6962c118 8) Found file: C:\Users/nikos/Desktop/NTYXIAKH/TOOLS/προγραμμα.docx
Hash: 781e3cb8f1b5fc9ca5d48f3f4fb240ae 9) Found file: C:\Users/nikos/Desktop/NTYXIAKH/guidelines/appendix.docx
Hash: 82b6fddccd458299e9bee587c4ddfae7 10) Found file: C:\Users/nikos/Desktop/NTYXIAKH/guidelines/submission.docx
Hash: 6c1218f6cd7936dbfa88c61555c99c26 11) Found file: (:\Users/nikos/Desktop/Digital triage in forensics investigation 2013.docx
Hash: e9864e47d492f9308360a2e14b117a17 12) Found file: C:\Users/nikos/Desktop/command prompt.docx
Hash: 27783cd306359028b200ea77f85ef0d7 13) Found file: (:\Users/nikos/Desktop/references.docx
Hash: 50d64996998f2a74cc46201b662009cb 14) Found file: C:\Users/nikos/Desktop/~\$ferences.docx
Hash: 6b292cffac42404002c0c51dc94281fb 15) Found file: C:\Users/nikos/Desktop/~\$gital triage in forensics investigation 2013 - Αντιγραφή.docx
Hash: 01251ed51722f58f6355c598fe80da40 16) Found file: C:\Users/nikos/Desktop/~\$gital triage in forensics investigation 2013.docx
Hash: 530cbe52073151f4001016be25f66147 17) Found file: C:\Users/nikos/Desktop/~\$lk extractor.docx
Hash: 5b9afee2026bd118131d3bdedfd54908 18) Found file: C:\Users/nikos/Desktop/~\$mmand prompt.docx
Hash: 60c043f8fbbd59380f537069d0af6991 19) Found file: C:\Users/nikos/Desktop/~\$ικονες.docx
Hash: 60c043f8fbbd59380f537069d0af6991 20) Found file: C:\Users/nikos/Desktop/~\$ο Ἐγγραφο του Microsoft Office Word (2).docx
Hash: 34dfee38ea67ea5a6105e793eaea7d9b 21) Found file: C:\Users/nikos/Desktop/~\$ο Ἐγγραφο του Microsoft Office Word.docx
Hash: 5b9afee2026bd118131d3bdedfd54908 22) Found file: C:\Users/nikos/Desktop/~\$ραψιμο.docx
Hash: 09357fbabce88a42b783199a68dbfbf9 23) Found file: C:\Users/nikos/Desktop/AFTEAIA.docx
Hash: 94f9d817063ad4fa1eeb66b9f067f1c2 24) Found file: C:\Users/nikos/Desktop/εικονες.docx
Hash: e1adcea97a5023502faf6ed1200366ec
v.
< >>

Fig. 21 The results Cdocx.txt file after running the scanner.php program in scan mode

with the above mentioned parameters.

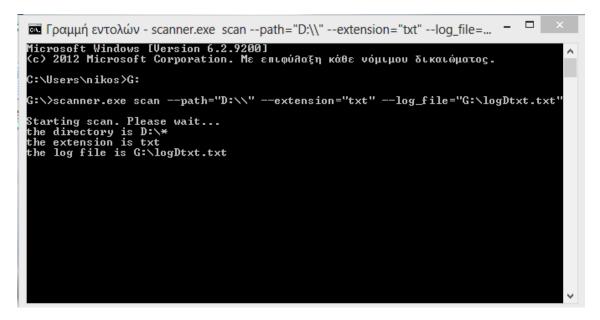


Fig. 22 Commands needed for running the scanner.exe program from a USB stick in scan mode with the above mentioned parameters.

🔤 Γραμμή εντολών 🗕 🗇 🗙
[1676]=> string(109) "D:\⊥μΕϝ╧╠ϝ⊥╱⊥=┘╨╧╦╠╱⊥μΕϝ╧╠╧╙╱−ϝ┸╓╧╤┸╱┸.Ε. =┵╬╧╒╱ά±≈ίѽΫϋίΪὑ╫╢ΫΫ ΫΕѽŊ᠉ѽҲϒ CD╱┼╦.┸╙╱┶╦╤╧┸╨╧╔ (U)╱┝┼═╔╩┸.txt"
[1677]=> string(110) "D:\┴ᄔ╞━╧╠╔┶╱┶═┘╨╧╦╠╱┵╙╘╒═╧╠╧╙╱╼╔┵╓╧╤┶╱┵.╘. ═┵╬╧╒╱ѽ±≈┊ѽŸӥ┆Ïѝ╫╢Ÿ ŸĔѽѷӍ ѼᡘŶ CD╱┼╦.┶╙╱┵╦╦╧┷╨╧╔ 〈U〉╱╦╧╔╨╧╒═.txt" [1678]=>
ͼϯϼ;ϳϼϣϥͻͺ; ϫ;ϫ;;ϫ;ϫ;;;;;;;;;;;;;;;;;;;;;;;;;;;;
נו6/אין => string(109) "D:\+++ בבבוור איבן אבן אבן אבן איבן איבן איבן איבן אי
string(78) "D:\┴╙╘╒═╧╠╓┵╱┵═┘╨╧╦╟╱┵╘ ╞┘┝╤┵╓╧╒╱┼┝╩╦┼╓╙╞╩╙╶╴┼╬┼╘┵╙╟╱╘╠╦┼╓┘═╧┼╔ ╙┵┝┝┽╦┿┵.txt" [1681]=>
/╨. [→] .12012008 ╨┼╓└レ╤╢┟┅└╵╹╔┶┰╔┵╶┸╙╏╔╧┨╠╓┷╵╽╤╩╙┘╙╔╩╒.txt [,] [1682]=> string(アア>) "D:ヽ┶╙╘╒╧╠╔┶╱╞┙┝╤┶╓╧╒╱╠╨┷╩╔╤╘╞║╙╱┼┝╩╦┼╔╙╠╧╙╶╸╀╬┼╘┷╙╟╱╘╠╦┼╓┙═╧┼╔╙ ┶┝┼┿╦┿┶.txt" [1683]=>
נוטטסייייטטסייייטטיטיייטיטיייטייטיייטייטיי
string(68) 'D:\للما = الما الما الما الما الما الما الم
string(112) "D:_Lutp=_ /
└1000]-/ string(108) "D:\⊥и⊧⊨╧╠╓┴╱╨┼╞┼╙ ╨┼╤╔╨╧╦╔┼╙╱═┼┸ ┼═╘╒╨┸ ╨ 120.08╱╨120]2008 ╨┼╔┞┘╤╢╔╨┶ -╔╙┸╔╧ ┸╙╘╒═╧╠╔┵┵ ╨╤┵╙╜╨╔╨┵╒.txt" [1687]=>
╺╘┲┲┙┙┙╖ ┺╦┙┙┙╖ ┺╦┙┙╴╖
[1688]=> string(82) "D:\-FHL+H HL=HHFL+A SEMESTER/CoNet/ASSIGNMENTS/CoNet Project 2013/README.txt" [1689]=>
string(61) "D:\-הְוְנֵשְׁוֹשׁ בּוְשְׁהֵע בּוְשְׁהֵע בוּשְׁהֵע און און בּוּשְׁהָע SEMESTER/CoNet/-הְעַתְּשְׁאַ/CoNet/i1.txt" [1690]=>
string(61) "D:\-FflL=fu ul=fuFuEl ffL/A SEMESTER/CoNet/-FLALFL/CoNet/i2.txt" [1691]=>
string(49) "D:\-FHL-H" HL-H"F"A SEMESTER/CoNet/urls.txt"
string(94) "D:\F L= U_HU_FU_FU_F F -/A_SEMESTER/WebIS/ASSIGNMENTS/2_ASSIGNMENT E-SHOP/assignment/readme.txt"
string(106) "D:\F+LL+" "L-+"F"L+" ()); E-SHOP/-F+F"F"L-+"F"L-+"F"L+"/Registration.txt"
string(99) "D:\HLHUHLHLA SEMESTER/WebIS/ASSIGNMENTS/2 ASSIGNMENT E-SHOP/_FL_HL_HL/login.txt"
נונסיקן=> string(100> "D:\ה+וב-+" אריין אין אין אין אין אין אין אין אין אין
string(83) "D:\F L= " = "F ^L = "F ^L = F ^L /C SEMESTER/GREEN ICT/GreenGrid_datacenter_ Certification.txt" [1697]=>
string(140) "D:\L ^L IFFI ⁴⁰ /Alfred Hitchcock/Alfred.Hitchcock.Collection.DVDRip.Xv iD/North.By.Northwest.1959.DVDRip.XviD.ROsubbed-NoGRP/CD1/Subs/2-gre(1).txt" [1698]=>
string(137) "D:\L ^L [-[]4/Alfred Hitchcock/Alfred.Hitchcock.Collection.DVDRip.Xv iD/North.By.Northwest.1959.DVDRip.XviD.ROsubbed-NoGRP/CD1/Subs/2-gre.txt" [1699]=>
string(148) "D:\LL_F_F_4/Alfred Hitchcock/Alfred.Hitchcock.Collection.DVDRip.Xv iD/North.By.Northwest.1959.DVDRip.XviD.ROsubbed-NoGRP/CD2/Subs/nogrp-tab-gre(1). txt"
[1700]=> string(145) "D:\\Lft ^u /Alfred Hitchcock/Alfred.Hitchcock.Collection.DVDRip.Xv iD/North.By.Northwest.1959.DVDRip.XviD.ROsubbed-NoGRP/CD2/Subs/nogrp-tab-gre.txt "
[1701]=> string(60) "D:\㎡ 世十十二㎡中小 ㎡ 世十十二㎡ 四十二章 }
G:\>

Fig. 23 Results after running the scanner.exe program from a USB stick in scan mode

with the above mentioned parameters. (1701 results)

A problem of the command line prompt is that it does not display words in Greek. It displays unknown symbols when it encounters Greek letters. The problem is solved in the *.txt files with the results, where every language including Greek is displayed correctly.

logDtxt.txt - Σημειωματάριο	- 0 >
ιο Επεξεργασία Μορφή Προβολή Βοήθεια	
Found file: D:\MUSIC/CLASSIC/Beethoven - The Best of Beethoven - Classical music album/READ THIS.txt	
h: 6da1dc480d602b68c02628a9245aea42	
Found file: D:\MUSIC/CLASSIC/Best of classical music/Information/1337x.org.txt	
h: 8a646fdfcbb389709c31ab5e0f236476	
Found file: D:\MUSIC/CLASSIC/Best of classical music/Information/HDScene - sceneunderground.org.txt	
h: d4231f8bd31d4f9dbb6d9422b26f2e0d	
Found file: D:\MUSIC/CLASSIC/Best of classical music/Information/Pix2links.txt	
h: 34d179fc66992f4eeb93199ac6df0173	
Found file: D:\WUSIC/CLASSIC/Best of classical music/Information/Torrent downloaded from AhaShare.com.txt	
h: 55e565dd59a868ba9d0366602e14c97b	
Found file: D:/MUSIC/CLASSIC/Best of classical music/Information/Torrent downloaded from Demonoid.me.txt	
h: 0ba9b8b077F33d011dbe5bF4892a3cfe	
Found file: D:\MUSIC/CLASSIC/Best of classical music/Information/Torrent downloaded from Sceneunderground.org.txt	
h: deacf10fa5bd707521a895a646d7af57 Found file: D:\MUSIC/CLASSIC/Best of classical music/Information/Torrent downloaded from h33t.com.txt	
round file. D. (Moste/CLESsic/Dest of Classical music/information/idirent downloaded from host com. CKL	
n. rchoraso/uosszeenus/szeenus/salasos Found file: D:WMSIC/CLASSIC/Best of classical music/tracklist.txt	
1 dbhcl1da3fdf168aa1659cb59c3982	
Found file: D:\WUSIC/CLASSIC/Classical Masterpiece of Music - Antonio Vivaldi/Antonio Vivaldi.txt	
7. 795Fa6dd993F4e664Fab5ae0e5F8Fd9c	
Found file: D:\MUSIC/CLASSIC/Classical Masterpiece of Music - Edvard Grieg/Edvard Grieg.txt	
h: a7729dc9cbbe5ee8538f9cdd8118eebf	
Found file: D:\MUSIC/CLASSIC/Classical Masterpiece of Music - Franz Schubert/Franz Schubert.txt	
h: edd1337c64fbe2a4da815a1ad4b1a0bb	
Found file: D:\MUSIC/CLASSIC/Classical Masterpiece of Music - Richard Wagner/Richard Wagner.txt	
h: a8af354e0942efb4371ad57264d2cfbe	
Found file: D:\MUSIC/CLASSIC/Classical Music/Beethoven's Symphonies/Torrent downloaded from Demonoid.me.txt	
h: 0ba9b8b077f34d011dbe5bf4892a3cfe	
Found file: D:\MUSIC/CLASSIC/Classical Music - Top 100 (Part 1)/Torrent downloaded from Demonoid.com.txt	
h: c347d69b388abbabaf2f894c4200465c	
Found file: D:\MUSIC/CLASSIC/Medieval Music from Old Serbia - Classical - flac/0000 info.txt	
h: adaa897d49c9a19d0982bde02142b284	
Found file: D:\MUSIC/CLASSIC/The 99 Darkest Pieces Of Classical Music/Torrent downloaded from Demonoid.com.txt	
h: c347d69b388abbabaf2f894c4200465c	
Found file: D:\MUSIC/CLASSIC/The Greatest Classical Hits - Wolfgang Amadeus Mozart - classic music album/READ THIS.txt	
h: 6da1dc480d682b68c92628a9245aea42	
Found file: D:/WUSIC/CLASSIC/Top 100 Masterpieces of Classical Music 1685-1928/The Top 100 Masterpieces of Classical Music 1685-1928	.txt
n: 8277302b15703c1133df2aedhc5a953	
Found file: D:\office/Office.2010.Toolkit.&.EZ-Activator.3.3.4/IMPORTANT! Readme!.txt h: 1781336a8808f2def4ddf381c60fad82	
. 1/01/01/01/01/01/01/01/01/01/01/01/01/01	
real in a second s	
Found file: D:\ANTIFPADA KINFD/Apge:o0ńkec SMS/EAENA/EIEEPXOMENA/rcv0015a.txt	
194fa/4ee7730478dbacdfbdb809737b1	
Found file: D:\ANTIFPADA KINHTO/Apge:oofikec SMS/EAENA/EIEEPXOMENA/rcv0016u.txt	
1: da266586c579cb7e2227a844d486c0	
Found file: D:\ANTIFAQA KINHTO/Apχειοθήκες SMS/EΛΕΝΑ/ΕΙΣΕΡΧΟΜΕΝΑ/rcv0016v.txt	
137458920413eea0ab1dd592e2d7ca51	
Found file: D:\ANTIFAQA KINHTO/Apχειοθήκες SMS/EΛΕΝΑ/ΕΙΣΕΡΧΟΜΕΝΑ/rcv0016w.txt	
h: f4ebe76110c22c807976759b4fb14d9d	
Found file: D:\ANTIFPAØA KINHTO/Αρχειοθήκες SMS/ΕΛΕΝΑ/ΕΙΣΕΡΧΟΜΕΝΑ/rcv0016x.txt	

Fig. 24 The results logDtxt.txt file after running the scanner.exe program from a USB drive in scan mode with the above mentioned parameters. (1701 results)

In all the above cases G drive is the USB stick.

4.4.4 Compare mode with parameters

The compare mode always needs parameters to run properly. If we want to use scanner.php program to compare two .txt files, the one with the MD5 values that we created by scanning the suspicious computer and the one with the clean MD5 values that we don't want to take into account when we see the results, then we have to insert in the command line the following commands:

1) .\php.exe C:\WAMP\www\scanner.php compare

--log_file="C:\WindowsMD5\log.txt"

--md5_values_file="C:\WindowsMD5\clean.txt"

--results_file="C:\WindowsMD5\results.txt"

Then the program will use as values (which the user can insert from the command prompt) the following:

The path for the log_file with all the MD5 values under investigation "C:\WindowsMD5\log.txt". The log.txt file is the file that we created with the scan mode of the program scanner.php and contains all the files under investigation including their paths and their MD5 hash values.

The path for the md5_values_file with all the clean MD5 values that we don't want to take into consideration during the investigation is "C:\WindowsMD5\clean.txt". The md5_values_file is the file that we created with the scan mode of the program scanner.php in a previous time or in the lab, in a clean from viruses, malware and additional programs computer and that contains all the files and their MD5 values that don't oppose a threat to us. So we want to eliminate them from the investigation process.

The file to store the results of the comparison is set from the user to be "C:\WindowsMD5\results.txt". The file WindowsMD5 is created from the user be-fore running the program.

For the specific example we created the two files to compare as following: for the clean MD5 values file we used the scan mode of the scanner.php to create a file with all the *.exe files of a clean Windows 8 installation (.\php.exe C:\WAMP\www\scanner.php scan --path="C:\Windows" --extension="exe" -- log_file="C:\WindowsMD5\clean.txt") and for the MD5 values under investigation we used the scan mode of the scanner.php to create a file with all the *.exe files of the entire computer, partition C (.\php.exe C:\WAMP\www\scanner.php scan -- path="C:\\" --extension="exe" -- log_file="C:\\" --log_file="C:\\" -- log_file="C:\\" -- log_file="C:

Figures 25, 26, 27, 28 and 29 visualize this functionality of the program.

	clean.txt - Σημειωματάριο	- 🗇 🗙
Αρχείο	Επεξεργασία Μορφή Προβολή Βοήθεια	
1783)	Found file: C:\Windows/assembly/NativeImages_v4.0.30319_32/vmconnect/44430f8a6396719e133b5ab441bf91d2/vmconnect.ni.exe	^
	a7e6b4c0224922d1228bca84c02263c0	
	Found file: C:\Windows/servicing/TrustedInstaller.exe	
	02d1fc0fda92fb34434166c612f95e5b	
	Found file: C:/Windows/HelpPane.exe	
	d93d02787065eaafd36deec059e84afd Found file: C:\Windows/IsUninst.exe	
	Sisek6400808556405816637eact2a	
	Found file: C:\Windows/RTHDCPL.exe	
	75eb71ec21903a57e38e367cfab0c55e	
	Found file: C:\Windows/RTLCPL.exe	
	fb2ad52c255527fad0dcae427c707586	
1789)	Found file: C:\Windows/SoundMan.exe	
	4ca0410064282d72edc28390859668c4	
	Found file: C:\Windows/alcwzrd.exe	
	c9db82f8965c9fe62b9a3f03bb02143f	
	Found file: C: Windows/bfsvc.exe	
	7d593720fc0c2c5dfb62bcc8d7573a21	
	Found file: C:\Windows/dchcfg32.exe 9804c1eda26e70e343edee9f1807bc62	
	Found file: C:\Windows/dciWds32.exe	
	4/2a5ae3465c2e532631adcf42c523	
	Found file: C:\Windows/dcmdev32.exe	
	18a749b2bd12ed74261434656a110b5a	
1795)	Found file: C:\Windows/explorer.exe	
	eafe46b0292d2bd2467835e2acf717cc	
	Found file: C:\Windows/hapint.exe	
	dfe8b187dcd083150c424024189339ec	
	Found file: C: Windows/hh.exe	
	7837Ab5539ae2bceac3ace5fb08ddce5	
	Found file: C:\Windows/notepad.exe 22e1963fe26d5bceab0575eb6ff60cb5	
	Found file: C:\Windows/regedit.exe	
	714445935904c68e67ea3d35a4b948	
	Found file: C:\Windows/slrundll.exe	
	987fee1415e95d146804d8d008ed0162	
1801)	Found file: C:\Windows/splwow64.exe	
Hash:	d5abb3abe528212fc51484c92afb1b59	
	Found file: C:\Windows/twunk_16.exe	
	f36a271706edd23c94956afb56981184	
	Found file: C: Windows/twunk_32.exe	
	b24577b1287a34qcc76ccf2ed2c1db35	
	Found file: C:\Windows/unin0408.exe 2c82955895a809c5bd6d7c0978cb93fb	
	Coard Signal Coard	
	Se67/351a5cb299c25621c6c1ab57884	
	Found file: C:\Windows/winhlp32.exe	
	eada08c87ad2a913563244ccf4391e5d	
	Found file: C:\Windows/write.exe	
Hash:	185b8e5d0e8ce317cd53294441fb4491	
		~
<		>

Fig. 25 The clean.txt file with all the *.exe files of the clean Windows 8 installa-

tion. (1807 results)

		log.txt - Σημειωματάριο	- 🗇 🗙
Αρχείο	Επεξεργασία Μορφή Προβολή Βοήθεια		
2467)	Found file: C:\Windows/HelpPane.exe		^
	d93d02787065eaafd36deec059e84afd		
2468)	Found file: C:\Windows/IsUninst.exe		
Hash:	515e4684008e955de0c81e6a7aea1c2a		
2469)	Found file: C:\Windows/RTHDCPL.exe		
Hash:	75eb71ec21903a57e38e367cfab0c55e		
	Found file: C:\Windows/RTLCPL.exe		
	fb2ad52c255527fad0dcae427c707586		
	Found file: C:\Windows/SoundMan.exe		
	4ca0410064282d72edc28390859668c4		
	Found file: C:\Windows/alcwzrd.exe		
	c9db82f8965c9fe62b9a3f03bb02143f		
	Found file: C:\Windows/bfsvc.exe		
	7d593720fc0c2c5dfb62bcc867573a21		
	Found file: C:\Windows/dchcfg32.exe		
	9804c1eda26e70e343edee9f1807bc62		
	Found file: C:\Windows/dciwds32.exe		
	442a5ae3465cc2e532631adcf42dc523		
	Found file: C:\Windows/dcmdev32.exe 18a749b2bd12ed74261434656a110b5a		
	Found file: C:\Windows/explorer.exe		
	eafe46b0292d2bd2467835e2acf717cc		
	Found file: C:\Windows/hapint.exe		
	dfe8b187dcd083150c424024189339ec		
	Found file: C:\Windows/hh.exe		
	7837ab5539ae2bceac3ace5fb08d4ce5		
	Found file: C:\Windows/notepad.exe		
	22e1963fe26d5bceab0575eb6ff60cb5		
	Found file: C:\Windows/regedit.exe		
	f71444a5935904c68e67ee3d35a4b948		
2482)	Found file: C:\Windows/slrundll.exe		
Hash:	987fee1415e95d146804d8d008ed0162		
2483)	Found file: C:\Windows/splwow64.exe		
Hash:	d5abb3abe528212fc51484c92afb1b59		
2484)	Found file: C:\Windows/twunk_16.exe		
Hash:	f36a271706edd23c94956afb56981184		
2485)	Found file: C:\Windows/twunk_32.exe		
	b24577b1287a340cc76ccf2ed2c1db35		
	Found file: C:\Windows/unin0408.exe		
	2c82955895a809c5bd6d7c0978cb93fb		
	Found file: C:\Windows/winhelp.exe		
	8e6f7d51a5cb299c25621c6c1ab57e84		
	Found file: C:\Windows/winhlp32.exe		
	eada08c87ad2a913563244ccf4391e5d		
	Found file: C:\Windows/write.exe		
	185b8e5d0e8ce317cd53294441fb4491		
	Found file: C:\wamp/unins000.exe		
	63468328dfcd0515969007a35d8152af		
	Found file: C:\wamp/wampmanager.exe 663392e75fd426ea94c75cdbf1916251		
nasn:	003332613104206934C13C0DT13T0231		*
<			×
			,

Fig. 26 The log.txt file with all the *.exe files of the entire computer, partition C.

(2491 results)

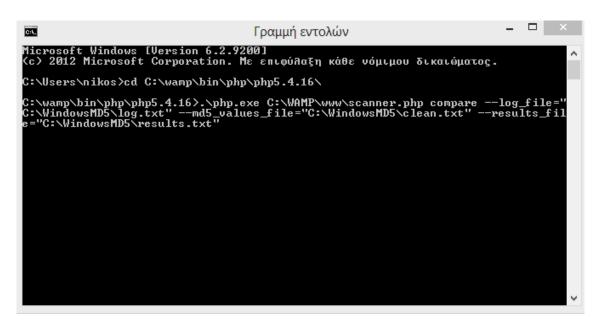


Fig. 27 Commands needed for running the scanner.php program in compare mode as mentioned above.

📼 Γραμμή εντολών – 🗇 🗙
Suspicious file found -> C:\Users/nikos/Desktop/ ¹¹ Efff ¹¹ //TOOLS/super kludge/md5d
eep-4.3/md5deep-4.3/tigerdeep64.exe Suspicious file found -> C:\Users/nikos/Desktop/ ^u Ephr ^{uu} h/TOOLS/super kludge/md5d
eep-4.3/md5deep-4.3/whirlpooldeep.exe Suspicious file found -> C:\Users/nikos/Desktop/ ^U Ef [[^{_1}]]/TOOLS/super kludge/md5d
eep-4.3/md5deep-4.3/whirlpooldeep64.exe
Suspicious file found -> Č:\Users/nikos/Desktop/ ^{UE} F _{[7} 14] /TOOLS/super kludge/rifi uti/rifiuti/rifiuti.exe
Suspicious file found -> C:\Users/nikos/Desktop/"F _"" /TOOLS/super kludge/srcs
/proxy.exe Suspicious file found -> C:\Users/nikos/Desktop/ ^u EF <mark>_uu</mark> /TOOLS/super kludge/7z92
Ø.exe
Suspicious file found -> C:\Users/nikos/Desktop/ ^{UE} F _{[7} _1] /TOOLS/super kludge/Soph os Virus Removal Tool.exe
Suspicious file found -> C:\Users/nikos/Desktop/ ^{UE} F _{[7} _4] /TOOLS/super kludge/catc hme.exe
Suspicious file found -> C:\Users/nikos/Desktop/"Ef _"[[].T00LS/super kludge/mbr.
exe Suspicious file found -> C:\Users/nikos/Desktop/ ^{UL} F F ^{LU} /TOOLS/super kludge/mdd_
1.3.exe Suspicious file found -> C:\Users/nikos/Desktop/scanner.exe
Suspicious file found -> C:\Users/nikos/Desktop/scanner_version_2.exe Suspicious file found -> C:\Users/nikos/Desktop/scanner_version_3.exe
Suspicious file found -> C:wam/bin/anache/Anache2.4.4/bin/AnacheMonitor.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/ApacheMonitor.exe Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/Ab.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/abs.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htcacheclean.exe Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htdbm.exe
Suspicious file found -> C:\uamp/bin/apache/Hpache/4.4/bin/htdbm.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htdigest.exe Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htpasswd.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/httpd.exe Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/httxt2dbm.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/httxt2dbm.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/logresolve.exe Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/openssl.exe Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/rotatelogs.exe
Suspicious file found -/ C. Wamp/bin/anache/Apache2.4.4/bin/openssi.exe
Suspicious file found \rightarrow C:wamp/bin/apache/Apache2.4.4/bin/wintty.exe
Suspicious file found -> C:\wamp/bin/apache/Apache2.4.4/bin/wintty.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/echo.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/innochecksum.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/my_print_defaults.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisam_ftdump.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisamchk.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisamlog.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisamlog.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisampack.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql_client_test.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql_client_test_emb
edded.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql_config_editor.e xe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql_embedded.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql_plugin.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql_tzinfo_to_sql.e
xe Suspicious file found -> C:\wamp/bin/mysgl/mysgl5.6.12/bin/mysgl upgrade.exe
Suspicious file found \rightarrow C:\wamp/bip/mysgl/mysgl5.6.12/bip/mysgladmin.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlbinlog.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlcheck.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlcheck.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqld-debug.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqld.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.0.12/bin/mysql4.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlimport.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqldump.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqldump.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlshow.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlshow.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlshow.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlshow.exe
Suspicious file found -> C:\uamp/bin/mysgl/mysgl5.6.12/bin/mysglslap.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqltest.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqltest_embedded.ex
e
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/perror.exe Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/replace.exe
Suspicious file found -> C:\wamp/bin/mysgl/mysgl5.6.12/bin/replace.exe
Suspicious file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/resolveip.exe Suspicious file found -> C:\wamp/bin/php/php5.4.16/php-cgi.exe
$\mathcal{C}_{\text{uonioiouo}}$ file found $-\mathcal{V}_{\text{uonn}}$ (his /nhn/nhnE / 16 /nhn-uin ave
Suspicious file found -> C:\wamp/bin/php/php5.4.16/php.exe
Suspicious file found -> C:\wamp/tools/xdc/xdc.exe
Suspicious file found -> C:\wamp/bin/php/php5.4.16/php.exe Suspicious file found -> C:\wamp/tools/xdc/xdc.exe Suspicious file found -> C:\wamp/unins000.exe Suspicious file found -> C:\wamp/wampmanager.exe
ouspicious file found 7 of wamp wampmanager exe
C:\wamp\bin\php\php5.4.16>

Fig. 28 The results after running the scanner.php program in compare mode.

	results.txt - Σημειωματάριο	- 0 ×
Αρχείο Επεξεργα	τία Μορφή Προβολή Βοήθεια	
583) Suspicio	us file found -> C:\Users/nikos/Desktop/scanner_version_2.exe	
584) Suspicio	us file found -> C:\Users/nikos/Desktop/scanner_version_3.exe	
585) Suspicio	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/ApacheMonitor.exe	
586) Suspicio	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/ab.exe	
587) Suspicio	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/abs.exe	
588) Suspicio	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htcacheclean.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htdbm.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htdigest.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/htpasswd.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/httpd.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/httxt2dbm.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/logresolve.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/openssl.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/rotatelogs.exe	
	us file found -> C:\wamp/bin/apache/Apache2.4.4/bin/wintty.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/echo.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/innochecksum.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/my_print_defaults.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisam_ftdump.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisamchk.exe us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/myisamlog.exe	
	us file found -> C:\wamp/bin/mysql/mysqls.o.12/bin/myisamlog.exe us file found -> C:\wamp/bin/mysql/mysqls.o.12/bin/myisamlog.exe	
	us file found -> C: (wamp/bin/mysql/mysql5.6.12/bin/mysqlex.exe us file found -> C: (wamp/bin/mysql/mysql5.6.12/bin/mysql	
	us file found -> C.(wamp/bin/mysql/mysqls.6.12/bin/mysql Clent test.exe	
	us file found -> C. (wamp/bin/mysql/mysql/ingsql.file). us file found -> C. (wamp/bin/mysql/mysql/sci.2(bin/mysql.filent test embedded.exe	
	us file found -> C: \wamp/bin/mysql/mysql5.6.1/bin/mysql config editor.exe	
	us file found -> C: (wamp/bin/mysql,mysql5.6.1/bin/mysql embedded.exe	
	us file found -> C: (wamp/bin/mysql; /mysql; bin/mysql plugin.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysql tzinfo to sql.exe	
	us file found -> C:\wamp/bin/mysql5.6.12/bin/mysql upgrade.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqladmin.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlbinlog.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlcheck.exe	
616) Suspicio	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqld-debug.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqld.exe	
618) Suspicio	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqldump.exe	
619) Suspicio	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlimport.exe	
620) Suspicio	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqlshow.exe	
621) Suspicio	us file found -> C:\wamp/bin/mysqlf.6.12/bin/mysqlslap.exe	
622) Suspicio	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqltest.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/mysqltest_embedded.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/perror.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/replace.exe	
	us file found -> C:\wamp/bin/mysql/mysql5.6.12/bin/resolveip.exe	
	us file found -> C:\wamp/bin/php/php5.4.16/php-cgi.exe	
	us file found -> C:\wamp/bin/php/php5.4.16/php-win.exe	
	us file found -> C:\wamp/bin/php/php5.4.16/php.exe	
	us file found -> C:\wamp/tools/xdc/xdc.exe	
	us file found -> C:\wamp/unins000.exe	
532) Suspicio	us file found -> C:\wamp/wampmanager.exe	

Fig. 29 The results.txt file with the results after running the scanner.php program in compare mode with the above mentioned parameters. (632 results)

If we want to use scanner.exe program, which is located in the G drive (USB stick), to compare two .txt files, the one with the MD5 values that we created by scanning the suspicious computer and the one with the clean MD5 values that we don't want to take into account when we see the results, then we have to insert in the command line the following commands (after making the working directory of the CMD the G:):

2) scanner.exe compare --log_file="G:\log.txt" --md5_values_file="G:\clean.txt" --results_file="G:\results.txt"

Then the program will use as values (which the user can insert from the command prompt) the following:

The path for the log_file with all the MD5 values under investigation "G:\log.txt". G drive is the USB stick. The log.txt is the file that we created with the scan mode of the program scanner.exe and contains all the files under investigation, including their paths and their MD5 values.

The path for the md5_values_file with all the clean MD5 values that we don't want to take into consideration during the investigation "G:\clean.txt". The md5_values_file is the file that we created with the scan mode of the program scanner.exe, in a previous time or in the lab, in a clean from viruses, malware and additional programs computer and contains all the files and their MD5 values that don't oppose a threat to us. So we want to eliminate them from the investigation process.

The file to store the results from the comparison is set from the user to be "G:\results.txt". As mentioned above G drive is the USB stick.

For the specific example we created the two files to make the comparison as following: for the clean MD5 values file we used the scan mode of the scanner.exe to create a file with all the *.dll files of a clean Windows 8 installation (scanner.exe scan --path="C:\Windows" --extension="dll" --log_file="G:\clean.txt") and for the MD5 values under investigation we used the scan mode of the scanner.exe to create a file with all the *.dll files of the entire computer, partition C (scanner.exe scan -path="C:\\" --extension="dll" --log_file="G:\log.txt").

The program has the ability to search for any file extension we want .exe, .doc, .docx, .dll, .pdf, .log and so on. It can also search at any path we want, even USB sticks, and store the results wherever we want, including USB sticks, but in .txt only format.

In some cases, depending on the Operating System (Windows 8, 7, Vista etc), the CLI mode must be executed as administrator. This must be done in order for the compare mode of the scanner.exe program to work properly. In these cases there are not enough privileges, for the program, to execute all its functions, concerning the files and wherever these might have been placed.

Figures 30, 31, 32, 33 and 34 visualize this functionality of the program.

📃 clean.txt - Σημειωματάριο	- 🗗 🗙
Αρχείο Επεξεργασία Μορφή Προβολή Βοήθεια	
12674) Found file: C:\Windows/diagnostics/system/DeviceCenter/DiagPackage.dll	^
Hash: 48025f5096666c9ccbd03d2fc775ed7f	
12675) Found file: C:\Windows/diagnostics/system/HomeGroup/DiagPackage.dll	
Hash: 7dec7fea00f9612eba5125015bd109f5	
12676) Found file: C:\Windows/diagnostics/system/HomeGroup/Microsoft-Windows-HomeGroupDiagnostic.Interop.dll	
Hash: 094829f4bbd83035e388dd234e45f86e	
12677) Found file: C: Windows/diagnostics/system/HomeGroup/Microsoft-Windows-HomeGroupDiagnostic.NetListMgr.Interop.	dll
Hash: 4dad5b3263a2ac2baeafc450ded119c0	
12678) Found file: C:Windows/diagnostics/system/IEBrowseWeb/DiagPackage.dll	
Hash: ff9f67ab23bc66ff5705d56cc2963917 12679) Found file: C:\Windows/diagnostics/system/IESecurity/DiagPackage.dll	
Hash: 9blad695bbbccdb83e053557bd9f2d	
nash: 501200752000CC00520535370005720 12680) Found file: C:\Windows/diagnostics/system/Networking/DiagPackage.dll	
Hash: 5a72e3b206e9649e6d313ee57b89f3	
12681) Found file: C:\Windows/diagnostics/system/Networking/NetworkDiagnosticSnapIn.dll	
Hash: 2fa53b758a8c7f3fa66836c89339afe7	
12682) Found file: C:\Windows/diagnostics/system/PCW/DiagPackage.dll	
Hash: 7b4ff08e778f07ec46298fd22ab797d7	
12683) Found file: C:\Windows/diagnostics/system/Performance/DiagPackage.dll	
Hash: a00be81c36cf2651c7ce1e2eedbdfffd	
12684) Found file: C:\Windows/diagnostics/system/Power/DiagPackage.dll	
Hash: 876495f00e6cb496ecb72d8f5bdb86bd	
12685) Found file: C:\Windows/diagnostics/system/Printer/DiagPackage.dll	
Hash: 276269e48e0acf045eac10fb10f797e5	
12686) Found file: C:\Windows/diagnostics/system/Printer/UpdatePrinterDriver.dll	
Hash: 83d89e1657e448721058f682aec0ba60	
12687) Found file: C:\Windows/diagnostics/system/Search/DiagPackage.dll	
Hash: bdd23008f07a0611098c910b545ba2cb	
12688) Found file: C:\Windows/diagnostics/system/UsbCore/DiagPackage.dll Hash: 5115de580fbde0f9f6304600489eb250	
nash: JIJUEJoorDueorJooJooodoodoologJoo 12689) Found file: C:Windows/diagnostics/system/WindowsMediaPlayerConfiguration/DiagPackage.dll	
Hash: Solabea9402cefaddea0669623cb	
12690) Found file: C:\Windows/diagnostics/system/WindowsMediaPlayerMediaLibrary/DiagPackage.dll	
Hash: a6a81efb930c226b06e92ffbec3fcb5a	
12691) Found file: C:\Windows/diagnostics/system/WindowsMediaPlayerPlayDVD/DiagPackage.dll	
Hash: 3040be46af9f50a6c600dfd19a4c1220	
12692) Found file: C:\Windows/diagnostics/system/WindowsUpdate/DiagPackage.dll	
Hash: fadb557dd4aa5f2d69b2c07c22638845	
12693) Found file: C:\Windows/servicing/CbsApi.dll	
Hash: f1720df60212ba9baa98a542119d69a4	
12694) Found file: C:\Windows/servicing/CbsMsg.dll	
Hash: 4b805e20ee9dc7897ad390459cd06d34	
12695) Found file: C:\Windows/servicing/wrpintapi.dll	
Hash: 9585f51ff09bdfa336f1475520583ca7	
12696) Found file: C:\Windows/RtlExUpd.dll	
Hash: 2a7b78f4cfa0f1a5655891ddaacefad9	
12697) Found file: C:\Windows/twain.dll Hash: 0bea3f79a36b1f67b2ce0f595524c77c	
nasn: vbeasr/yasbolt6/b2cet7595524C//C 12698) Found file: C:Windows/twain 32.dll	
Hash: darb63d52fr2b1676aa96e621e68	
<	

Fig. 30 The clean.txt file with all the *.dll files of the clean Windows 8 installation.

(12698 results)

	log.txt - Σημειωματάριο	- 🗇 🗙
Αρχείο Ε	Επεξεργασία Μορφή Προβολή Βοήθεια	
15522)	Found file: C:\wamp/bin/php/php5.4.16/icuin49.dll	^
Hash: 2	2fc93eee81cbcf56f9aa1eac989cdcdd	
15523)	Found file: C:\wamp/bin/php/php5.4.16/icuio49.dll	
Hash: c	:1ab4944e12135c911ee7e1036a4dd8b	
15524)	Found file: C:\wamp/bin/php/php5.4.16/icule49.dll	
	v814f28ebd6e06b3cb0a7dd37a7db6c3	
	Found file: C:\wamp/bin/php5.4.16/iculx49.dll	
	34ddd4f22fd92ce2bb2edc2506860f6f	
	Found file: C:\wamp/bin/php/php5.4.16/icutest49.dll	
	8d80d139365f5afda49e000a1d38816	
	Found file: C:/wamp/bin/php/php5.4.16/icutu49.dll	
	18-7-877/d7959497/d0a7eddff255be5	
	Found file: C:\wamp/bin/php/php5.4.16/icuuc49.dll f9de78c85e2deabalc274c834f621b	
	irou/rocobec/cdabalc/4C04HO2LD Found file: C:\wamp/bin/php/php5.4.16/libeay32.dll	
	Found Title: C: (wamp/Dif)/pit/pit/pit/pit/pit/pit/pit/pit/pit/pit	
	Dud file C: Vwamp/bin/php/bin/php.4.16/libenchant.dll	
	Solable2-06-2048-240557ce+61422a	
	Found file: C:\wamp/bin/php/php5.4.16/libenchant ispell.dll	
	2386bac8a64953316bcd4817289d35e	
	Found file: C:\wamp/bin/php/php5.4.16/libenchant myspell.dll	
	3702745fd9589a5e25837315affa5f02	
	Found file: C:\wamp/bin/php/php5.4.16/libpq.dll	
	546268cccce67d9df5ccc65b729f5d69	
	Found file: C:\wamp/bin/php/php5.4.16/libsasl.dll	
	0fe364b483df847c8ce91390e01d6e18	
15535)	Found file: C:\wamp/bin/php/php5.4.16/php5apache2_2.dll	
Hash: 0	02b96cb2ce4d91f5e15c910781241e88	
15536)	Found file: C:\wamp/bin/php/php5.4.16/php5apache2_2_filter.dll	
Hash: 1	Lc15a147ed27f1e411b9d30a00c93164	
15537)	Found file: C:\wamp/bin/php/php5.4.16/php5apache2_4.dll	
	113163101732e5d96ed917a44fe259b4	
	Found file: C:\wamp/bin/php/php5.4.16/php5nsapi.dll	
	/ae4cc4d580ad00c3efb91f185099434	
	Found file: C:\wamp/bin/php/php5.4.16/php5ts.dll	
	34e1a5b5F325d115c884bc2192c7324c	
	Found file: C:/wamp/bin/php/b5.4.16/ssleay32.dll	
	2883341b17e5067e95f81c36bcc5853	
	Found file: C:\wamp/tools/xdc/Aga.Controls.dll	
	Jd82db175493fc8e679994a49b8e3fa1 Found file: C:\wamp/tools/xdc/ICSharpCode.TextEditor.dll	
	Found File: C: (wamp/1001s/X0C/1CSharpCode.TextEditor.dl) F903786c431892f60f5hba93c7048	
	Found file: C:\vamp/tools/xdc/WeifenLuo.WinFormsUI.Docking.dll	
	Pound Tite: C. (wamp/cols) Adc/meifentad.winFormsof.bocking.uii 9073/1136044dd844ebc3489490de	
	Found file C: \windows,RtExUpd.dll	
	Joint Title (Millows/Millows/Millows/	
	Found file: C:\Windows/twain.dll	
	bea3779a36b1f67b2ce0f595524c77c	
	Found file: C:\Windows/twain 32.dll	
	Ja7eb5d3652fe2b1676aaa9e6e241e68	
		~
۲		>

Fig. 31 The log.txt file with all the *.dll files of the whole computer, partition C.

(15546 results)

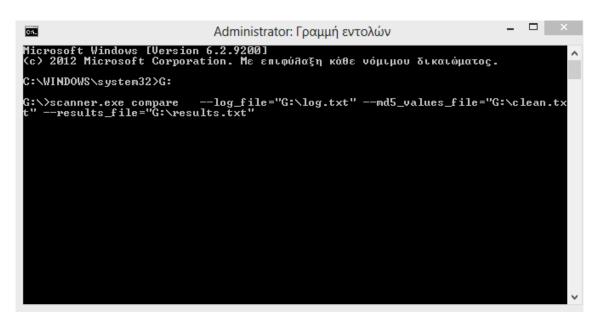
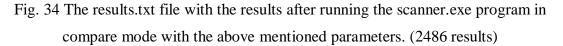


Fig. 32 Commands needed for running the scanner.exe program in compare mode as mentioned above. (run as administrator)

Administrator: Γραμμή εντολών – 🗇 🗙
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_pdo_pgsql.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_pdo_sqlite.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_pgsql.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_shmop.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_snmp.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_soap.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_sockets.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_sqlite3.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_sybase_ct.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_tidy.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_xmlrpc.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ext/php_xsl.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/zend_ext/php_xdebug-2.2.3-5.4 -vc9.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/glib-2.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/gmodule-2.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/icudt49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/icuin49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/icuio49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/icule49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/iculx49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/icutest49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/icutu49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/icuuc49.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/libeay32.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/libenchant.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/libenchant_ispell.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/libenchant_myspell.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/libpq.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/libsasl.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/php5apache2_2.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/php5apache2_2_filter.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/php5apache2_4.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/php5nsapi.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/php5ts.dll
Suspicious file found -> C:\wamp/bin/php/php5.4.16/ssleay32.dll
Suspicious file found -> C:\wamp/tools/xdc/Aga.Controls.dll
Suspicious file found -> C:\wamp/tools/xdc/ICSharpCode.TextEditor.dll
Suspicious file found -> C:\wamp/tools/xdc/WeifenLuo.WinFormsUI.Docking.dll
G:\>

Fig. 33 The results after running the scanner.exe program in compare mode as mentioned above.

7					results.txt - Σημειωματάριο	- 0 ×
Αρχείο	Επεξεργασία Ν	Λορφή	Προβ	ολή	Βοήθεια	
2437)	Suspicious	file	found	->	C:\wamp/bin/php/php5.4.16/ext/php intl.dll	
2438)	Suspicious	file	found	->	· C:\wamp/bin/php5.4.16/ext/php_ldap.dll	
2439)	Suspicious	file	found	->	<pre>C:\wamp/bin/php/php5.4.16/ext/php_mbstring.dll</pre>	
2440)	Suspicious	file	found	->	<pre>C:\wamp/bin/php/php5.4.16/ext/php_mysql.dll</pre>	
					<pre>C:\wamp/bin/php/php5.4.16/ext/php_mysqli.dll</pre>	
					C:\wamp/bin/php5.4.16/ext/php_oci8.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_oci8_11g.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_openss1.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_pdo_firebird.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_pdo_mysql.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_pdo_oci.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_pdo_odbc.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_pdo_pgsql.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_pdo_sqlite.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_pgsql.dll	
					· C:\wamp/bin/php/php5.4.16/ext/php_shmop.dll · C:\wamp/bin/php/php5.4.16/ext/php_snmp.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_soap.dll C:\wamp/bin/php/php5.4.16/ext/php sockets.dll	
					C:\wamp/bin/php/php5.4.16/ext/php_sockets.dll	
					C: (wamp/bin/ppip/pip/sit/set/pip_sqltes.dlt C: (wamp/bin/ppip/bin/set/php5.4.16/ext/pip_sybase ct.dll	
					C: (wamp/Dir/php/php/s.4.16/ext/php_subsect.dir C: (wamp/bir/php/php5.4.16/ext/php_tidy.dll	
					C: (wamp/bin/php/php5.4.16/ext/php_cluy.ull C: (wamp/bin/php/php5.4.16/ext/php_mlrpc.dll	
					C: (wamp/bin/php/php5.4.16/ext/php_xsl.dll	
					C: (wamp/bin/php/php.4.10/exc/php_A11011 C: (wamp/bin/php/php.4.16/zend ext/php xdebug-2.2.3-5.4-vc9.dll	
					C: \vamp/bin/php/php54.16/glb-2.dll	
					C: \vamp/bin/php/php5.4.16/gmodule-2.dll	
					C:\wamp/bin/php/php5.4.16/icudt49.dll	
					C:\wamp/bin/php/php5.4.16/icuin49.dll	
					C:\wamp/bin/php/php5.4.16/icuio49.dll	
					C:\wamp/bin/php/php5.4.16/icule49.dll	
					C:\wamp/bin/php/php5.4.16/iculx49.dll	
2469)	Suspicious	file	found	->	C:\wamp/bin/php/php5.4.16/icutest49.dll	
2470)	Suspicious	file	found	->	C:\wamp/bin/php/php5.4.16/icutu49.dll	
2471)	Suspicious	file	found	->	C:\wamp/bin/php/php5.4.16/icuuc49.dll	
2472)	Suspicious	file	found	->	C:\wamp/bin/php/php5.4.16/libeay32.dll	
2473)	Suspicious	file	found	->	C:\wamp/bin/php5.4.16/libenchant.dll	
2474)	Suspicious	file	found	->	· C:\wamp/bin/php/php5.4.16/libenchant_ispell.dll	
475)	Suspicious	file	found	->	C:\wamp/bin/php/php5.4.16/libenchant_myspell.dll	
476)	Suspicious	file	found	->	C:\wamp/bin/php/php5.4.16/libpq.dll	
					C:\wamp/bin/php/php5.4.16/libsasl.dll	
2478)	Suspicious	file	found	->	<pre>C:\wamp/bin/php/php5.4.16/php5apache2_2.dll</pre>	
2479)	Suspicious	file	found	->	<pre>C:\wamp/bin/php/php5.4.16/php5apache2_2_filter.dll</pre>	
					<pre>C:\wamp/bin/php/php5.4.16/php5apache2_4.dll</pre>	
					<pre>C:\wamp/bin/php/php5.4.16/php5nsapi.dll</pre>	
					C:\wamp/bin/php/php5.4.16/php5ts.dll	
					<pre>C:\wamp/bin/php/php5.4.16/ssleay32.dll</pre>	
					C:\wamp/tools/xdc/Aga.Controls.dll	
					<pre>C:\wamp/tools/xdc/ICSharpCode.TextEditor.dll</pre>	
2486)	Suspicious	tile+	found	->	C:\wamp/tools/xdc/WeifenLuo.WinFormsUI.Docking.dll	
_						
						>



As we can verify the results.txt file contains all the *.dll files of the whole partition C except the *.dll files that are included in the Windows 8 installation file.

In the next chapters, two versions of the scanner.php and scanner.exe programs are presented, which implement some differences and alterations that could be useful to the investigator.

4.5 The scanner_version_2 program

This version of scanner.php and scanner.exe has this difference: for the comparison in the compare mode, uses as the md5_values_file with all the clean MD5 values, a *.txt file that contains only MD5 values and nothing else. This *.txt file consists of one MD5 value in each separate line and nothing else. So when the user inserts from the command prompt, the path of the md5_values_file with all the clean MD5 values (that we don't want to take into consideration during the investigation), this file consists of one MD5 value in each separate line and nothing else.

All the other functionality of the program remains unchanged.

This differentiation was necessary in order, for the program, to have the ability to utilize and exploit possible dump files from other programs or other created files that contain only MD5 values. This makes it more valuable for commercial use. The first program has the restriction that works only with files that were created with the scan mode of the same program.

4.6 The scanner_version_3 program

This version of scanner.php and scanner.exe has this difference from the first program: for the comparison, in the compare mode, uses as the md5_values_file, with all the clean MD5 values, a *.txt file that contains only MD5 values and nothing else, but also has the ability to create these *.txt files with only MD5 values inside by using the scan mode of this version of the program.

So the user has the ability to create a *.txt file with only MD5 values inside but also afterwards compare this file with the log file (log_file) created from the first or the se-cond program.

All the other functionality of the program, and the way it is used, remains unchanged.

This differentiation was necessary, in order for the user to have the ability to create himself the *.txt files with only MD5 values inside, in order to use them as input for other programs or for investigation reasons. This makes it more valuable for trial and investigation use.

In the below example we used the scanner_version_2.exe and scanner_version_3.exe programs from a USB stick (G drive) to demonstrate their use.

For the specific example we created the two files to make the comparison as following: for the clean MD5 values file, with only MD5 values inside, we used the scan mode of the scanner_version_3.exe to create a file with all the *.log files of a clean Windows 8 installation (scanner_version_3.exe scan --path="C:\Windows" --extension="log" -- log_file="G:\clean.txt") and for the MD5 values under investigation (.txt file that includes the path and the hash code of each file) we used the scan mode of the scanner_version_2.exe to create a file with all the *.log files of the entire computer, partition C (scanner_version_2.exe scan --path="C:\\" --extension="log" -- log_file="G:\log.txt").

Figures 35, 36, 37, 38, 39, 40, 41, 42 and 43 visualize this functionalities of the programs.

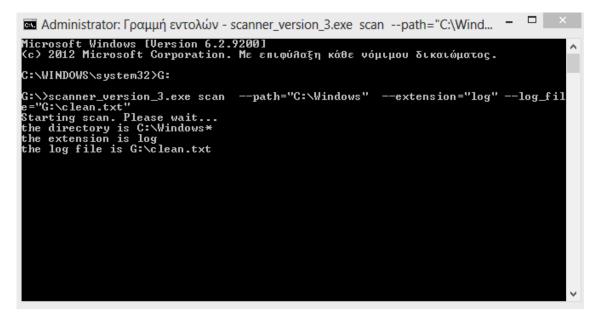


Fig. 35 Creating the clean.txt file with only MD5 values inside by using the scanner_version_3.exe program in scan mode.

C34.	Administrator: Γραμμή εντολών 🗕 🗇 🛛 🗡				
_	UsageLogs/NGenTask.exe.log"				
CLR_v4.0_32∕) "C:\Windows/System32/config/systemprofile/AppData/Local/Microsoft/ UsageLogs/taskhost.exe.log"				
CLR_v4.0_32∕	> "C:\Windows/System32/config/systemprofile/AppData/Local/Microsoft/ UsageLogs/taskhostex.exe.log"				
	"C:\Windows/System32/sru/SRU.log"				
	"C:\Windows/System32/sru/SRU00502.log"				
	"C:\Windows/System32/sru/SRU00503.log"				
	"C:\Windows/System32/sru/SRU00504.log"				
	"C:\Windows/Temp/vmware-SYSTEM/vmware-usbarb-SYSTEM-3068.log"				
	"C:\Windows/Temp/vmware-SYSTEM/vmware-usbarb-SYSTEM-5724.log"				
	"C:\Windows/Temp/ASPNETSetup_00000.log"				
	"C:\Windows/Temp/MpCmdRun.log"				
[73]=> string(32) [74]=>	"C:\Windows/Temp/Silverlight0.log"				
	"C:\Windows/Temp/SilverlightMSI.log"				
	"C:\Windows/Temp/chrome_installer.log"				
	"C:\Windows/Temp/vminst.log"				
	"C:\Windows/Temp/winstore.log"				
	"C:\Windows/WinSxS/pogexec.log"				
	"C:\Windows/debug/WIA/wiatrace.log"				
	"C:\Windows/debug/mrt.log"				
	"C:\Windows/debug/mrteng.log"				
	"C:\Windows/debug/netlogon.log"				
	"C:\Windows/debug/sammui.log"				
	"C:\Windows/inf/setupapi.app.log"				
	"C:\Windows/inf/setupapi.dev.20130730_200027.log"				
	"C:\Windows/inf/setupapi.dev.log"				
	"C:\Windows/inf/setupapi.setup.log"				
	"C:\Windows/security/logs/scesetup.log"				
string(27) [90]=>	"C:\Windows/security/edb.log"				
string(25) [91]=>	"C:\Windows/DtcInstall.log"				
string(23) [92]=>	"C:\Windows/KB835221.log"				
	"C:\Windows/MSI30-KB884016.log"				
	"C:\Windows/PFRO.log"				
	"C:\Windows/WindowsUpdate.log"				
string(22) [96]=>	"C:\Windows/chipset.log"				
string(18) [97]=>	"C:\Windows/iis.log"				
	"C:\Windows/vmgcoinstall.log"				
	Warning: md5_file(res:///PHP/C:\Windows\System32\catroot2\edb.log): failed to op en stream: Permission denied in scanner_version_3.php on line 1				
G: \>					

Fig. 36 The results after running the scanner_version_3.exe program in scan mode.

heqP6ard809673.340cBabc64bc55a ^ begR84D8794973.580664bc971.6401		clean.txt - Σημειωματάριο	- 🗇 🗙
22820879494995965065097949555 9974aee5785171e9995764089555 19872064267280745473291408557 5312489064267284732643185637 154733008908426728473543185637 154733008908426728478643244344 97715740259074084528346452444344 97715740259074084528346452444344 97715740259074084528346452444344 9771574025907408452833464559 1771574025905426504528334 9771574025905426504528334 9771574025905426504528334 9771574028054274504528334 978174457594864528344524 97817445759486452834545459 978174457594864528345459 978174457594864528345459 9781744575948645283345476957 9781744575948645283345476957 9781744575948645283345476957 9781744575948645283454767574 97817445759486452834547677574 97817445759486452844487452823916457 97817445759486452844487452823916457 97817445759487976595759 978174457594897976595759 978174457594897976595759 978174467592897764957759 9781744675928977649577549 9781744675928977649577549 97817446759284449745228977649 978174467592844977852897769 978174467598848977264775459 978174467598977649379759 978174467598977649379759 978174467598977649379769 978174467598977649379769 978174467598977649379769 978174647597897769 9781746475978978977579 97817464759828497764577549 97817464759786977549 97817464759786977578 97817464759786977569 97817444597898077757769 97817464759786977569 97817464759786977569 97817464759786977569 97817464759786977569 97817464759786977569 97817464759786977569 97817464759786978775789 97817464759786977569 97817464759786977569 97817464759786977569 9781746475978697877569 9781746475978697877569 97817464759786978775789 97817464759786978775789 97817867647877869787878775789 9781786764787786978788775789 97817867647877869787885775789 9781786764787786787788 9781786764787788789786978775789 97817867647877887887877887878788787887878	Αρχείο Επεξεργασία Μορφή Προβολή Βοήθεια		
la adf. 500: dat. 2009 fc. 600 399.0550 9241 acc. 670 371 14: 14: 14: 14: 14: 14: 14: 14: 14: 14	99e40f8afd0196f334bc0eab664bc95a		^
994aacs78511eb0577b443c2931d4 5147290643dc72547752043185e37 52765933040be3c422eabeccadac0235 52505930540252eabeccadac0235 52505930540252eabeccadac0235 527654052054045204325ea0675307 576012065740543804230434300 1077c426302654045043434309 57601206740543804253464514383 5270575405295405405438345446414380 5270575405295405405438345446414380 527057540529540540543834546414383 527057540529540540543834546414383 527057540529540540543834546414383 527057540529540540543834546414383 527057540529540540543974549 5270575405295405405495405414534854495 52705754052954054054954054145348549867405 52705754052954054054954954054145348549867405 52705754052954054054954954054145348549867405 52705754052954054054954954054145348549867405 5270577540405795295405405475 52807774446790299049674755494 528077754446790299049674755494 52807375409511990529055175769 52807375409511990529055175769 528073754095219905897557509 5280737446790290942054571467952 5280737446790290942054571467952 5280737446790290942054571467952 5280737446790290942054577549 5280737446790290942054511935444465 5280737446790290942054511935444465 528074744679029094205450577549 528074744679029094205450577549 528074744679029094205450577549 528074744679029094205450577549 52807474467902904205450547677549 52807474467902904205450547677549 52807474467902904205450547677549 5280747446790290420545057106775549 5280747446790290420545057106775549 5280747446790290420545057106775549 528074744549020927475449 52807475444590590577549 52807474454459058046767754949 52807474454459058047677549 52807474454459058047677549 5280747454459459247454524545348 528074592774052896405757549 528074744545905804767754949 528074744545905804767754949 52807545454445995547546404239559778 528075475444459555757669 52807474474745656588 528075578576580 528075578576580 528075578576580 52805656867657858 52805656867657858 52805656867657858 52805656867657858 52805656867657858 52805656867657858 52805656867657858 5280565686765785 52805656766779878 528056568646578588 52	0b28e820b7949c93658d6c49bfa1c041		
3311efeek-Gri078b43c20241d4 14720640at/C54752b431b5837 h5256330400bae4fc30eb1c60111 55265330400bae4fc30eb1c60133 5506506fdb15f8044623d4c343c0 5506506fdb15f8044623d4c343c0 576724630ec64049548c2c2e1d7 476374253b7280402335g4f1653ee 4763744253b728042335g4f1653ee 4712304075347353436f1f835ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042335g4f1653ee 370253be2528042835g4f76753 370253be25280428042397b553be4276 370253be2528042804297b25353756 370253be25280397b556de276 370253be25280397b556de276 370253be25280397b556de276 370253be25280397b5596de276 380203461212028042812397b553be27756 380203461212028042812397b553be27 3802034512120528047b27754395 3802034512120528047b27754395 380203452804728027b2404287 380203452804728027b2404287 380203452804728027b2404287 380203452804728027b2404287 3802034528047280775495 380203452804780775495 380203452804780775495 38020452804748772804780780 3802045232804780775495 38020452804780775495 38020452804780775495 3802045232804780775495 3802045232804780775495 3802045232804780775495 3802045232807780775495 3802045232807780775495 3802045232807780775495 3802045232807780775495 3802045232807780775495 3802045232807780775495 3802045232807780775495 38020452328077807776495 38020452328077807776495 38020452328077807778495 38020452328077807778495 38020452328077807778495 38020452328077807778495 38020452328077807778495 38020452328077807778495 380204523280780778778078078777807807877780780787787	41aa0fc59bc4da7c990fc6409399d55b		
514729045yd272475yd32040byd2422ebecaddd0325 5721693904222ebecadd0320433c0 5721693904222ebecadd0320433c0 5721693904222ebecadd0320433c0 57264502046347534623046344734633c0 57275472575757 57285129641633364534645347555757 5728512964163338244853 572931296116333824163383634855 572931296116333824163383634855 57293129811633382418455 57294129811633382418455 57294129811633382418455 57294129811633382418455 5729412981163338241843874986 572941298116343824184374986 572941298116343824184374986 57294129811634384218448374986 572941298116343842184444542523113474748 57294129811398043977598044214748 5729412981139804397757498 57299541298113981439747757489 572995412981139814374374844598299864144759299864 57299754129854980797757489 57299754129854980797757489 57299754129854980797757489 57299754129854980747757489 57299754985498074184753199347444545239965 572997549854980741847534199437429 572997549854980747757489 57299754985498748976186531935337489 5729754978654989449844789	d09f4aaee657851f1e9b995fe408b57c		
hz5r6333400bae4fc30ebc1c60111 hz5r6333400bae4fc30ebc1c601925 hz5r6333400bae4fc30ebc20abc43430c0 hz5r635340bc22abeccda0fc9325 hz5r6353540bc23335cf140543cc327050bc3511 hz12325bf235bc23335cf16557 hz6r5355534ac6124798225 hz6r5355534ac6124798235 hz6r53553440c42284798235 hz6r5458425942748444be74525291fc87 hz6r5458425942748444be745253448c347855 hz6r5458425942748444be7452531fc8787 hz6r5458735546674278235 hz6r54777848444be7452891fc8787 hz6r54777848444be7452891fc8787 hz6r54777848444be7452891fc8787 hz6r54777848454827841827848278487887 hz6r547778484548787847887 hz78784548788787878788 hz7878454878787878788 hz7878454878787878887887878788 hz87878487878878787787489 hz87878487878878787787489 hz87878487878878787787489 hz878784878788787877877849 hz87878487878878787878788 hz887878887878878787878788 hz887887887878878787878788 hz8787888787878787887878878787887878878	453211e4eeb4c5d7078b443c0291d1c4		
552165906ad2ac2abeceadadc325 55065906ad2ac2abecedadc3445443c4 b77642630ce6d4463442cac34346 b77642630ce6d4463442cac37566517d7 7761374254745745464f1f1635ace 127082555bc53565104583334cf1c53sec 127082555bc53565104583334cf1c53sec 127082555bc53565104583334cf1c53sec 12708255bc5356104583333ccf1c53sec 12708255bc53550440583334cf1c53sec 12708255bc535504405843334cf1c53sec 12708255bc535504405843334cf1c53sec 12708255bc535504405843334cf1c53sec 12708255bc535504405843334cf1c58 1571825782784256343511445824e9046 157182578278059375690427412824 158118325412647828678678775490 15811832541264782867867757649 15811832541264782867867757649 1583059905255135194757549 1583059378506427478428698660649 15830593286136151313931544463 158305932861361513933454897c1c26756 1584054974164928644978742848978614493 1584054974164928678727 15130486528172c4505891148615c159 158534269355911486475705 15130486528172c450583591148647577 15130486528172c450583591148647577 15130486528172c4505853591148647577 15130486528172c4505835591148	251ef290649adc7254f752b434185e37		
TobBesdericht 1: Fred dut Abzulau - La dut For Zuck 2: Sole - Cert 4: Fred dut Abzulau - La dut For Zuck 2: Sole - Cert 4: Fred dut Abzulau - La dut For Zuck 2: Sole - Cert 4: Fred dut Abzulau - La dut For Zuck 2: Sole - Cert 4: Fred dut Abzulau - La dut For Zuck 2: Sole - Cert 4: Fred dut Abzulau - La dut For Zuck 2: Fred du	bfb25f63330400bae4fc300eb1c60111		
bb77e46630e.c644f0346.22e.d1471 Fr/ed120bc/fda49c.ae3759683141 a: 139037055475334cf0f1635ec 1270e255bc536540b828339cdfb.0557 2270e255bc536540b828339cdfb.0557 2270e255bc536540b828339cdfb.0557 2270e255bc536540b828339cdfb.0557 2270e255bc536540b828339cdfb.0557 2270e255bc536540b828393cdfb.0557 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e255bc536540b828392dfb.0582 2270e25520dfb.05827b04557540 2280b924520b3275c510b4220b292dfb.058551 2280b9328661285119435210943261 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943271c5550412 2280b328661285210943286045610 2280b328661285210943286045610 2280b328661285210943286045610 2280b328661285210943286045610 2280b3286612852109428510272829 2280b3286612852109428510272829 2280b3286612852109428510272829 2280b3286612852109428510272829 2280b3286612852109428510272829 2280b3286612852109428510272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328661285501272829 2280b328627670829 2280b328667670829 2280b328667670829 2280b328667670829 2280b328667670829 2280b328667670829 2280b328667670829 2280b328667670829 2280b328667670829 2280b328667670829 2280b32867670829 2280b3280b77888977888 2280b328677788889778	64521059036a2d2e2eabeecadadc9325		
Fr/d574425b47a/db22esie0F5b7d57 Fr/d57425b47db434esie76768a51d1 ac11293075a547b534a6c147635ece 12704255be57567b382833ydc14fb35ec 2706255be375254abc2037978236 280b67c7cba8891df6378c256 280b67c7cba8891df6378c2 280b75c82 280b75c82 <t< td=""><td>37b50e5d96fdb15f8dd4462da4c43dc0</td><td></td><td></td></t<>	37b50e5d96fdb15f8dd4462da4c43dc0		
7-#dd12bc+Cfd0a40c-as27968a5141 112930757-657534670116155 1270a255bc>25bc>2	40b77e246630ce6d4f0548c22ced1471		
ak 1290375a57k554bb28339c4tfc57 27b235bb263554bb28339c4tfc57 27b235bb263554bb28339c4tfc5778236 28bb67c7cba8891dfd5438c34f65b 151f47247b428b4d4bb278c2391fa787 59bf148c35rba4022e1d4882fe96f6 5359905cc37f348c1d987c78128c 589905fc37f348c1d987c78128c 58905ffc37f348c1d987c78f28c 58905fc37f28d298c9fc18f551193f74c 58905ffc37f348c 58904754f1218d882d848g97fc657f348c 58905ffc37f28c 58905fc38fc38f648f978c 58905ffc37f28f28d986fc48b71be84c2 58905ffc37f28f28d986fc48b71be84c2 58905ffc37f28f28d986fc48b71be84c2 58905ffc37f28f28d986fc48b71be84c2 58905ffc37f28f28d986fc48b71be84c2 58905ffc38f78b716f28f28f28f28f28f28f28f28f28f28f28f28f28f	8e7fd574425b47ad0a25e3e60f5b7d57		
1270e255be52654bb2839c4fbc577 280bf727cb89811df53483cf49fb 562dc91c4832653adce2d297e8236 15472072844dba726s2317467 F9abf14e35fbad0220e144882fe90f6 573967b6cc3185d1c0fear4711820 2668d871c48033960057556de42ffe 1011380dc871745362d887c676372c 336274bf121692897b655377368 31362744bf92b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744dcf902b932f1c35e55c1 536871744bcf902b932f1c35e55c1 536871744bcf902b932f1c35e55c1 536871744bcf902b932f1c35e55c1 536871744bcf902b932f1c35e55c1 536871744bcf902b932f1c35e55c1 536871744bcf902b932f1c35e55c1 536871744bcf902b932f1c35e55c1 53687174bcf01525526552b1 536872545b1 536872545b1 53687254552656871cc740473762 53687254552658804c230259b1 5368725455265805458256265855 5368725454564805585 536872545456448052372c39805786780776 536872545456448052372c3980578678077687 536872545456448052372c3480767877 5376872648464238228598578644805787 5368725454556444782382844785478555645454478 53685267876444782382844785478555645454478 5368526787644478784547884784478880447873547887 536852678746478788458478478847847884784788878478878478878847847	6f7ed0120bc6fd0a49cae367968a51d1		
28bb7/crb/a8b91dr054abc.2449bb 28bb7/crb/a8b91dr054abc.2449bb 28bb7/crb/a8b91dr054abc.2449bb 28bb7/crb/a8b91dr054abc.244832r90f6 79ab714a57bad022be14d832r90f6 553969bbcc.3185d1c0fac7dr12182d 26ed8071c088939b057b596d82ffe 1b011111111111111111111111111111111111	cac3129d3075a547b534a6fd1f635ece		
Fó2Le91c4832625adaced2497e8236 Fó2Le91c4832625adaced2476 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad8228c1448827e90f6 Fj9abf14257bad828c1448627e90f8657575d9 Fj1abj24c14bad778b328e9a66f9 C588717f44d67902b99a271c45551 St909336c97105155159c2-2299cf Fj2abf3139037a4acc 888bdd9254146425165159f2-2299cf Fj2abf3139037a4acc 888bdd9254146425165159f2-2299cf Fj2abf3139037a4acc 888bdd9254146425165159f2-2299cf Fj2abf313937f2 Pedaced8a92cb283a0f21c479f35b41bd 988bd32561446749f33189454194705 988bd3256146214956216449735 988bd325614621482316444518193642 988bd32562146214893616125148 988bd325542948492851572e408ced6a 988bj26467144793baek265561438 988534298880cd768b71be4082 988534298880cd768b71be4082 988880cd768b71be4082	41270e255be52654bb828339cdfbc957		
161 f+ 72472a8d4dbp 745 c2391 f+ 874 163 f+ 27677a8d4d22be14882 f+ 9966 175 350 590 55 cc 31356 f+ 9966 175 350 570 56 dc 274 e 181 182 52 c1 416b 4c 770 1828 95 ac 666 e f0 1580 174 4dc 670 920 592 11 c1 565 5c 1 1580 174 4dc 670 920 592 11 c1 565 5c 1 1580 174 4dc 670 920 592 11 c1 565 5c 1 1580 174 4dc 670 920 592 11 c1 655 5c 1 1580 174 4dc 670 920 592 11 c1 c1 655 5c 1 1580 174 4dc 670 920 592 11 c1 c1 c7 754 d93 180 321 20 50 300 7 7 775 74d9 3 180 489 12 90 482 21 c3 4c 310 917 36c 1 180 489 12 90 482 21 c3 4c 310 917 36c 1 180 489 12 90 482 21 c3 4c 310 917 36c 1 180 489 12 90 482 21 c3 4c 310 917 36c 1 180 489 12 90 480 23 21 c3 4c 310 917 36c 1 180 489 12 90 480 23 24 c9 8a 91 c1 647 193 3b ca 180 52 c2 c1 80 5c c1 55 5c c1 c3 as 180 52 c2 c1 80 5c c1 55 5c c1 c3 as 180 52 c2 c1 80 5c c1 55 5c c1 c3 as 180 52 5c c1 55 5c c3 c1 as 80 7 c2 c1	c28bb67c7cbe38891dfd543a8c34f05b		
Fabrilation Fabrilation Fabrilation Fabrilation Stone	d962dc9e1ca832625adaced2497e8236		
PabeTLad3STp.ad0220012408827e09f6 2539699b5cca3185d1c6faar7d7182d 25804871cc0889330837b556ded27fa 253859919b5c6da127fa 25804871cc1889330837b556ded27fa 2538591754de076a129c 258071744de716922892a606ef0 258871754de076255521 2588712744db7022892a66164792159257c1 258882d932286518453113943744acc 288021a29d622b6280407e77575449d 2880ed93236618458113943744acc 2880ed9323651267427356411d 3484874545511cc77647376414d 2880ed932940938475104764756414d 3480e483724504371cc77407376414d 2880ed9329409384751047647576449d 2880e493231694945310973762 2980e39847540451045326574545cd3a 2885740961253223961f4dbc96 2982886476871045286574545cd3a 28857409612532239617440bc96 298498472404528575246080cccade 28857409612532239617440bc96 298457235559514040497804728475 28888647680710487627 2181334698464261580966139461255 288964693256164697667 2786572071144256480ece44935861644978617457480 2889864978616478710487627 21813346493586164744798a104807386777 28898644938661649786164579676 2786526464a647411442436c14338 28615362566558 2086562647441444935861645479676 778654146465169686646497861164897861648797180	2161fef20f2a84d44be745e2391faf8f		
533699bsce3185d1c4feq 5336274c6121645287 Dbd13189dde3773d58d2d8c76a129c 53362744f612169b2897b65b3775d0 11ba12c41db4c77b02be9a2f1cd5e55c1 55987157c60 5989adf93260c515c5159f2c2a299c 48802122b205add7e775f4043 889badf9326b13d581193193d144acd 88b4d971dbe35d48971c10c7b1e 889badf9326b13d581193193474acd 88b6d9215b159f2c27f406376b41bd 386483726b13d581193193752 88b6d925b149541947975f4043 88b6d9271db453b199737c2 988b6d9328b19974623b295054d4bc76 568c204c704db72b25b265d34a5199737c2 988b647328c306478b77b644bc3 568c204c704db72b325b2655b367c4dbc32b 984b29328b74a6478b77b644bc32b329504764bc32b329504764bc32b329504764bc32b329504764bc32b32950446b32b42988b7640b71ba4ba2d7 51335369376425245944b40876576 988b740671657b647b7 578c72cc704b1552355095144adb4073bF7708 988b744c5461ba996b19461c5b 578c731cc716680b4c44d42b3427566 988b744c5461ba996b19461c5b 578c731cc716680b4c4d42b3427566 988b744c5461ba996b19461c5b 578c731cc716680b4c4d42b44073bF7780 988b745611447436cb1333 50860bc5cc2d44d4938ca14b404767676 77765612665 578c731cc71680b144d4424676467676 7786512665c13828b4d4736c14343 5086bc5cc2d4444936ca14b4267586 578857477780 5086bc5cc2d4444936ca14b49767676	0f9abf14e35fbad0220e14d882fe90f6		
DeBuB11LcBB3390B337b596ded2ffe Lbd131B9de3f73d5Bd2d98C76a129c 336274bf612169b2897b45b53775d0 S11ab232c414bb4c77bb28e9a606ef0 S288717444b7982b98y21Lc3d5551 S288712744b76982b98y21Lc3d5551 S288712744b76982b98y21Lc3d5551 S289137444b7982b98y21Lc3d5551 S289137444b7982b98y21Lc3d550 S8804d93286618d581139d3fa4acdc S8804d93286618d581139d3fa4acdc S8804d9328618d571c74f9716b14b Sa8e4d93285b721c74f9716b14b Sa8e4d93285b294649895f124f9493beae 665ec6ardc9404b623a2936bf4adbc36 S989284938961d45871c74f94793beae 865ec6ardc9404b623a2936bf4adbc36 S989285f22fce00ecdca0 S3805f360bf5138725329864bf4b71be4082d S981374c428587b25769814b87bc27 S131b3b48652817ca6d568aee42c95e6 S482c44493bac164b473be777 S131b3b48652817ca6d568aee42c95e6 S482c4493bac164b473be777 S131b3b48652817ca6d568aee42c95e6 S482c4493bac164b473be7767 S78e55ac444f47bad404738b7762 S482b652817ca6d568aee42c95e6 S482b652817ca6d568aee42c95e6 S482b652817ca6d568aee42c95e6 S482b652817ca6d568aee42c95e6 S484562817ca6d568ae	0f9abf14e35fbad0220e14d882fe90f6		
httlsshde3r73ds8dzd98c76a129c a336274bf612169b2897b05b53775d0 s11ab23c414bb4c77bb289aa7b1c45e55c1 s508314570c2161551b9f2c2a299cf 4880212b2050add7e7f75fd9d1 s896add932b6618d581139d3fa4acdc s86bcd9c97140ea5a48e971c1c7b1e se8bcdd923bf139d3fa4acdc s86bcd923bf140ea5a48e971c1c7b1e se8bcdd923bf140e45a48b971c2c7fd975b41bd sade483f80dc423b1e3a45a19973c2 se4ba8252a45b3d571cc7fd975b41bd sade483f80dc423b1e3a45a19973r2c se4ba252a45b3d571cc7fd973b64b1bd sade483f80dc423b1e3a45a19973r2c se4ba252a445b283cff3b7b1be32a2e3b6bf4adc56 se4ba252a45b388bcfd6b71b45b28cf555bc63aa ae4b3526dc9888bcfd6b71b45b28cf555bc8 se7b53e4cc88a7bc353ca9a0762be3 s805dd92577509514da4b87bc77 s103bd4652817ca6d568aee42c95e6 sdc4r48a2b4c493besc14db47b1d45d5 sab3365c49e11442b58eesc74abe766 s7be5dc4aed473besc14b467676 s7ee552bec6daa647d114d243cc4b433 sd5ba4c493besc14b47b41d473besc1333 sd5ba4c493besc14b47b5768 sd5ba4c423897c68637be53b8 sd5ba4c4847ba4c4473besc14473besc147b445 sd5ba4c44443besc14443besc144345 sd5ba4c4443besc144345be1	10539699b5eca3185d1c0fae7df2182d		
a336274bf012169b2897b63b53775d0 811ab23c414bb4c770b289ea606ef0 538071744d6f902bb9a2f1cd5e55c1 54805143446f902bb9a2f1cd5e55c1 548051435741b46s5348971c1c775f403 8898ed03286f1845811393fa4acdc 8805d015c714b6a5348971c1c0c7b1e 5e48872a54b3d571cc7fd0f376b41bd 3a0e4837809da23b1e9a45a109f3762 949ac8d8a392d983bf104f9493baea 805sec0afc040d623a2396bf4edbc36 949cba2594d49285h2fe60edca0 caa88f7fa0bf610a5a26cf545dc3aa 8afb7160bf610a5a26cf545dc3aa 8afb73694c45088b9cd104b71b48a2d 9003f3adc583bre352a080762be3 981534c9984c5d511a996b19461c5b 981534c9984c45d51ba996b19461c5b 981534c9984c42d54b87bf2e6d238b75fc17 311b3b48652817cca668aee42c95e6 3adc4832abbf44fb0abd40738b75fc7 311b3b48652817cca68aee42c95e6 3adc4832abbf44fb0abd40738b76fc7 77ee5529e6daa647111427436cb333 34a5186415595acf7171147436cb333	c26e8d871cd8893900397b596ded2ffe		
81 lab23c414bb4cf78b28e9a686ef8 c588717f44d6f902b89a2f1cd5e55c1 539034365702615e5159f72c2a299cf te88021a29d82b2b28ba8d727f75f439d 889bc403286134581139345f4acdc 88bc403c9f140ea5a48e97c1c8c7b1e 98e387a54054571cc746975b41bd 3a0e4837a54054571cc7469715b41bd 3a0e4837a54054251c2674875b41bd 3a0e4837a54054571c2746975b41bd 3a0e4837a54054571c2746975b41bd 3a0e4837a54054571c2746975b41bd 3a0e4837a54054571c2746975b41bd 3a0e4837a54054571c2746975b41bd 3a0e4837a54054571c2746975b41bd 3a0e4837a54054571c274697555c123aa 2a6857f30fc74b57255095140ab876f27 3103b484c53817ca6d568ae42c556 3ac64832ab9f44fbbab440738bf767a 3103b484c53817ca6d568ae42c556 3ac64832ab9f44fbbab440738bf767a 3103b484c53817ca6d568ae42c556 3ac64832ab9f44fbbab440738bf767a 3103b484c53817ca6d568ae42c556 3ac64832ab144fbbab440738bf776a 32654831cc74b45bbab440738bf776a 32654831cc74b45bbab440738bf776a 32654831cc74b45bbab440738bf776a 32654831cc74b47bbab440738bf776a 33644518652817ca6d568ae42c556 33c447832abf44fbbab440738bf776a 33644518652817ca6d568ae42c556 33644518652817ca6d568bb444b2677566 33644518652817ca6d568bb444b2677566 33644518652817ca6d568bb444b2738bf776a 336451865c484744fbbab440738bf776a 336451865c484744fbbab440738bf776a 336451865c484744fbbab440738bf776a 33645186552817ca6d568bf444bbab4738bf776a 33645186552817ca6d568bf444bbab47378bf776a 33645186552817ca6d568bb44c4284555 346578531cc74b5748bf444bbab4738bf776a 346578531cc74b57445bbab44738bf776a 346578515cc757786511658bb4444738cb1343 346451865548bf7ca665165588bf7ca66548bf7786 3465785585777865116865548bf7ca665165588 347885361677857865176857865786 34788536176785786578657865788 3478853617665786578657865788 3478853617665786578657865788 347885361766578657865788 34788536176657865788 3478853617665786578867868578865788 3478856317c66598578653888888858888888888888888888888888	f1bd13189dde3f73d58d2d98c76a129c		
5887174446f992b992f1cdse55c1 5a9b934569702615e5159f2c2a99cf 48021a2904822b2b28ad7r2775f4d9d 8898cd49328661845811393fa4acd 8896cd9257404ea5348697c1cdc7b1e be48872a54b3d571cc746973fb41bd 3a0e48378004a23b1e9a45a109f3762 980ac8daa92c908a9fc1044993baea 65ecedar20404623a22b2b4edbc92642a8 65ecedar20404623a22b6548c40b71bc40a2d 90043f3ad6c58arb235c464bc926 8805d3697144c4br9364078c762 8805d3697144c4br9364078c762be3 88153dc987a4bc148398c1f48b71bc72be3 88153dc987a4bc14845285b72fc408b71bc40a2d 90043f3ad6c58arb2355269640a4b762be3 88153dc987a4bc44b93be167bc77 3103bd8652817cc6658aee42c95e6 34cf8a2babf44b93be61264978b766 77ee552e64dae473611447436cb333 34a45186415b95scd7171144745cb333 34a5186415b95scd7171144745cb333 34a5186415b95scd7171144745cb333 34a5186415b95scd7171144745cb333 34a5186415b95scd7171144745cb333 34a5186415b95scd7171144745cb333 34a5186415b95scd71741147436cb333 34a5186415b75scd71741147436cb333 34a5186415b75scd71741147436cb333 34a5186415b75scd71741147436cb333 34a5186415b75scd71741147436cb333 34a5186415b75scd71741147436cb333 34a5186415b75scd71741147436cb333 34a5186415b75scd71741147436cb333 34a5186415b755scd71741147436cb333 34a5186415b7558cd717475788 37855347444b3668ae265588 37855347444b3668ae265588 37855347444b3668ae265588 378553474445387768 17885286484741144736cb33876767 3785534374655388284d	5a336274bf612169b2897b05b53775d0		
Say Bas Jas Say Tool Sis Say Carlow Say Bas Jas Say Tool Sis Say Carlow Jas Bas Jas Say Tool Sis Say Carlow Say Carlow Bas Carlow <	d811ab23c414bb4cf70b28e9ea606ef0		
4e801.230482.2b2085.add7e7f75f403 e808.add93286618d581139d3fa4.acd 8806.dd93286618d581139d3fa4.acd 8806.dd93286618d581139d3fa4.acd 8806.dd93286618d581139d3fa4.acd 8806.dd9328618d581139d3fa4.acd 8806.dd9328618d581139d3fa4.acd 8806.dd9328618d581139d3fa4.acd 8806.dd9328618d58110947562 980acd833828042331649451810947562 984ba25344650285fb2fc4080cedca8 880b26485717480F61885826cf4857154648a 980534298880cf4887115448420 98063438280cf4887115448420 98064338280cf4887115448420 98053429880cf4887115448420 98053429880cf4887115448420 98053429880cf4887115448420 98053429880cf4887115448420 98053429880cf4887115489619481155 98153429884cf48871154961948155 98153429884cf488711549842797 1103048652817.acd588aee4229566 340cf482386164893867646777 1103048652817.acd588aee429586 34054852817.acd588aee429586 34054852817.acd588aee429586 34054852817.acd588aee429586 34054852817.acd588aee429586 34054852817.acd588aee429586 34054852817.acd588aee429586 34054852817.acd588aee429586	fc508717f44d6f902b09a2f1cd5e55c1		
#898edd93286f18d581139d3fa4acdc a86bdd929f140es5a48e97c1c07b1 a86bdd9c9f140es5a48e97c1c07b41bd 3a0e4837a80bd23ht29a45a109f37c2 948ac8da3e2yd83b4f1a4f939baea 965ec0afc0440623a2396b74edbc36 94eha2534d4928fb2fc0408ccca0 caa88f7fa0bf610a5a26cf545dcd3aa 3arbb3e9ca923bt298abf1a4bt293 94eha2534d49785bf2fc04bt293 94eha2534d49785bf2fc04bt78b71be40a2d 9003f3adc53b7b353ca08b762be3 98153dc98f4c4b18b71be40a2d 9003f3adc53b7b353ca08b762be3 98153dc98f4c4b10b40b76f7 311b3bd8652817ca6d568aee42c95e6 32dc483a2abbf44fb0abd40738b79f0a 2056c3cc71d680b4e4d4b2b1d45d5 9b5bc4c5c2dt4ed935eac164bq46796676 77ee562e6daa647d11142745cb3d33 34a45186415b95shc474fb1fs9f8b 776b5d1e86c1ad3890e6b25d0c55b8 778e5f3d37ec55s98514dade538828dd	25a9b034369702615e5150f2c2a299cf		
886bdd9c9f140ea5a48e97c1c0c7b1e ee48877a54b3d571cc77d0f37b641bd 9aebd837800d623bte39d510973f62 9edac83870d604532bc39d54bef1044993beae 655ce0afc40d40623a2b30bf4c4dbc96 49aeba25944469285fb2fed00cedca0 caa8877ra0bf610a5a2c30c50bf1be40a2d 2000d5880bcf(d8b71be40a2d 2000d573adc30bf20bc40ad 2000d573adc50bf1be40a2d 2000d57adc50bf1be50bf1bf1bf5253550bf140adb76f2 311b3dc52817cadc50baee42c5be6 3dc478a2bbf44fbb1add473b1d5d53 abb3d55c491c1d42b50be5c3df1ad91fbf59f6 77ee552be6daa647d1144745bc43d3 3da451864fb5bs5add71d1fbf59f8b 778e552be6daa647d114743bc5d3d3 3da45186c1b555adf74dfbf59f8b 778e552be6d5ad59b96b52d055b8 778e554d74e505399f494c428977c80	d4e8021a29d822b205a0d7e7f75fd49d		
be4837.2545.351571c.7740F375641bd 3a0e48378004a23b1e2945a109f3762 968c.e3daa92cd98a47e1047933beae 055ecdafc040d623a23950f4edbc36 969e4ba25944c892857b2fe080cedca8 2a8887fza0bf103a52cf545dc3aa 3afbb3e94ca9880cdfd8b71be40a2d 90003f3adc5387be353ca8a0762be3 98153dc998f4c5887be353ca8a0762be3 98153dc998f4c5887be3525599514aab876727 31103bd84552817ca6d568aee42c95e6 34cf8a2abbf44b93bea1679819709a 285f8c31cc71d680dbe4d4b2b1d45d5 9805bc4cef2d44935ea164946798676 77ee5520e6daa647d11147436cb333 34a518641595acbf17d1147436cb333 34a518641595scd717d1147436cb333 34a518641595scd717d1147436cb333	0e898edd93286618d581139d3fa4acdc		
Jade437800dz3b1e945a10945762 9e8ac8da92ed9839fe18df993beae 65ec8afc404d623a2e3906f4adbc98 9a9eba2594469285H2fed90cedca0 ca8887f30bf16Ja526cf55dc3aa 9aFb3594ca98880cfd8b71be40a2d 09004154adc587b152a55605140adb876f27 151b30486c52817ca60568ae42c95e6 3dc478a2abbf44fbbab440738bF970a 295f8231cc716808b6444b21d4505 8b5b6ec6c2dd4493bea1649d576f7 556b6bec6c2dd4493bea1649d576f7 576e5d5286cfaa647d11447436cbd3d3 3da45186415b95cb711d14f5e9f8b 776e5d1e86c1da38906e6525d0c5588 47885431cc7066591b5548128dd	fa86bdd9c9f140ea5a48e97c1c0c7b1e		
beBaceBdaa92ed98a9fe104f993beae b65ecba232e2936bf4edbc96 b65ecba232e2936bf4edbc96 caa887frabf61085a26cf55fcd3aa barbb39e4ca98888cdr6db71be40a2d b80b34f3ad6c58a7be353ca0a0762be3 b8153dc998f4c5d61ba96b19461c5b 981c3dc998f4c5d61ba96b19461c5b 981c3dc998f4c5d61ba96b19461c5b 981c3dc982hbf4fba04b07677 1105bd4652817ca6d568aee42c95e6 34cf8a2abbf4e4b3ba61493be5789b790a 285f8c31cc71d680dbe4d4b2b1d45d5 b80b6bc6cc2dd4493be5ac164078076 77ee552be6daa647d11447436cbd333 34a5186415b95ach714711hf59ef8b 776e552be6daa647d11447436cbd333 34a5186415b95ach71471hf59ef8b 776e552be6daa647d1147436cbd333 34a5186415b95ach71471hf59ef8b 776e551e86c1da38900e6b25d0c55b8 778ef53d37e6b59a9f4946c128977c80	7be48872a54b3d571cc7fd0f376b41bd		
b65ec0afc20406(23a2e3906/r4adbc)6 49eaba25944690285fb2fcd00cadca0 aa8877a0bf510a5a26cf545dcd3a barbb3=94ce988806dfd8b71be40a2d 000413f3adc587bc353ca080762bc3 308157a0bf510a5325b95144adba08762bc3 308157a0bf510a5325b95140adba08762bc3 308157a0bf510a5325b95140adba08762bc3 31b3bd84652817ca6d568aee42c95e6 36cd76a2abbf44fbba14d73bf970a 2058c31cc71d680bde44db73bf970a 2058c34cc71d4b30bee5c3fabe8a9 8b6bbecc5c2d4c4d493bea16494796f76 77ee5529e6daa647d111427436cb3d3 3da45186415b59acf47dc71bf59f8b 776eb51286c1da38900e6b25d0c55b8 778eb51247co6691f552848 778eb51437e6b539af4946c138977c80 109f44bf24c7c665f3bf5484db46	a3a0e483f800da23b1e9a45a109f3762		
49e4ba25944469285Fb2fed00cedca0 caa887fsa0bf610a5a20cf545cd3aa aab5b39e4ca9880cfd8b71be40a2d 0900475a40c58a7be353ca0a0762be3 881534:0984rc54651ba960b44ct5b 881534:0984rc54651ba960b44ct5b 881534:0984rc44bbb40d738b6727 31b3b484c52817ca6bf58aee42c95e6 34cdr88a2bbf283b67d82b738b6770a 208548:1cc71d688dbe4d4b2b1d45d5 abb3d95c49e11d42b50ee5c3fabe8a9 866b6bcc6c2d4d4d93bea1c49d679676 77ee5520e6daa647d11147436cbd3d3 3d45186415b95ach7147011659cf8b 77685f1a68c1c438900e6b25d0c55b8 77685f1a68c1c438904e6b25d0c55b8 77685f1a68c1c43897056 77685f1a68c1d389dbe6b25d0c55b8	79e0ace8daa92ed98a9fe104f993beae		
caa8877480bf10a5a26cf545dc3aa Dafbb3e94ca9880cdfd8b71be40a2d 30afb3e94ca9880cdfd8b71be40a2d 308153dc58a7be35ca0a0762be3 308153dc99874c5d61ba996b19461c5b 97dccf0b1525355095140a40b876f27 3103bd84652817ca64568aee42c95e6 3dcdf8a2abbf44fb0a40d7380b79070 205f6c31cc71d680dbe4d4b2b1d45d5 b05bc6cc62dd44d935ea1649d679676 77ee5520e6daa647d11447436cbd3d3 3da45186415b95acbf17d114F59e78b 776e5d1e86c1da38900e6b25d0c55b8 7786f5d337ec559af4946c138977c80 13944b6f2c47c66591455e34828dd	7065ec0afc040d623a2e396bf4edbc96		
Bafbb3e94ca98880.cfd8b7lbe40a2d 30803F3ad6c58a7be353ca8a0762be3 38153dc984c5d5153co8a0762be3 38153dc984c5d513co7ad6568ae42c95e6 3dcr68a2abcf44fb0abd4073bF970a 285f8c31cc71d6880be4d4b2b1d45d5 ab3d95c9e11d42b59e5c75fabe8a9 886b6bec6c2dd4ed936aa1649d679676 77ee5520e6daa647d11447436cbd3d3 Jd45186415b95acbf12d11bf5e9f8b 77685fd1e86c1ad3890e6b25d0c55b8 ar58f5dd37e6b59a9f4964c38977c80	149e4ba25944469285fb2fed00cedca0		
300d3f3ad6c58a7be332ca0a0762be3 308153dc998f4c5d61ba906b19461c5b 47dccr0b1552355095140adb876f27 31b3bd84552817ca6d568aee42c95e6 3dcr8a2abt/a4fbbad40738be7970a 2085f8c31cc71d680dbe4d4b2b1d45d5 3b65be6cc2dd4d4d935ea1649d679676 77ee5520e6daa647d11447436cb333 3da45186415b95acbf7d71fbr5e9f8b 77685d1e86c1da38900e6b25d0c55b8 a738f5d3d3re6b59a9f4946c138977c80 13944b6f2c7c066591455e34828dd	ecaa88f7fa0bf610a5a26cf545dcd3aa		
88153/c998f42cf01b996h19461c5b 6Fd2ccf0b1552355095140adb876f27 51b3bd84652817cadb156aee42c95e6 3dcf8a2abbf44fb0abd4073bF970a 205f831cc71d680b4e44b2b1d45d5 abb3d95c49e11d425b0ee5c3fabe8a9 86bb6ec6c2dd4ed936ea1649d679676 77ee5520e6daa647d11447436cbd3d3 3da45186415b95acbd71d71bf5e9f8b 776e5d1e86c1da38900e6b23d0c55b8 a758f5d37ecb59a9f4964c38977c80 10944b6f24c7c066591455e3d828dd	a0afbb3e94ca98880cdfd8b71be40a2d		
Bfd2ccf0b1552355095140adb876727 31D3bd84552817ca6d568aee42c95e6 3dcf8a2abbf44fbab4d4738bf70a 205F8c31cc71d680dbe4d4b2b1d45d5 abb3d95c49e11d4256be5c57abe8a9 3666bec6c2dd4ed936ea1649d579676 77ee5520e6daa647d11447436cb3133 3d45186451b95acbf17d17bf5e9f8b 77685fd186c1da3890e6b25d0c55b8 a758f5dd37e6b59a9f494c138977c80 1309f4b6f24c7c06691fb55ed8828dd	e000d3f3ad6c58a7be353ca0a0762be3		
31b3bd84552817cad368aee42c95e6 33dc4f8a2abbf44fbabd40738bf970a 205f8c31cc71d680dbe44d42b1d45d5 3bb3d95c49e11d42b50ee5c3fabe8a9 3b6bbecc5c2dd4c935ea1649d679676 77ee5520e6daa647d11447436cb33d3 3da45186415b95acb47d71fbf59cf8b 77605d1e86c1da38900e6b25d0c55b8 a758f5d37e6b59a5f44964c38977c80	b98153dc998f4c5d61ba996b19461c5b		
3dcdf8a2abbf44fb0abd40738bf970a 205F8c31cc71d680dbe4d4b2b1d45d5 abb3d9c54911d425b6ec575fabe8a9 86b6bec6c2dd4ed936ea1649d679676 77ee5620e6daa647d11447436cbd3d3 3d45186415b95acbd71d71bf5e9f8b 77685d1e86c1da3890e6b25d9c55b8 ar58f5dd37e6b59a9f4964c38977c80	68fd2ccf0b1552355095140adb876f27		
205f8c31cc71d680dhe4d4b2b1d45d5 abb3d95c49e11d42b50ee5c3fabe8a9 S605bec5c2d4ded936ea1649d679676 77ce5520e6daa647d11447436cb3d3 Jd45186415b95acb47d71hF5e9f8b 77685d1e86c1da38900e6b25d0c55b8 a738f5dd37e6b59a5f4494c138977c80 13944b6f247c066591455e3d828dd	131b3bd84652817ca6d568aee42c95e6		
abb3d95c49e11d42b50ee5c3fabe8a9 8666bec6c2dd4ed336ea1649d679676 77ee562e6daa6a47d1144736cbd3d3 3da45186415b95acbd71d71bf5e9f8b 776867d1e86c1da3890e6b25d8c55b8 a758f5dd37e6b59a9f4964c38977c80 13944b6f24c7c066591fb55ed3828dd	13dcdf8a2abbf44fb0abd40738bf970a		
8666bec6c2dd4ed36ea1649d679676 77ee5620e6daa647d11447436cbd3d3 3d45186415b95acbd71d71br5e9f8b 77685d1e86c1da3890e6b25d9c55b8 a758f5dd37e6b59a9f4964c38977c80	a205f8c31cc71d680dbe4d4b2b1d45d5		
77ee5620e6dae647d11447436cbd3d3 3da45186415b95acbd71d71bf5e9f8b 77605d1e86c1da38900e6b25d0c55b8 a758f5dd37e6b59a9f4964c38977c80 1399f4b6f24c7co86691fb55e3d828dd	1abb3d95c49e11d42b50ee5c3fabe8a9		
3da45186415b95acbd71d71bf5e9f8b 77605d1e86c1da3800e6b25d0c55b8 a758f5dd37e6b59a9f4964c38977c80 1309f4b6f24c7c066591fb55ed3828dd	a86b6bec6c2dd4ed936ea1649d679676		
77605d11866c1da38900e6b25d0c55b8 a758f5dd37e6b59a9f4964c38977c80 13947b6f24c7c06691fb55ed3828dd	077ee5620e6daa647d11447436cbd3d3		
a758f5dd37e6b59a9f4964c38977c80 1190f4b6f24c7c06691fb55ed3828dd	b3da45186415b95acbd71d71bf5e9f8b		
1190f4b6f24c7c06691fb55ed3828dd	877605d1e86c1da38900e6b25d0c55b8		
	8a758f5dd37e6b59a9f4964c38977c80		
bba3d30f95fd906dbc2bd101d6358bb	21190f4b6f24c7c06691fb55ed3828dd		
• •	bbba3d30f95fd906dbc2bd101d6358bb		
>			×
	<		>

Fig. 37 The clean.txt file after running the scanner_version_3.exe program in scan mode.

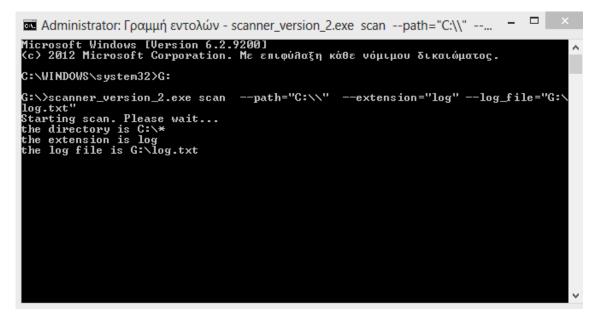


Fig. 38 Creating the log.txt file by using the scanner_version_2.exe program in scan mode.

•

G 34.	Administrator: Foguuń sytolyjw – 🗇 🗙
	Administrator: Γραμμή εντολών – 🗠 🔨
[218]=>	"C:\Windows/Temp/Silverlight0.log"
[219]=>	"C:\Windows/Temp/SilverlightMSI.log"
[220]=>	
[221]=>	"C:\Windows/Temp/chrome_installer.log"
[222]=>	"C:\Windows/Temp/uminst.log"
[223]=>	"C:\Windows/Temp/winstore.log"
[224]=>	"C:\Windows/WinSxS/poqexec.log"
string(33) [225]=>	"C:\Windows/debug/WIA/wiatrace.log"
string(24) [226]=>	"C:\Windows/debug/mrt.log"
	"C:\Windows/debug/mrteng.log"
	"C:\Windows/debug/netlogon.log"
	"C:\Windows/debug/sammui.log"
	"C:\Windows/inf/setupapi.app.log"
string(47)	"C:\Windows/inf/setupapi.dev.20130730_200027.log"
	"C:\Windows/inf/setupapi.dev.log"
	"C:\Windows/inf/setupapi.setup.log"
	"C:\Windows/security/logs/scesetup.log"
	"C:\Windows/security/edb.log"
	"C:\inetpub/logs/LogFiles/W3SUC1/u_ex130221.log"
	"C:\inetpub/logs/LogFiles/W3SUC1/u_ex130418.log"
	"C:\inetpub/logs/LogFiles/W3SUC1/u_ex130422.log"
	"C:\inetpub/logs/LogFiles/W3SUC1/u_ex130423.log"
	"C:\inetpub/logs/LogFiles/W3SUC1/u_ex130424.log"
	"C:\inetpub/logs/LogFiles/W3SUC1/u_ex130425.log"
	"C:\wamp/bin/apache/Apache2.4.4/logs/install.log"
[242]=> string(22)	"C:\wamp/logs/mysql.log"
[243]=> string(41)	"C:\System Volume Information/tracking.log"
[244]=> string(25)	"C:\Windows/DtcInstall.log"
[245]=> string(23)	"C:\\indows/KB835221.log"
[246]=>	"C:\\/indows/MSI30-KB884016.log"
[247]=>	"C:\Windows/PFRO.log"
[248]=>	"C:\Windows/WindowsUpdate.log"
[249]=>	"C:\Windows/chipset.log"
[250]=>	"C:\Windows/iis.log"
[251]=>	"C:\Windows/vmgcoinstall.log"
>	G. Arthuws/ Viigto Instatt. 10g
	_file <res: c:\users\nikos\appdata\local\microsoft\windows\webc<br="" php="">): failed to open stream: Permission denied in scanner_version_2.php</res:>
	_file(res:///PHP/C:\Windows\System32\catroot2\edb.log): failed to op ermission denied in scanner_version_2.php on line 1
G:\>	✓

Fig. 39 The results after running the scanner_version_2.exe program in scan mode.

🔲 Ιοg.txt - Σημειωματάριο 🗕	∎ ×
Αρχείο Επεξεργασία Μορφή Προβολή Βοήθεια	
1) Found file: C:\Intel/Logs/IntelChipset.log	^
Hash: c5666c6c4fde24199a42a1044a158e89	
 Found file: C:\Program Files/Mozilla Firefox/uninstall/uninstall.log 	
Hash: e98ff3dd191d5a516f33cffc06abbc94	
3) Found file: C:\Program Files/Mozilla Firefox/install.log	
Hash: f0ceb93b7c0705320d03c4ca2d302165	
4) Found file: C:\Program Files/Sony/Media Go/RegSettings.log	
Hash: d7ac46e45915551b69635cbac459a1da	
5) Found file: C:\Program Files/VideoLAN/VLC/uninstall.log	
Hash: 10bb2331b9ae5033de36d39c3bc53dd4	
6) Found file: C:\ProgramData/MFAData/logs/avgcei.log	
Hash: 96d217bced7d3169172fc39b1f94f800	
7) Found file: C:\ProgramData/Microsoft/Search/Data/Applications/Windows/edb.log	
Hash: 7228f1e4d79107e6421e3119ae7c8489	
8) Found file: C:\ProgramData/Microsoft/Search/Data/Applications/Windows/edb001C7.log	
Hash: b266d42f7370ac7d5599f1030951c0a1	
9) Found file: C:\ProgramData/Microsoft/Search/Data/Applications/Windows/edb001C8.log	
Hash: b8f478be9fdfd550d758dcdbab8dba24	
10) Found file: C:\ProgramData/Microsoft/Search/Data/Applications/Windows/edb001C9.log	
Hash: 8a5c929b483c196e6850bff4475b2610	
11) Found file: C:\ProgramData/Microsoft/Search/Data/Applications/Windows/edbtmp.log	
Hash: 41e19f891e2cfe2ed96e4d74a569761c	
12) Found file: C:\ProgramData/Microsoft/Windows/AppRepository/edb.log	
Hash: f8dcbcb1c6631867248692ace216ee2b	
13) Found file: C:\ProgramData/Microsoft/Windows/AppRepository/edb00004.log	
Hash: ca5c4a7bde3d9caa1cb743201b16d672b	
14) Found file: C:\ProgramData/Microsoft/Windows/AppRepository/edb00005.log	
Hash: f46a793a6e2b95a5fecb3085942e349	
15) Found file: (:\ProgramData/Microsoft/Mindows/AppRepository/edbtmp.log Hash: b6d810360a5672480473153e2c	
16) Found file: (:\ProgramData/Woilla/logs/maintenanceservice-1.log Hash: 887re6cide031c818f7dab15re46f38	
nash: oor/eoclucos/clator/udu/steroio 17) Found file: C:/ProgramData/Mozilla/logs/maintenanceservice-10.log	
Hash: cc92e789798a9615ae4be95c55f561d	
18) Found file: (:\ProgramData/Mozilla/logs/maintenanceservice-2.log	
Table Total The Configuration and the second s	
19) Found file: C:/ProgramData/Mozilla/logs/maintenanceservice-3.log	
Hash: aeb97cbd724a94b7a6377019a9332bc	
20) Found file: C:\ProgramData/Mozilla/logs/maintenanceservice-4.log	
Lash: b3a30eddb3eb3ad06deda880bcb65a	
21) Found file: C:\ProgramData/Mozilla/logs/maintenanceservice-5.log	
Hash: 939da1b7cd492b6f64bade78b95A7f4	
22) Found file: C:\ProgramData/Mozilla/logs/maintenanceservice-6.log	
Hash: 140f773722a42a52edcbab6781b1a5d0	
23) Found file: C:\ProgramData/Mozilla/logs/maintenanceservice-7.log	
Hash: 33d4f4ee206d1f0bbdf57d32c276c505	
24) Found file: C:\ProgramData/Mozilla/logs/maintenanceservice-8.log	
Hash: 6dbba8892c1c6aa27edc4998220ccdfa	
25) Found file: C:\ProgramData/Mozilla/logs/maintenanceservice-9.log	
Hash: 3bf02b668d8843183b46edb3a062a91a	
26) Found file: C:\ProgramData/Mozilla/logs/maintenanceservice-install.log	~
	>

Fig. 40 The log.txt file after running the scanner_version_2.exe program in scan mode.

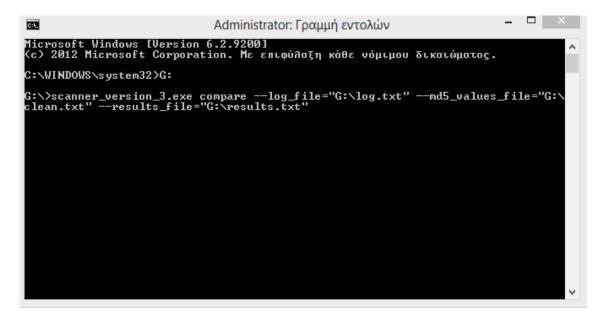


Fig. 41 Creating the results.txt file with the results by using the scanner_version_3.exe program in compare mode.

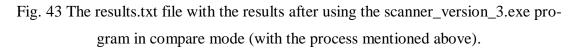
C	١.

Administrator: [οσιιμή	εντολών
Autorities alor. I	ραμμη	evionuv

68.	Administrator: Γραμμή εντολών	-	a ×
	\Users/nikos/AppData/Roaming/Sc	ony/Media Go Inst	aller⁄ ,
	\Users/nikos/Desktop/ ^u tf _F ¹ /]	00LS/super kludg	e∕Wang
dera.Controls-0.9.1.0-src/d Suspicious file found -> C:	locs/Documentation.log \Users/nikos/Documents/Virtual	Machines/Windows	XP Pr
ofessional/vmware-0.log	\Users/nikos/Documents/Virtual		
ofessional/vmware.log			
ofessional/vprintproxy.log	\Users/nikos/Documents/Virtual	nachines/windows	AF FF
Suspicious file found -> C: Suspicious file found -> C:	\Windows/Logs/CBS/CBS.log \Windows/ServiceProfiles/LocalS	ervice/AppData/L	ocal/T
emp∕MpCmdRun.log Suspicious file found -> C:	\Windows/SoftwareDistribution/I)ataStore/Logs/ed	b.log
Suspicious file found -> C:	<pre>\Windows/System32/catroot2/edb. \Windows/System32/config/system</pre>	log	
Avg2014/log/avgadvisor.log	\Windows/System32/config/system		
Avg2014/log/avgcfg.log			
Avg2014/log/avgchjw.log	\Windows/System32/config/system		
Suspicious file found -> C: Avg2014/log/avgcore.log	\Windows/System32/config/system	profile/AppData/	Local∕
Suspicious file found -> C: Avg2014/log/avgcsl.log	\Windows/System32/config/system	profile/AppData/	Local⁄
Suspicious file found -> C: Avg2014/log/avgdiagex.log	\Windows/System32/config/system	nprofile/AppData/	Local/
Suspicious file found -> C:	\Windows/System32/config/system	profile/AppData/	Local/
	\Windows/System32/config/system	profile/AppData/	Local/
Avg2014/log/avgemc.log Suspicious file found -> C:	\Windows/System32/config/system	profile/AppData/	Local/
Avg2014/log/avgidpagent.log Suspicious file found -> C:	\\ \\Windows/System32/config/system	 mrofile/AnnData/	Local/
Avg2014/log/avgidpdrv.log	\Windows/System32/config/system		
Avg2014/log/avgidpeh.log			
Avg2014/log/avgldr.log	\Windows/System32/config/system		
Avg2014/log/avgmf.log	\Windows/System32/config/system		
Suspicious file found -> C: Avg2014/log/avgmsgdisp.log	\Windows/System32/config/system	profile/AppData/	Local⁄
Suspicious file found -> Č: Avg2014/log/avgns.log	\Windows/System32/config/system	profile/AppData/	Local⁄
	\Windows/System32/config/system	profile/AppData/	Local⁄
Suspicious file found -> C:	\Windows/System32/config/system	profile/AppData/	Local/
	\Windows/System32/config/system	profile/AppData/	Local/
Avg2014/log/avgsecapi.log Suspicious file found -> C:	\Windows/System32/config/system	profile/AppData/	Local/
Avg2014/log/avgshred.log Suspicious file found -> C:	 \Windows/System32/config/system	 profile/AppData/	Local/
Avg2014/log/avgtdi.log	\Windows/System32/config/system		
Avg2014/log/avgwd.log			
Avg2014/log/avgwdsvc.log	\Windows/System32/config/system		
Avg2014/log/commonpriv.log	\Windows/System32/config/system		
Ava2014/log/fixcfg.log	\Windows/System32/config/system		
Suspicious file found -> C: Avg2014/log/lng.log	\Windows/System32/config/system	profile/AppData/	Local⁄
Suspicious file found \rightarrow C:	Windows/System32/sru/SRU.log	10%	
Suspicious file found -> C:	\Windows/System32/sru/SRU00506. \inetpub/logs/LogFiles/W3SUC1/u \inetpub/logs/LogFiles/W3SUC1/u	_ex130221.log	
Sugnicious file found -> C:	<pre>\inetnuh/logs/LogFiles/W3SUC1/</pre>	. ev130422_log	
Susnicious file found -> C:	\inetpub/logs/LogFiles/W3SUC1/u \inetpub/logs/LogFiles/W3SUC1/u	ι ex130424.log	
Sugnicious file found $- > C$	<pre>\inetwub/logs/LogFiles/U3SUC1/u</pre>	1 ev130425 log	
Suspicious file found \rightarrow C Suspicious file found \rightarrow C	\wamp/bin/apache/Apache2.4.4/lo \wamp/logs/mysql.log \Sustem Uolume Information/trac	king log	
Suspicious file found -> C:	\System Volume Information/trac \Windows/WindowsUpdate.log		

Fig. 42 The results after running the scanner_version_3.exe program in compare mode.

	results.txt - Σημειωματάριο	- 0 ×
Αρχείο Επεξεργασί	Μορφή Προβολή Βοήθεια	
104) Suspiciou	file found -> C:\Users/nikos/AppData/Local/Packages/WinStore_cw5n1h2txyewy/AC/Temp/winstore.log	
	file found -> C:\Users/nikos/AppData/Local/Packages/microsoft.windowscommunicationsapps_8wekyb3d8bbwe/LocalState/LiveComm/nouse	
	file found -> C:\Users/nikos/AppData/Local/Packages/microsoft.windowsphotos_8wekyb3d8bbwe/LocalState/LiveComm/nouser/120712-004	
	file found -> C:\Users/nikos/AppData/Local/Packages/microsoft.windowsphotos_8wekyb3d8bbwe/LocalState/LiveComm/nouser/120712-004	
	file found -> C:\Users/nikos/AppData/Local/Packages/microsoft.windowsphotos_8wekyb3d8bbwe/LocalState/LiveComm/nouser/120712-004	19/DBStore/Log
	file found -> C:\Users/nikos/AppData/Local/Packages/microsoft.windowsphotos_8wekyb3d8bbwe/LocalState/edb.log	
	file found -> C:\Users/nikos/AppData/Local/Packages/microsoft.windowsphotos_8wekyb3d8bbwe/LocalState/edbtmp.log	
	file found -> C:\Users/nikos/AppData/Local/SlimWare Utilities Inc/SlimDrivers/Logs/2013-01-27 21-45-48 0.log	
	<pre>file found -> C:\Users/nikos/AppData/Local/SlimWare Utilities Inc/SlimDrivers/Logs/2013-01-27 21-49-28 0.log file found -> C:\Users/nikos/AppData/Local/SlimWare Utilities Inc/SlimDrivers/Logs/2013-01-27 22-07-41 0.log</pre>	
	file found -> C:\Users/nikus/Applata/Local/Simmare Otifities Inc/SimDrivers/Log/2013-01-27 23-05-14 0.log	
	file found -> C:\Users/nikus/Applata/Local/Simmare Otilities Inc/SimDrivers/Logs/2013-01-27 23-45-37 0.log	
	file found -> C:\Users/nikos/AppData/Loca/Silmware offities Inc/SilmDrivers/Logs/2013-01-28 00-44-46 0.log	
	file found -> C:\Users/nikos/AppData/Loca/Silmware offities Inc/SilmDrivers/Logs/2013-01-28 15-46-55 0.log	
	file found -> C:\USES/intoS/AppBata/Local/Silminare Utilities Inc/SilmDriverS/LogS/2013-01-28 16-31-59 0.log	
	file found -> C:\USES/intoS/AppBata/Local/Silminare Utilities Inc/SilmDriverS/LogS/2013-01-30 16-00-07 0.log	
	file found -> C:\Users/nikos/AppData/Local/SlimWare Utilities Inc/SlimDrivers/Logs/2013-01-30 22-15-19 0.log	
	file found -> C:(Users/nikos/AppData/Local/VMware/playerUploadedData.log	
	file found -> C:\Users/nikos/AppData/Local/VirtualStore/Windows/Temp/winstore.log	
	file found -> C:\Users/nikos/AppData/LocalLow/Google/GoogleEarth/unified cache leveldb leveldb2/011051.log	
	file found -> C:\Users/nikos/AppData/Roaming/BSplayer/AC3 Filter/unreg.log	
128) Suspiciou	file found -> C:\Users/nikos/AppData/Roaming/BSplayer/FFDShow/unreg.log	
	file found -> C:\Users/nikos/AppData/Roaming/BSplayer/Flash Video (FLV)/unreg.log	
130) Suspiciou	file found -> C:\Users/nikos/AppData/Roaming/BSplayer/Haali media splitter/unreg.log	
131) Suspiciou	file found -> C:\Users/nikos/AppData/Roaming/BSplayer/MPEG audio decoder/unreg.log	
132) Suspiciou	file found -> C:\Users/nikos/AppData/Roaming/BSplayer/MPEG2 decoder/unreg.log	
	file found -> C:\Users/nikos/AppData/Roaming/BSplayer/RealMedia splitter/unreg.log	
	file found -> C:\Users/nikos/AppData/Roaming/Mozilla/Firefox/Crash Reports/submit.log	
	file found -> C:\Users/nikos/AppData/Roaming/Mozilla/Firefox/Profiles/gvsey6ld.default-1375459513834/marionette.log	
	file found -> C:\Users/nikos/AppData/Roaming/Sony/Media Go Installer/debug.log	
	file found -> C:\Users/nikos/AppData/Roaming/Sony/Media Go Installer/installer.log	
	file found -> C:\Users/nikos/AppData/Roaming/Sony/Media Go Installer/msi.log	
	file found -> C:\Users/nikos/Desktop/NTYXIAKH/TOOLS/super kludge/Wangdera.Controls-0.9.1.0-src/docs/Documentation.log	
	file found -> C:\Users/nikos/Documents/Virtual Machines/Windows XP Professional/vmware-0.log	
	file found -> C:\Users/nikos/Documents/Virtual Machines/Windows XP Professional/vmware.log	
	file found -> C:\Users/nikos/Documents/Virtual Machines/Windows XP Professional/vprintproxy.log	
	<pre>file found -> C:\Windows/System32/catroot2/edb.log</pre>	
	<pre>file found -> C:\Windows/System32/config/systemprofile/AppData/Local/Avg2014/log/avgwd.log file found -> C:\Windows/System32/config/systemprofile/AppData/Local/Avg2014/log/avgwd.log</pre>	
	file found -> C:\inetpub/logs/LogFiles/W3SVC1/u_ex130221.log	
	file found -> C:\inetpub/logs/LogFiles/W3SVC1/u_ex130418.log file found -> C:\inetpub/logs/LogFiles/W3SVC1/u ex130422.log	
	file found -> C:\inetpub/logs/LogFiles/M35VC1/u_ex130422.log	
	file found -> C:\inctpub/logs/LogFiles/W3SVC1/u_ex130423.log	
	file found -> C:\inctpub/logs/LogFiles/W35VC1/u_ex130425.log	
	file found -> C:\wamp/bin/apache/Apache2.4.4/logs/install.log	
	file found > C:\wamp/log/mysql.log	
	file found -> C:\System Volume Information/tracking.log	
,	0	
<		>



As we can confirm, the results.txt file contains all the *.log files of the whole partition C, except the *.log files that are included in the Windows 8 installation file.

4.7 Advantages

The scanner.php program is a simple and functional tool. It is written in a well known language (PHP) with million users around the world, with numerous applications and a wide variety of implementations. There are many plug ins that can be attached to this program. In addition this program can be easily incorporated into other programs. It is easy to carry, because of its minimum size. Also it is user friendly because it is easy to run even from someone with little knowledge and little expertise. The parameters are no longer hard coded and they are easy to be inserted or changed from

the command line prompt. It is very fast, reliable and trustworthy because of its simplicity and the small number of code lines.

4.8 Drawbacks

The program is very simple. So it has only a small number of functions, options, commands and parameters. It can be used only by using the command line prompt. A web interface could make it more user friendly and more attractive for the simple user.

4.9 Evaluation

The program was tested in all possible scenarios that could be encountered by a digital forensics investigator or by a simple user. In all conditions the program worked as expected and the results were correct.

4.10 Suggestions

There are some things that must be taken into consideration before using the program. First of all the investigator must have knowledge, of what he is searching for, inside the computer under investigation. If the program is used for digital triage, the time is limited. If the program is used in the examination laboratory, there is plenty of time to do many tests and search for a wide variety of traces, depending always on the case under investigation.

Additionally the user of the program must create a wide range of correct clean MD5 files. In this way he will be able to use the correct files in every specific and different case. He must create files with clean MD5 values of all the windows versions and releases installations, Linux, Ubundu and other OS installations, clean installations of programs that are widely used, a wide number of software installations, browser installations and many more. So in each case he will be able to make the comparison using

the correct pre constructed clean MD5 files, and therefore produce solid and helpful findings. In addition the user must always have updated clean MD5 files from all the new releases and updated programs. Nowadays the Operating Systems whether it is Windows or any other, they update very frequently and automatically. Also all the programs in the modern computers from the antivirus programs to media players update all the time, so there is a need to create the clean MD5 files from all the up to date versions of these programs.

Furthermore this program has a certain functionality and the capabilities are constrained and predefined. The investigator and user of this program in a real scenario cannot depend only on this tool. Digital triage and digital investigation are very wide and complex fields. In order to achieve the necessary findings many tools must be applied. As mentioned in the chapters above there is a great number of tools with different potentials, different targets, different use, with case oriented applications producing different results and findings. The investigator must be very well informed and prepared in the digital triage and digital investigation field in order to achieve the required results and eventually success. A wide range portfolio of programs is unquestionable. A true necessity in every investigation.

4.11 Future Work – Enhancements

In the future many things can be done to improve the program and its functionality. First of all a web interface could be developed to make it more attractive and user friendly.

Functionalities can be added, including the ability to search for more difficult files and do a wide variety of comparisons. An upgrade would be to have libraries with clean MD5 values, from various program installations, and all the possible Windows installations, and be able to choose each time the files we want to compare. Furthermore, when running, the program could find automatically the versions of installations and make the comparisons without any help or any intervention from the user.

The results could be presented in a web environment using statistics, diagrams, bars, pies and percentages for the reports. This could help the user take fast decisions, come quickly with the correct conclusions and decide in which way to proceed.

The program as mentioned above can be incorporated in other digital triage and digital investigation tools to enhance their functionality and usability. Also other tools and programs could be added in this program to make it more complex and become useful in more difficult cases. The simplicity of the program and the PHP language make all the above an easy task for the programmer. In addition it is easy to transform this program in other languages like C, C++, Java, VBscript, Python and many more.

This program could also be used for Data Reduction. It could be implemented like the FTK (Forensic Toolkit). By using the Known File Filter, or KFF, we can eliminate or highlight known files, by using MD5 hashes that are generated by the user or from NIST or Hashkeeper. [29] [45] [56] [42] These KFF lists are MD5 values from files that we don't care to examine and we want to avoid analyze them. Also they are files from similar, previews, or other suspicious real cases.

Further more, plug-ins and extensions could be found to enhance the functionality of the program. Many tools like this could be integrated to create a bigger and better tool. The new tool, after the integration, would have none of the drawbacks but all the advantages of each individual tool.

4.12 Conclusion

Digital Forensics is a very demanding and exciting sector but it has many difficulties. There are many types of data to be analyzed, the data size is enormous and there is lack of skilled analysts. The above problems will get worse in the future, and the only way to keep up is to develop new techniques that will enhance our ability to collect, maintain and analyze big data sets with information. [32]

5 Personal Reflection

From my personal experience, while experimenting with the four forensics tools Bulk Extractor, TriageIR, TR3Secure and Kludge I encountered all their problems and disadvantages. First of all I installed these programs in 6 different home desktop computers with different versions of Windows operating systems (Windows XP, Vista, 7, 8, 32 and 64 bit). The installation of the tools may look simple to the medium user but when it comes to start using them, then the problems start. Most of the times they don't even work and they don't create any reports. When running they display error messages and when they work they don't produce all the reports they claim to be able to produce. Some reports are created and some other not, depending each time on the operating system. The language of the OS affected their compatibility and implementation. So it was obvious that they were OS sensitive. In Windows 8, the most recent of the OS, the problems were even worse. Probably new releases of the tools should be developed. In the internet there is not enough information by the developers or the users to bypass all the problems encountered, that could help and assist in making them work. The collection of browsing history, which was the initial target, by using Kludge, was never produced in any computer tested. I tried many solutions, personal and suggested by the internet, but with no luck. My personal opinion is that these programs address to the expert user that knows exactly what he wants and how to achieve it. They are not very useful for the beginner and the medium user. Anyone choosing them would have problems in using these tools. And in a real case scenario these problems and malfunctions would be at least catastrophic for triage and analysis. My research showed that the most digital triage tools have numerous problems and drawbacks and this is expected when considering the nature of the investigation. Also most of them are written in simple DOS batch scripting, a very poor programming practice. In addition most of them need improvements and enhancements.

All the above, lead me first to think, the development of a program that would collect all the browsing history from all the browsers installed in a computer. After reading many articles and conducted extensive research I understood that all the new browsers (latest releases) were very complicated and needed special tools, specifically designed for each and every one of them, to be able to extract the browsing history and other use-ful information stored in the browsers. For example Mozilla Firefox needs the SQLite Manager tool. [83] Developing a tool that could be able to process all the available browsers in all their possible and available releases would be something really demanding, complicated and advanced. In a real case scenario having a tool to fetch the brows-ing history of a specific only browser would be of no use. The suspect has the ability to install many browsers in his personal computer and use any of them at will.

These findings lead me to the decision to develop my own program to help the digital forensics investigator in my way. To develop a program that could help him during the digital triage but also to be useful it in the lab as well. So the idea before starting developing my own program was to create a script that could find all the .exe files in a computer, to reject the default .exe files from Windows and present only the .exe files installed by the user. This could be achieved by finding all the .exe files installed in the computer, calculating their MD5 and then compare these MD5 values with an archive file / database with the produced MD5 values of a Windows installation only. For example notepad.exe in Windows 7 always gives the same MD5. So comparing this MD5 with a database of MD5 can be distinguished and be ignored during the presentation of the installed applications to the investigator. The general solution is easy, but there are many differentiations in each case that could make the whole process very complicated.

So a tool was developed that has the ability to search a whole computer or any partition or file chosen, for files and programs installed or created by the user and that may have any possible extension. This was possible by comparing the MD5 hashes of the files under investigation. In this way the examiner can search in a very short time the computer under examination for all the installed and created files or programs, but also for altered programs, possible malware and harmful programs.

This program will gain even greater usability if it is incorporated into other digital triage programs or if it is enhanced with more advanced functionality.

I hope that this paper will help others to learn not only from my paper research but also from the program I developed, the presented personal experiences, and any mistakes that were made along the way. Writing tools that will be used for digital forensics is very difficult and very different from other programming attempts because of the multiple data types that need to be taken into consideration, the desire for high performance, the advanced skills needed from users, and the requirement the software to run without ever crashing. Since the digital forensics field grows continuously, many people are engaged in the practice of writing software for digital forensics. Only a small number of today's forensic tool developers have adequate knowledge and training in developing and design software. A number of them do not even think themselves of being programmers. [32] And this belief must change.

6 Conclusions

Appreciating the change of technology, and understanding the nature of the threat, the evolving discipline of anti-forensics and increasing application of cryptography, we understand that the domain of forensics has an extremely challenging and exciting future ahead of it. However, the need for organizations to equip themselves with a forensic capability is becoming essential in order to combat and manage incidents effectively. [55]

To appreciate the necessity of computer forensics in the organization, first we have to understand the scale and nature of the threats. Unfortunately, truly understanding the scale of the threat is difficult as the reporting of cybercrime is relatively patchy. Many organizations see such reporting as something that will affect their brand image and reputation. Whilst discussions are being held in some countries about implementing laws to force organizations into reporting incidents, at this stage the industry relies upon survey statistics to appreciate the threat. [55]

It is no longer enough to pull the plug and take the computer to the lab when making a digital examination. Technology changes continuously and digital forensic analysts have to learn new methods and develop tools to succeed. This is necessary in a live response case. [93]

Forensic analysis help to identify privacy issues, detect forgery and manipulation, establish a chain of custody for sources and employ write protection for capture or transfer. It can find content and metadata, help indexing and searching by examiners, and enable audit control. [48]

6.1 Digital forensics is different

Digital Forensics software development makes it really different from other branches. These differences are: data diversity, data scale, temporal diversity, human capital, and the so-called "CSI effect." [32]

6.1.1 The challenge of data diversity

Digital Forensics and other kinds of software have a big difference in the range of data that have to be examined. Most software development is specialized in a specific problem. Digital Forensics has as target all the data that can be stored or transmitted using computer and digital media. In addition most software tools work only with proper input and crash otherwise. Digital Forensics tools don't have this luxury. They must run at any circumstances and produce any results possible. [32]

6.1.2 Data scale

A second problem in the development of digital forensics tools is the huge bulk of information that has to be analyzed. Furthermore there is the problem of the difference between the storage and performance bottlenecks.

Examiners have to analyze new and up to date computer systems. So they are using high end computers to examine high end computers and they also have to examine information in hours that the suspect needed weeks, months, or even years to create. We will never overcome the performance lack. When the analysis will move to the cloud we will have to examine multi-terabyte data caused by the cloud-based crime. [32]

6.1.3 Temporal diversity: the never-ending upgrade cycle

Most organizations believe that upgrades in software are a difficult process that can cause problems and incompatibilities. So they use out-of-date operating systems and update only when they buy the new hardware.

Digital forensics examiners do not have this flexibility. They have to update the software all the time because the target is not only the obsolete but also the newest software and hardware possible. Nowhere else it is so important to upgrade the software when the new software is released. In upgrades, two things have to be taken into account. The examiners tool's version and the target's version [32]

6.1.4 Human capital demands and limitations

Digital forensics tools users are from law enforcement, with little knowledge in computer science. They have strict deadlines and are exhausted. Certifications and degrees certainly help this situation but cannot solve the problem. Analysis may have as target any possible kind of information. So many organizations train their own developers to create the needed software. [32]

6.1.5 The CSI effect

CSI Effect is the belief, that when television shows crime scenes, investigations, forensics, courts, juries, judges and prosecutors to have exceptionally high demanding concerning what forensic analysis can actually achieve, this is also true in reality. On television every digital forensics examiner knows every tool, correlation is easy and instantaneous, there are never false positives, overwritten data can easily be recovered, encryption can be cracked, it is impossible to delete anything and the tools never crash. In reality things are not so easy. Overwritten data cannot be recovered and modern encryption algorithms can be decrypted only by using password cracking. [32]

6.1.6 The cost of development and the role of government

Digital forensics tool development is exceptionally expensive and the software produced has small number of users. The more sophisticated the analysis, the smaller the market. Few digital forensics companies have been commercially successful. It is not that digital forensics is an immature market with customers only from the government; it is that digital forensics is a mature market with high and increasing development costs. These high development costs in addition to customers being federal, state and local governments makes it difficult for the traditional commercial software development model to be successfully applicable. [32]

6.2 Lessons learned developing digital forensics tools

In this chapter we discuss about software engineering and design issues that have been confronted when developing the above mentioned digital forensics tools. [32]

6.2.1 Platform and language

Windows is the most widespread operating system used by computer forensics developers and examiners. But also Linux and MacOS seem to consolidate their places. An easy way to write multi-platform forensics tools is to use C, C++, C#, Java or Python because tools in these languages can be easily transferred between these three platforms. C was historically the preferred developer's language but nowadays many have shifted to C++. Many believed that Java was running much slower than C/C++. But the testing so far shows that this belief is only partially true.

Writing programs in Python is quite easy but the experience so far shows that these programs are slow and intensive for memory. [32]

6.2.2 Parallelism and high performance computing

The data scale problem led many researchers to spend lots of effort and time on issues such as multithreading and high performance computing in an effort to gain more performance. But until now the efforts made are mixed and the results produced not so clear. [32]

6.2.3 All-in-one tools vs. single-use tools

There are many kinds of forensic investigations and the same tool many times has to be used at the same data but for different reasons. This difference in the use cases complicates the programs development, documentation, and training. Some say it is better to have a single tool than many because:

- If there are many tools, the investigators will try to have them all.
- Whatever a digital forensics program does: decoding and enumerating data, data ingest; preparing a report is necessary whatever the expected results may be.
- There is a standard cost to packaging, distributing, and promoting a program. When a tool has many functions the cost is distributed to a broader base.

An opinion to solve the problem of different use cases is the programs to organize the results into different partitions or files. For example using one section storing information needed for usual cases, and another saving all the extracted data. [32]

6.2.4 Evidence container file formats

The diversity of programs and the lack of proper user training make it necessary for forensic software to be able to process inputs at any format. In real cases a single input layer should enable programs to transparently manage disk images in raw, split-raw, EnCase or AFF formats. [32]

6.3 Conclusion

This paper makes contributions not only to the theory but also the practice of digital forensics. First, it shows that all the existing freeware and licensed forensics tools have many drawbacks and incompatibilities. This paper presents Bulk Extractor, TriageIR, TR3Secure and Kludge, powerful freeware tools to perform bulk data analysis. It highlights the experience of installing and using these tools noticing all the advantages, drawbacks, enhancements, suggestions and future work. It presents a detailed evaluation comparing Bulk Extractor, TriageIR, TR3Secure and Kludge. It shows that each tool has a strong and a weak point and there is no solution for every case that an examiner may encounter.

Finally, this paper presents a tool, developed by the author, which can search a whole computer or any partition or file chosen, for files and programs installed or creat-

ed by the user and that may have any possible extension. This was possible by comparing the MD5 hashes of the files. In this way the examiner can search in a very short time the computer under examination for all the installed and created files or programs, altered programs, but also for possible malware and harmful programs.

This program will have even greater usability if it is incorporated into other digital triage programs or if it is enhanced with more advanced functionality.

References

[1] ACPO. (2008) *Good practice guide for computer-based electronic evidence*. ACPO, United Kingdom.

[2] Adams, R. (2012) The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice. *National Library of Australia*, Murdoch University, Australia.

[3] Adelstein, F., and Golden, G. (2008) Live Forensics Tutorial, Part 1 Traditional Forensics. *Usenix Annual Technical Conference 2008*, Boston, Massachusetts, USA.

[4] Aljaedi, A., Lindskog, D., Zavarsky, P., Ruhl, R., and Almari, F. (2011) Comparative analysis of volatile memory forensics: live response vs. memory imaging. *Proceedings of the 2011 IEEE third international conference on Social Computing (SocialCom),* Boston, MA, USA, pp.1253–1258.

[5] Bamcompile (2013) http://www.bambalam.se/bamcompile/.

[6] Bednar, P., Katos, V., and Hennell, C. (2008) Cyber-Crime Investigations: Complex Collaborative Decision Making. *Third International Annual Workshop on Digital Forensics and Incident Analysis, 2008 IEEE.*

[7] Brezinski, D., and Killalea, T. (2002) Guidelines for evidence collection and archiving. *The Internet Society*.

[8] Broadhurst, R. (2006) Developments in the Global Law Enforcement of Cyber-Crime. *Policing: An International Journal of Police Strategies & Management, vol. 29, no.3, Emerald,* pp. 408- 433.

[9] Brownlee, N., Guttman, E., (1998) Expectations for computer security incident response. *The Internet Society*.

[10] Bulk Extractor (2013) http://www.securitytube-tools.net/index.php@title= Bulk_Extractor.html.

[11] Bulk Extractor (2013) http://www.forensicswiki.org/wiki/Bulk_extractor.

[12] Bulk Extractor (2013) http://digitalcorpora.org/downloads/bulk_extractor/.

[13] Bulk Extractor (2013) http://wiki.bitcurator.net/index.php?title=Using_ bulk_extractor_to_Find_Personal_Identifiable_Information_%28PII%29_on_a_Disk_I mage.

[14] Bunting, S. (2008) EnCase Computer Forensics, The Official EnCE : EnCase Certified Examiner, Study Guide, Second Edition. Wiley Publishing, Inc, Indianapolis, Indiana, USA.

[15] Buster Sandbox Analyzer (BSA) (2013) http://bsa.isoftware.nl/.

[16] Cantrell, G., Dampier, D., Yoginder, S., Dandass, N., and Bogen, C. (2012) Research toward a Partially-Automated, and Crime Specific Digital Triage Process Model. *Computer and Information Science*, Vol. 5, No. 2, March.

[17] Carrier, B. (2006) Basic Digital Forensic Investigation Concepts. http://www.digital-evidence.org/.

[18] Carrier, B. (2001) Defining digital forensic examination and analysis tools. *International Journal of Digital Evidence, Digital Research Workshop II.*

[19] Carvey, H. (2012) Windows Forensic Analysis Toolkit, Advanced Analysis Techniques for Windows 7. Syngress, Elsevier, USA.

[20] Casey, E. (2009) Handbook of Digital Forensics and Investigation. Academic Press.

[21] Computer forensics (2013) https://en.wikipedia.org/wiki/Computer_forensics.

[22] Computer forensics (2013) http://computer-forensics.safemode.org/.

[23] Dickson, M. (2010) *Digital Triage*. Institute for Advanced Studies, SCDEA (Scottish Crime and Drug Enforcement Agency).

[24] Digital forensics (2013) http://en.wikipedia.org/wiki/Digital_forensics.

[25] DumpIt memory utility (2013) http://www.moonsols.com/windowsmemorytoolkit/.

[26] Dunbar, B. (2001) A detailed look at Steganographic: Techniques and their use in an Open-Systems Environment. *SANS Institute InfoSec Reading Room*.

[27] Eoghan, C. (2004) *Digital Evidence and Computer Crime, Second Edition*. Academic Press, Elsevier.

[28] Forensic Artifacts (2013) http://forensicartifacts.com/.

[29] Forensic Toolkit (2013) http://www.forensicswiki.org/wiki/Forensic_Toolkit.

[30] Garfinkel, S. (2013) Digital media triage with bulk data analysis and bulk extrac-

tor. Computers and Security 32, pp. 56-72.

[31] Garfinkel, S. (2012) Using bulk extractor for digital forensics triage and crossdrive analysis. Navy's Research University, Monterey, California, USA.

[32] Garfinkel, S. (2012) Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus. *Digital Investigation 9 S80–S89*, Elsevier.

[33] Garfinkel, S., Nelson. A., White, D., and Roussev, V. (2010) Using purpose-built functions and block hashes to enable small block and sub-file forensics. *Proceedings of the tenth annual DFRWS conference*, Elsevier, Portland.

[34] Garfinkel, S. (2007) Carving contiguous and fragmented files with fast object validation. *Proceedings of the 7th annual Digital Forensic Research Workshop (DFRWS)*, vol. 4, Elsevier, Pittsburgh, pp. 2 - 12.

[35] Garfinkel, S. (2006) Forensic Feature Extraction and Cross-Drive Analysis. *Digital Investigation* 3S S71–S81, Harvard University, Cambridge, USA.

[36] Geiger, M. (2005) Evaluating Commercial Counter-Forensic Tools. 2005 Digital Forensic Research Workshop (DFRWS,) New Orleans, USA.

[37] Gomez, L.S.M. (2012) *Triage in-Lab: case backlog reduction with forensic digital profiling*. Simposio Argentino de Informatica y Derecho, JAIIO - SID 2012, Argentina.

[38] Grobler, C., Louwrens, C., and Solms, S. (2010) *A framework to guide the implementation of Proactive Digital Forensics in organizations*. 2010 International Conference on Availability, Reliability and Security, Academy for Information Technology, University of Johannesburg, Johannesburg, South Africa.

[39] Gunsch, G. (2002) An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, Fall, Volume 1, Issue 3.

[40] Haggerty, J., and Taylor, M. (2006) *Managing corporate computer forensics*. Computer Fraud & Security Magazine, June 2006, School of Computing and Mathematical Sciences, Liverpool, John Moores University, United Kingdom.

[41] Halderman, A., Schoen, S., Heninger, N., Clarkson, W., Paul, W., Calandrino, J., Feldman, A., Appelbaum, J., and Felten, E. (2008) Lest We Remember: Cold Boot Attacks on Encryption Keys. *17th USENIX Security Symposium*, Princeton University, San Jose, California, USA.

[42] Hashkeeper (2013) http://www.forensicswiki.org/wiki/Hashkeeper.

[43] Hobocopy Utility (2013) https://github.com/candera/hobocopy/downloads.

[44] Horsman, G., Laing, C., and Vickers, P. (2011) *A case based reasoning system for automated forensic examinations*. PGNET 2011, the 12th annual postgraduate symposi-

um on the convergence of telecommunications, networking and broadcasting, 27–28 June, 2011, Liverpool.

[45] KFF (2013) http://www.forensicfocus.com/Forums/viewtopic/t=7307/.

[46] Kludge-3.20110223 (2013) http://theinterw3bs.com/?pO503.

[47 Lee, R., (2012) Sans-Digital-Forensics-and-Incident-Response-Poster 2012. Sans DFIR Faculty.

[48] Leighton, J. (2012) *Digital Forensics and Preservation*. DPC Technology Watch Report, Digital Preservation Coalition, Great Britain.

[49] Leigland, R. (2004) A Formalization of Digital Forensics. *International Journal of Digital Evidence*, Fall, Volume 3, Issue 2, University of Idaho, USA.

[50] MD5 (2013) http://www.forensicswiki.org/wiki/MD5.

[51] Md5deep and Sha1deep utilities (2013) http://md5deep.sourceforge.net/.

[52] Merriam-Webster dictionary Free (2013) http://www.merriam-webster.com/ dictionary/.

[53] Mislan, R., Casey, E., and Kessler, G. (2010) The growing need for on-scene triage of mobile devices. *Digital Investigation*, pp. 112–124.

[54] Mobile device forensics (2013) http://en.wikipedia.org/wiki/Mobile_device _forensics.

[55] Nathan, C. (2010) *Computer Forensics A Pocket Guide*. IT Governance Publishing, United Kingdom.

[56] National Software Reference Library(2013)http://www.forensicswiki.org/wiki/National_Software_Reference_Library.

[57] Nelson, B., Phillips, A., and Steuart, C. (2010) *Guide To Computer Forensics And Investigations, Third Edition.* Course technology, Cengage Learning.

[58] Netmarketshare. (2013) Market share statistics for internet technologies. Netmarketshare.

[59] Nirsoft web browsers tools package (2013) http://www.nirsoft.net/web_

browser_tools.html.

[60] Noblett, M., Pollitt, M., and Presley, L. (2000) Recovering and examining computer forensic evidence. Forensic Science Communications, Volume 2, Number 4, FBI, USA.

[61] OPSWAT. (2012) Antivirus market analysis. San Francisco, USA.

[62] Patterson, D. (2004) Latency lags bandwidth. *Communications of the ACM*. Volume 47, Issue 10, October 2004, pp. 71-75, New York, USA.

[63] Pearson, S., and Watson, R. (2010) *Digital Triage Forensics: processing the digital crime scene*. Syngress.

[64] Phillip, A., Cowen, D., and Davis, C. (2009) *Hacking Exposed: Computer Forensics*. McGraw Hill Professional.

[65] PHP (2013) http://el.wikipedia.org/wiki/PHP.

[66] PHP (2013) http://php.net/.

[67] Python (2013) http://el.wikipedia.org/wiki/Python.

[68] Python (2013) http://www.python.org/.

[69] RCFL (2013) RCFL annual reports FY2003 - FY2012, USA.

[70] RegRipper (2013) http://code.google.com/p/winforensicaanalysis/downloads/ list.

[71] Reith, M., Carr, C., and Gunsch, G. (2002) An examination of digital forensic models. *International Journal of Digital Evidence*.

[72] Resendez, I., Martinez, P., and Abraham, J. (2008) An Introduction to Digital Forensics, University of Texas Pan American.

[73] Ricci, S.C. (2006) FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital investigation* 3S S29 – S36.

[74] Rogers, M.K., Goldman, J., Mislan, R., Wedge, T., and Debrota, S. (2006) Computer forensics field triage process model. *Proceedings of the conference on Digital Forensics, Security and Law,* Las Vegas, Nevada, USA, pp. 27–40.

[75] Roussev, V., Quates, C., and Martell, R. (2013) Real-time digital forensics and triage. *Digital Investigation*, University of New Orleans, USA.

[76] Sandboxie (2013) http://www.sandboxie.com, http://www.sandboxie.com/ index.php?AllPages.

[77] Shiaeles, S., et al. (2013) On-scene triage open source forensic tool chests: Are they effective?. *Digital Investigation*.

[78] Skoudis, E. (2006) *Windows Command-Line Kung Fu with WMIC*. SANS Technology Institute.

[79] Sleuthkit (2013) http://wiki.sleuthkit.org.

[80] Sliter, J. (2006) Organized Crime in Business. *Journal of Financial Crime, vol. 13, no.4, Emerald*, pp. 383-386.

[81] Sommer, P. (2005) Directors and Corporate Advisors' Guide to Digital Investigations and Evidence. *Information Assurance Advisory Council*, United Kingdom.

[82] SPEKTOR triage tool (2013) http://www.evidencetalks.com/index.php?

optionOcom_content&viewOcategory&layoutOblog&idO83&ItemidO513.

[83] SQLite Manager (2013) https://addons.mozilla.org/el/firefox/addon/sqlitemanager/.

[84] Sublime Text Editor (2013) http://en.wikipedia.org/wiki/Sublime_Text.

[85] Sublime Text Editor (2013) http://www.sublimetext.com/.

[86] Suiche, M. (2008) Windows hibernation file for fun 'n' profit. Black hat 2008.

[87] Sysinternals Suite (2013) http://technet.microsoft.com/en-us/sysinternals/ bb84206.

[88] The Flex Project (2013) http://flex.sourceforge.net/.

[89] TR3Secure (2013) http://code.google.com/p/jiir-resources/downloads/detail?

nameOtr3secure_data-collection-script.zip&canO2&qO.

[90] TriageIR v.79 (2013) http://code.google.com/p/triage-ir/downloads/list.

[91] VBScript (2013) http://en.wikipedia.org/wiki/VBScript.

[92] VBScript (2013) http://msdn.microsoft.com/enus/library/t0aew7h6%28v=vs.84%29.aspx.

[93] Waits, C., Akinyele, J.A., Nolan, R., and Roggers, L. (2008) *Computer forensics: results of live response inquiry vs. memory image analysis.* CERT Digital Intelligence and Investigation Directorate (DIID), Software Engineering Institute, Carnegie Mellon University.

[94] WAMP Server (2013) http://en.wikipedia.org/wiki/WAMP.

[95] WAMP Server (2013) http://www.wampserver.com/en/.

[96] Wikipedia - Memory Imaging (2013) http://www.forensicswiki.org/ wiki/Tools:Memory_Imaging.

[97] Windows XP Embedded (WinXPe) OS (2013) http://www.microsoft.com/

windowsembedded/en-us/develop/windows-xp-embedded-fordevelopers.aspx.

[98] Wolfe, P. (2007) EXP-SA: Prediction and Detection of Network Membership through Automated Hard Drive Analysis. *National Science Foundation*, Harvard University, Cambridge, USA.

[99] Yasinsac, A., Erbacher, R., Marks, D., and Pollitt, M. (2003) Computer forensics education. *IEEE Security & Privacy*.

[100] 7Zip Command Line (2013) http://www.7-zip.org/.

Appendix

1) The program scanner.php in the PHP programming language:

<?php

error_reporting(E_ERROR | E_WARNING | E_PARSE);

//solution to return *.* files

```
$array = array();
```

function recursiveGlob(\$dir, \$ext) {

global \$array;

\$globFiles = glob("\$dir/*.\$ext");

```
$globDirs = glob("$dir/*", GLOB_ONLYDIR);
```

foreach (\$globDirs as \$dir) {
 recursiveGlob(\$dir, \$ext);

}

```
foreach ($globFiles as $file) {
    if(!in_array($file,$array)) {
        array_push($array,$file);
    }
}
return $array;
```

//only use in CLI mode because of extra large buffer and execution time

```
if ($argv[1] == "help" || $argv[1] == null) {
  echo "-- SCAN MODE --\r\n";
  echo
           "Usage:
                        php
                                scanner.php
                                                          --path=path to check
                                                 scan
                                                                                    --
extension=extension_to_filter --log_file=path_and_name_of_log_file \r\n";
  echo "r\n";
  echo "Example: php scanner.php scan --path=\"C:\myfolder\\\" --extension=\"exe\" --
\log_{file=\"C:\mydocuments\md5_log.txt\"\r\n";}
  echo "r\n";
  echo
           "Default
                       values:
                                  --path=\"C:\Windows\"
                                                           --extension=\"exe\"
                                                                                    --
log_file=\"C:\\logfile\md5_log_file.txt\" \r\n";
  echo "r\n";
  echo "-- COMPARE MODE --\r\n";
  echo "Usage: php scanner.php compare --log_file=path_and_name_of_log_file --
md5 values file=path and name of md5 values file
                                                                                    ___
results_file=path_of_results_file \r\n";
  echo "r\n";
  echo "Example: php scanner.php compare --log_file=\"C:\\log_file_after_scan.txt\" --
md5_values_file=\"C:\\file_with_clean_md5_values.txt
                                                                                    ___
results_file=\"C:\\file_with_results.txt \r\n";
  echo "r\n";
  die();
}
if ($argv[1] == "debug") {
```

```
for ($i=2; $i < $argc; $i++) {
    $tempvar = explode("=", $argv[$i]);</pre>
```

```
echo $tempvar[1]."\r\n";
  }
}
if ($argv[1] == "scan") {
  echo "Starting scan. Please wait...\r\n";
  for ($i=2; $i < $argc ; $i++) {
     $tempvar = explode("=", $argv[$i]);
     switch ($tempvar[0]) {
       case '--path':
       $directory = $tempvar[1]."*";
       break;
       case '--extension':
       $extension = $tempvar[1];
       break;
       case '--log_file':
       $log_file = $tempvar[1];
       break;
     }
  }
  if ($argc < 5) {
     if (!$directory) {
       $directory = "C:\Windows\\*";
     }
     if (!$extension) {
       $extension = "exe";
     }
     if (!$log_file) {
       $log_file = "C:\\logfile\md5_log_file.txt";
```

} }

```
echo "the directory is ".$directory."\r\n";
echo "the extension is ".$extension."\r\n";
echo "the log file is ".$log_file."\r\n";
```

```
$files = recursiveGlob($directory,$extension);
  fh = fopen(flog_file, "w") or die("can't open file \r\n");
  var_dump($files);
  $i = 1;
  foreach ($files as $file) {
     $stringData = $i.") Found file: ".$file."\r\n";
$stringData .= "Hash: ".md5_file($file)."\r\n";
$i++;
fwrite($fh, $stringData);
```

```
fclose($fh);
```

}

```
if ($argv[1] == "compare") {
  echo "Starting compare. Please wait...\r\n";
  for ($i=2; $i < $argc ; $i++) {
     $tempvar = explode("=", $argv[$i]);
     switch ($tempvar[0]) {
       case '--md5_values_file':
       $md5_values_file = $tempvar[1];
```

```
break;
case '--log_file':
$log_file = $tempvar[1];
break;
case '--results_file':
$results_file = $tempvar[1];
break;
default:
echo "error: loop defaulted\r\n";
break;
}
```

```
if ($argc < 4) {
```

echo "Wrong count of parameters. Please type php scanner.php help for more info";

die();

if (\$check[0] == "Hash:") {

}

```
$scanned
                =
                        file($log_file,
                                           FILE_IGNORE_NEW_LINES
                                                                             FILE_SKIP_EMPTY_LINES);
                      file($md5_values_file,
  $clean_md5
                =
                                              FILE_IGNORE_NEW_LINES
                                                                             FILE_SKIP_EMPTY_LINES);
  $clean_md5_size = count($clean_md5);
  $i = 1;
  fh = fopen(fresults_file, "w") or die("can't open file \r\n");
  foreach ($scanned as $line_num => $line) {
    $check = explode(" ", $line);
```

```
foreach ($clean_md5 as $clean_line_num => $clean_line) {
          $md5_check = explode(" ", $clean_line);
          if ($md5_check[0] == "Hash:") {
            if ($check[1] == $md5_check[1]) {
             break;
           }
           if (($clean_line_num + 1) == $clean_md5_size) {
             echo "Suspicious file found -> ".$pathname[1]."\r\n";
             $stringData = $i.") Suspicious file found -> ".$pathname[1]."\r\n";
             $i++;
             fwrite($fh, $stringData);
           }
         }
      }
    } else {
  $pathname = explode(": ", $line);
  }
fclose($fh);
```

2) The program scanner_version_2.php in the PHP programming language:

<?php

}

}

?>

error_reporting(E_ERROR | E_WARNING | E_PARSE);

```
//solution to return *.* files
```

```
$array = array();
function recursiveGlob($dir, $ext) {
  global $array;
  $globFiles = glob("$dir/*.$ext");
  $globDirs = glob("$dir/*", GLOB_ONLYDIR);
  foreach ($globDirs as $dir) {
    recursiveGlob($dir, $ext);
  }
  foreach ($globFiles as $file) {
    if(!in_array($file,$array)) {
       array_push($array,$file);
    }
  }
  return $array;
}
```

//only use in CLI mode because of extra large buffer and execution time

```
if ($argv[1] == "help" || $argv[1] == null) {
```

```
echo "-- SCAN MODE --\r\n";
```

echo "Usage: php scanner.php scan --path=path_to_check -extension=extension_to_filter --log_file=path_and_name_of_log_file \r\n";

echo "\r\n";

echo "Example: php scanner.php scan --path=\"C:\myfolder\\\" --extension=\"exe\" -log_file=\"C:\mydocuments\md5_log.txt\" \r\n"; echo " $r\n";$

```
echo "Default values: --path=\"C:\Windows\" --extension=\"exe\" --
log_file=\"C:\\logfile\md5_log_file.txt\" \r\n";
```

echo " $r\n";$

echo "-- COMPARE MODE --\r\n";

```
echo "Usage: php scanner.php compare --log_file=path_and_name_of_log_file --
md5_values_file=path_and_name_of_md5_values_file --
```

results_file=path_of_results_file \r\n";

echo "rn";

```
echo "Example: php scanner.php compare --log_file=\"C:\\log_file_after_scan.txt\" --
md5_values_file=\"C:\\file_with_clean_md5_values.txt --
results_file=\"C:\\file_with_results.txt \r\n";
```

echo " $r\n";$

die();

}

```
if ($argv[1] == "debug") {
```

```
for ($i=2; $i < $argc; $i++) {
    $tempvar = explode("=", $argv[$i]);
    echo $tempvar[1]."\r\n";
}</pre>
```

```
}
```

```
if ($argv[1] == "scan") {
```

echo "Starting scan. Please wait...\r\n"; for (i=2; i < argc; i++) {

```
$tempvar = explode("=", $argv[$i]);
```

```
switch ($tempvar[0]) {
```

```
case '--path':
```

```
$directory = $tempvar[1]."*";
     break;
     case '--extension':
     $extension = $tempvar[1];
     break;
     case '--log_file':
     $log_file = $tempvar[1];
     break;
  }
}
if ($argc < 5) {
  if (!$directory) {
     $directory = "C:\Windows\\*";
  }
  if (!$extension) {
     $extension = "exe";
  }
  if (!$log_file) {
     $log_file = "C:\\logfile\md5_log_file.txt";
  }
}
echo "the directory is ".$directory."\r\n";
echo "the extension is ".$extension."\r\n";
echo "the log file is ".$log_file."\r\n";
```

```
$files = recursiveGlob($directory,$extension);
$fh = fopen($log_file, "w") or die("can't open file \r\n");
var_dump($files);
```

```
$i = 1;
foreach ($files as $file) {
    $stringData = $i.") Found file: ".$file."\r\n";
    $stringData .= "Hash: ".md5_file($file)."\r\n";
    $i++;
    fwrite($fh, $stringData);
}
```

```
fclose($fh);
```

```
if ($argv[1] == "compare") {
  echo "Starting compare. Please wait...\r\n";
  for ($i=2; $i < $argc ; $i++) {
     $tempvar = explode("=", $argv[$i]);
     switch ($tempvar[0]) {
       case '--md5_values_file':
       $md5_values_file = $tempvar[1];
       break;
       case '--log_file':
       $log_file = $tempvar[1];
       break;
       case '--results_file':
       $results_file = $tempvar[1];
       break;
       default:
       echo "error: loop defaulted\r\n";
       break;
```

```
}
}
if ($argc < 4) {
    echo "Wrong count of parameters. Please type php run.php help for more info";
    die();
}</pre>
```

```
$scanned
                  =
                          file($log_file,
                                               FILE_IGNORE_NEW_LINES
                                                                                    FILE_SKIP_EMPTY_LINES);
  $clean md5
                  =
                       file($md5_values_file,
                                                  FILE_IGNORE_NEW_LINES
                                                                                    FILE_SKIP_EMPTY_LINES);
  $clean_md5_size = count($clean_md5);
  $i = 1;
  $fh = fopen($results_file, "w") or die("can't open file \r\n");
  foreach ($scanned as $line_num => $line) {
    $check = explode(" ", $line);
    if ($check[0] == "Hash:") {
       foreach ($clean_md5 as $clean_line_num => $clean_line) {
         if ($check[1] == $clean_line) {
            break;
         }
         if ((\text{sclean\_line\_num} + 1) == \text{sclean\_md5\_size})
            echo "Suspicious file found -> ".$pathname[1]."\r\n";
            $stringData = $i.") Suspicious file found -> ".$pathname[1]."\r\n";
            $i++;
            fwrite($fh, $stringData);
         }
```

```
}
else {
    $pathname = explode(": ", $line);
}
fclose($fh);
}
```

?>

3) The program scanner_version_3.php in the PHP programming language:

<?php

error_reporting(E_ERROR | E_WARNING | E_PARSE);

//solution to return *.* files

```
$array = array();
```

```
function recursiveGlob($dir, $ext) {
```

global \$array;

```
$globFiles = glob("$dir/*.$ext");
```

```
$globDirs = glob("$dir/*", GLOB_ONLYDIR);
```

```
foreach ($globDirs as $dir) {
   recursiveGlob($dir, $ext);
```

```
foreach ($globFiles as $file) {
```

```
if(!in_array($file,$array)) {
    array_push($array,$file);
    }
    return $array;
}
```

//only use in CLI mode because of extra large buffer and execution time

```
if ($argv[1] == "help" || $argv[1] == null) {
```

```
echo "-- SCAN MODE --\r\n";
```

echo "Usage: php scanner.php scan --path=path_to_check -extension=extension_to_filter --log_file=path_and_name_of_log_file \r\n";

echo " $r\n";$

```
echo "Example: php scanner.php scan --path=\"C:\myfolder\\\" --extension=\"exe\" --
log_file=\"C:\mydocuments\md5_log.txt\" \r\n";
```

echo " $r\n";$

 $echo "Default values: --path=\"C:\Windows\" --extension=\"exe\" --log_file=\"C:\logfile\md5_log_file.txt\" \r\n";$

echo " $r\n";$

```
echo "-- COMPARE MODE --\r\n";
```

```
echo "Usage: php scanner.php compare --log_file=path_and_name_of_log_file --
md5_values_file=path_and_name_of_md5_values_file --
```

results_file=path_of_results_file \r\n";

echo " $r\n";$

echo "Example: php scanner.php compare --log_file=\"C:\\log_file_after_scan.txt\" -md5_values_file=\"C:\\file_with_clean_md5_values.txt --

results_file=\"C:\\file_with_results.txt \r\n";

echo "rn";

```
die();
```

```
}
if ($argv[1] == "debug") {
  for ($i=2; $i < $argc; $i++) {
     $tempvar = explode("=", $argv[$i]);
     echo $tempvar[1]."\r\n";
  }
}</pre>
```

```
if ($argv[1] == "scan") {
  echo "Starting scan. Please wait...\r\n";
  for ($i=2; $i < $argc ; $i++) {
     $tempvar = explode("=", $argv[$i]);
     switch ($tempvar[0]) {
        case '--path':
        $directory = $tempvar[1]."*";
        break;
        case '--extension':
        $extension = $tempvar[1];
        break;
       case '--log_file':
        $log_file = $tempvar[1];
        break;
     }
   }
  if ($argc < 5) {
     if (!$directory) {
```

```
$directory = "C:\Windows\\*";
}
if (!$extension) {
    $extension = "exe";
}
if (!$log_file) {
    $log_file = "C:\\logfile\md5_log_file.txt";
}
```

```
echo "the directory is ".$directory."\r\n";
echo "the extension is ".$extension."\r\n";
echo "the log file is ".$log_file."\r\n";
```

```
$files = recursiveGlob($directory,$extension);
$fh = fopen($log_file, "w") or die("can't open file \r\n");
var_dump($files);
```

```
foreach ($files as $file) {
```

```
$stringData = md5_file($file)."\r\n";
```

```
fwrite($fh, $stringData);
```

```
}
```

```
fclose($fh);
```

```
if ($argv[1] == "compare") {
  echo "Starting compare. Please wait...\r\n";
  for ($i=2; $i < $argc ; $i++) {
     $tempvar = explode("=", $argv[$i]);
     switch ($tempvar[0]) {
       case '--md5_values_file':
       $md5_values_file = $tempvar[1];
       break;
       case '--log_file':
       $log_file = $tempvar[1];
       break;
       case '--results_file':
       $results_file = $tempvar[1];
       break;
       default:
       echo "error: loop defaulted\r\n";
       break;
     }
  }
  if (\$ argc < 4) {
    echo "Wrong count of parameters. Please type php run.php help for more info";
    die();
  }
                          file($log_file,
  $scanned
                  =
                                               FILE_IGNORE_NEW_LINES
                                                                                    FILE_SKIP_EMPTY_LINES);
                        file($md5_values_file,
  $clean_md5
                  =
                                                 FILE_IGNORE_NEW_LINES
                                                                                    FILE_SKIP_EMPTY_LINES);
  $clean_md5_size = count($clean_md5);
```

```
$fh = fopen($results_file, "w") or die("can't open file \r\n");
  foreach ($scanned as $line_num => $line) {
    $check = explode(" ", $line);
    if ($check[0] == "Hash:") {
       foreach ($clean_md5 as $clean_line_num => $clean_line) {
         if ($check[1] == $clean_line) {
            break;
          }
         if (($clean_line_num + 1) == $clean_md5_size) {
            echo "Suspicious file found -> ".$pathname[1]."\r\n";
            $stringData = $i.") Suspicious file found -> ".$pathname[1]."\r\n";
            $i++;
            fwrite($fh, $stringData);
          }
       }
     }
    else {
       $pathname = explode(": ", $line);
     }
  }
  fclose($fh);
?>
```