Digital Forensics Random Access Memory Using Live Technique Based On Network Attacked

By periyadi periyadi

WORD COUNT 3671 TIME SUBMITTED 19-FEB-2019 08:38AM
PAPER ID 44491798

Digital Forensics Random Access Memory Using Live Technique Based On Network Attacked

Periyadi[1], Giva Andriana Mutiara[1], Roni Wijaya[1]
[1]Applied Science School, Telkom University
Bandung, Indonesia
periyadi@tass.telkomuniversity.ac.id
giva.andriana@tass.telkomuniversity.ac.id
roni.wijaya.2728@gmail.com

***Abstract*—The development of information and communication technologies are increasing rapidly. The security of data processed and stored also must be prepared in higher security. One of the techniques in data security is digital forensics. Digital forensics is an investigative technique to identify or collect the information on a digital storage as evidence to expose crimes legally defensible. However, in this research we use a live forensics digital technique. Investigations using live forensics technique requires special handling because the volatile data in Random Access Memory which can be lost if the system is in off investigation. This investigation conducted on the system by dump memory investigator to the system which has been attacked and then transferred the file on system investigator. We investigate the data inside the RAM and make analysis about the accuracy using several cyber attacks like session hijacking, FTP attack, and illegal access. The result shows that all the attacks can be investigated and produced the evidence which is authentic, reliable, and defensible.**

Keywords—digital forensics; dumpmemory; live forensics; memory accuisition; Random Access Memory

I. INTRODUCTION

The utilization of information and communication becomes very important and must be presents in the process of developing an institution or company. This dependency unwittingly will increase the crime of technology and communication which will be a risk for institutions or companies.

The presence of information and electronic transaction laws turns out less a major contribution in the process of enforcement of legal cases in Indonesia. This is because this law appears to be merely regulate the flow of electronics information in general. Yet, there are a lot of things that are detailed in legal cases and enforcement issues in Indonesia that have not been regulated in the law. The things that are detailed is used as reference in information technology security which is leading to the digital forensics.

Inside a computer system, there are main memory or known as Random Access Memory (RAM), which play a very important component in a system [1]. RAM is one of volatile storage media or data. Volatile is the technique of storage media that data will be lost if there is no electricity [1]. Volatile data in RAM is very useful for forensics process, because the RAM in computer system describes all the activities that have been occurred on the system during the system was running.

Forensics investigators memory is the process of analyzing the volatile data in RAM to obtain digital evidence that can be responsible accounted for [2]. Handling of volatile data in RAM must be careful because data can be lost if the system is turned off. Therefore, we need a memory forensics techniques to ensure data integrity volatile without losing data that could potentially be evidence.

Some of security researcher Sam Stover and Matt Dickerson do the digital forensics on non-volatile storage such as hard drive that has been physically removed by The Coroners Toolkit (TCT) [3]. Timothy Vidas do the research in the acquisition and analysis of Random Access Memory, and discusses the benefits and drawbacks of traditional incident response methods compared to augmented model that includes the capture and subsequent analysis of a suspect system's memory, provides a foundation for analyzing capture memory [4].

In this research, we investigate the data in Random Access Memory using live forensics and make an analysis about the accuracy of the data as the result of forensic memory by using some variation of several case scenarios that were tested. The attacked scenario that will be used is session hijacking, FTP attack, and illegal access using 64 bit operating system Kali Linux 2.0.

II. LITERATURE STUDY

A. Digital Forensic

Digital Forensics is the use of analysis and investigate techniques to identify, collect, examine, and save the evidence of information which is stored in a digital storage that can be used as evidence in exposes crimes legally defensible [5]. Digital forensics is commonly used in both criminal law and private investigation.

Fig.1 shows a process of forensics digital. The first step is collection the data. Digital media that can be used as evidence such as a storage like flash disk, mobile phone, memory and hard disk are collected as the data to be examine in the next step. The second process is examination, data which has been collect will be examined by cloning or imaging the data. This

ISBN: 978-1-5090-4911-0 (c) 2017 IEEE

can be done by doing a copy data bit stream image in a safe place. Bit stream is a method of storing digital image by copying all the bits of the original data including hidden files, temporary files, defragmented file and the file which has not overwrite yet.

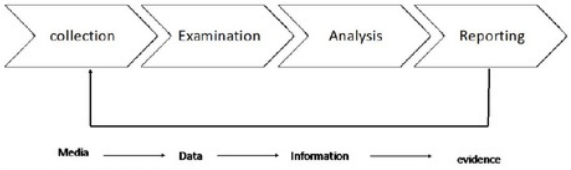

Fig. 1. Forensics Process

The third step is analysis. In this step all the data will be analyzed and make the recovery to store back the file and the folder. The tools for analyze the data is using MD5. The last step is reporting. This step is presenting and describing the investigation report and the evidence that had been analyzed in detail and can be justified as scientific.

B. *Random Access Memory*

Random Access Memory is the main memory of a computer. RAM is volatile, it is means that in RAM data will be lost when the power of computer is turned off. Besides that, RAM is used to store data temporarily and randomly, and issued the requested data processor also data flow from RAM as dynamic and in a very high speed [6].

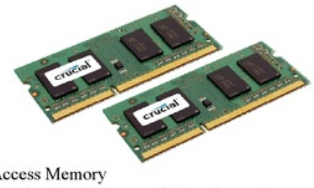

Fig. 2. Random Access Memory

Fig.2 shown the hardware of Random Access memory as the main memory of system computer. RAM in computer system will be analyzed to found the evidence of the intrusion from the attacker. RAM analysis captured is a process of capturing live memory from running computer system. RAM analysis consists of performing forensics analysis on the data gathered from the live computer.

After conducting a memory dump on any live machine to capture RAM, the memory image can be used to determine information about running program, the operating system, and the overall state of a computer, as well as to locate deleted or temporary information that might otherwise not be found on a normal image [7].

There are a lot of tools that available to serve aid forensics analysis in the capturing of RAM data. There are FTK Imager, Volatility (using Kali Linux tool), Win64dd/MWMT DumpIt.

C. *Operating System*

Operating System (OS) is a program that controls the execution of application programs and act as the user interface of computers and computer hardware. An Operating System has a kernel. Kernel is a computer program that set the input/output requests from the software and translate them into instructions on the processor or on other electronic components on a computer.

In general, the operating system is divided into several sections: (1) boot mechanism, placing the kernel into memory, (2) kernel, the core part of an operating system, (3) shell or command interpreter, which reads input from the user, (4) library as providers of basic sets of functions and instructions in operating system [8].

D. *Live Forensic*

Forensics Memory is one of the existing forensics techniques. In the digital's world forensics, there are two forensics techniques. The traditional forensics and live forensics. Traditional or known as offline forensics techniques is a first technique using in computer forensics and commonly used by the researcher to do the forensics data. This technique requires the investigator to shut down the attacked system. Its aimed to anticipation any malicious processes running on the system which can be delete the important data for investigation purposes [9].

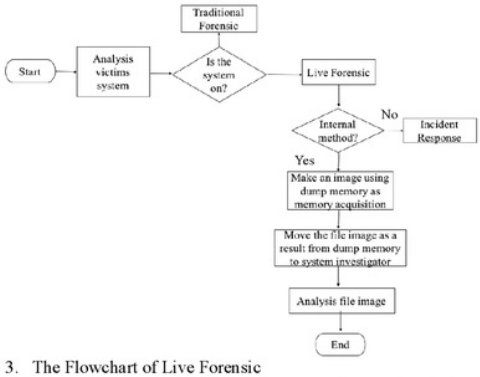

Fig. 3. The Flowchart of Live Forensic

Meanwhile, live forensics is an enhanced of traditional forensics. This technique is performed in the volatile data on a computer system [9]. This technique is much different from the traditional forensics technique, because this data must be investigated in lively.

Live forensics analysis is divided into two ways, internal analysis and external analysis. Internal analysis commonly called as incident response is a method of analysis that is performed directly in the attacked system. While the external analysis done the analysis first by acquisition the memory or called as dump memory or memory imaging, using software installed on an attacked system that aims to provide digital files containing snapshots (portrait) static volatile memory on attacked system [9].

The result of this dump memory is a file image form that can be moved to an investigator's system for further analysis. Fig.3. shown the step of live forensics.

III. Design Requirement System

This research conducts an investigation on the attacked system. Before doing the design of the system, we made an analysis of the requirement system. This system requires three

virtual machines that will be used as an investigator (host), the victim (windows OS), and the attacker (kali linux). The specification of those virtual machines can be seen in the following table.

TABLE I. SPECIFICATION VIRTUAL MACHINE

Virtual Machine no.	Act As	Hardware and Software Specification
Virtual Machine 1 on Virtual Box GUI Version 4.3.36	As investigator (host)	Using a 64 bit XUbuntu Operating System 14.04.1 LTS with IP address configuration 192.168.25.1. The software specification in this VM is Volatility, Bulk Extractor, and wireshark
Virtual Machine 2 on Virtual Box GUI Version 4.3.36	As the victims	Using a 32 bit Windows XP SP3 Professional with IP address configuration 192.168.25.101. The software specification added is Browser, XAMPP, DVWA
Virtual Machine 3 on Virtual Box GUI Version 4.3.36	As the Attacker	Using a 64 bit Kali Linux with IP Address Configuration 192.168.25.102.

Based on the specification above, the design testing topology for this research shown in Fig 4.

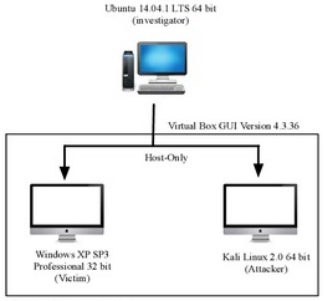

Fig. 4. Topology of Testing system

After designing the testing topology, we design a procedure to implement the system that appropriate with requirement system. The procedure can be shown in Fig 5 below.

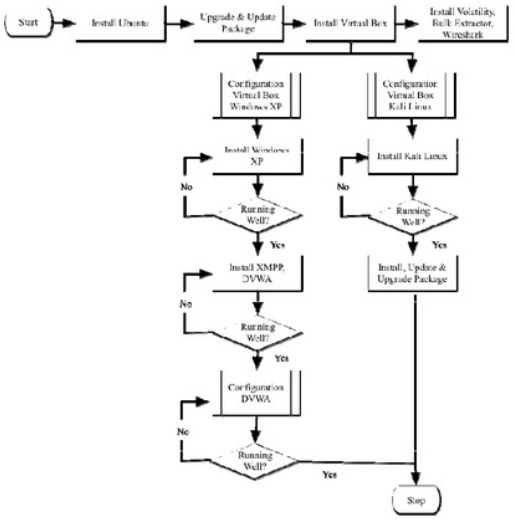

Fig. 5. Implementation Flowchart

IV. INVESTIGATE AND RESULT ANALYSIS

After determine the requirement system, topology testing system and implementation the system, the next step is doing the investigation and analysis system. The implementation of the system adapted to the requirements of each virtual machine was already planned in the previous chapter.

Fig.6 shows flow diagram about the logic testing diagram that will be done as the step of investigator to get the evidence of the intrusion. The logic test block diagram is adopted from the forensics process.

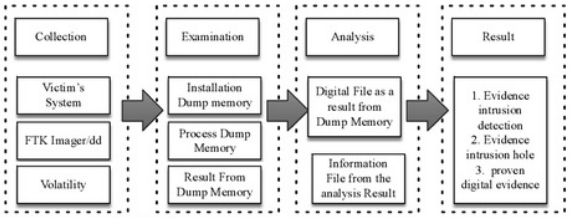

Fig. 6. Logic Testing Diagram

A. *Investigation*

Testing scenario as the investigation in this system is using several cyber attacked techniques. The first scenario is hijacking session. This scenario is the process of taking control the victim's session. But, the attacker should get the ID of authentication session which stored in the cookie. So that, the attacker will try to get a cookie's victims.

The second scenario is FTP Attack. This scenario is the process of taking control of the system by taking a security gap in the FTP. The attacker will perform a brute force on FTP. After successfully entered the system, attacker will perform activities using the victim's system.

The last scenario is Illegal Access. In this scenario, the attacker will do the access to the victim's system through the network. The attacker will try to find the hole in the security network and go through the system using this gap. Once attackers get into the system, the attacker will make some changes and downloading the file. After that the attacker will upload the payload on the system.

All the scenario will apply as an investigator. To determine the accuracy of this method, the investigator should identify IP address attacker, the security hole using to login the system, the changes that have been made by the attacker, what files were downloaded by the attacker, find the payload, and the timing of the attack.

Fig.7 shown the flow diagram about the all scenario as the intrusion to the system.

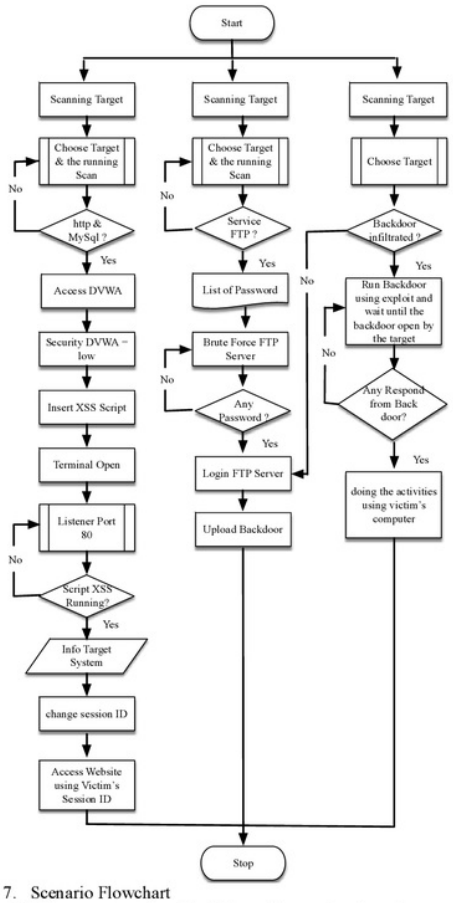

Fig. 7. Scenario Flowchart

All the system that had been intrusion by the attacker will be investigated with different step of investigation. The flowchart of investigation can be shown in Fig.8 below. The investigation of session hijacking and FTP attack have the same step of investigation while the investigation of illegal access is different with the others.

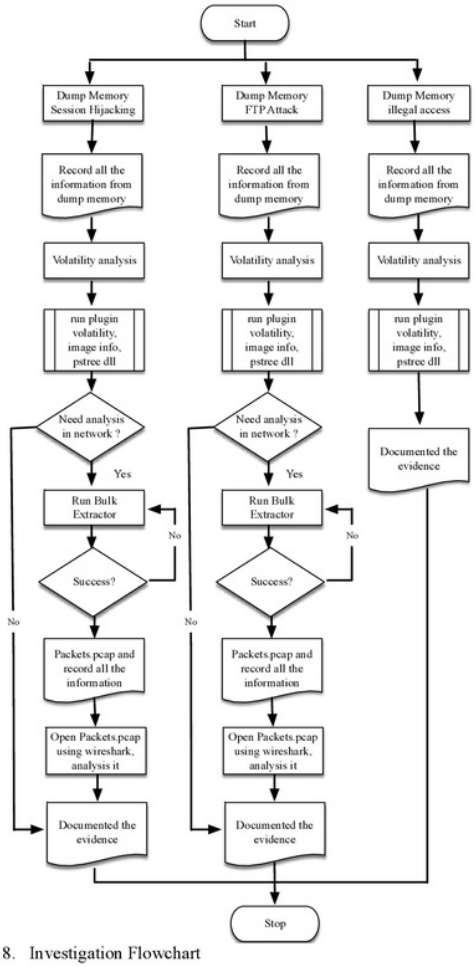

Fig. 8. Investigation Flowchart

B. *Result Analysis*

The result of the investigation conducted to several intrusion scenarios that have been tested will be described shortly only about the information file of dump memory, the information file of packets, pcap, information file of timeline MACtime, and the summary of result analysis on each intrusion scenario.

- Session Hijacking

Information file of session hijacking can be seen at table II, while the summary record result analysis of session hijacking can be seen in table III below.

TABLE II. INFORMATION FILE OF SESSION HIJACKING

Parameter	Dump Memory	Packets.pcap	Timeline Mac-time
File name	22juni2016-SH.mem	Packets.pcap	Timeline-mactime.txt
File size	536805376	172689	5131951
File Address	/media/cyber/ 3C0A072C0A06E2 AE/ capturememory/ 22juni2016-SH.mm	/home/cyber/ out-bulk/ 22juni2016-SH/packets.pcap	/home/cyber/ timeliner/SH/ timeline-mactime.txt
MD5SUM	245538328fdd873cf 4d9e3392e5668c4	Cb94e3cd728 2b70761656a7 61566e90	940d40f2f1 86c2577dc5 10d8300e9710
Image local date and time	2016-06-22 17:26:59 +0700	-	-
Last Modify	2016-06-22 17:27:47.238921000 +0700	2016-07-15 23:11:28.40038 0827 +0700	2016-07-16 17:35:23.2499 04995 +0700
Last Change	2016-06-22 19:43:20.558112600 +0700	2016-07-15 23:11:28.40038 0827 +0700	2016-07-16 17:55:12.9579 31311 +0700

After doing analysis on timeline mac-time file, we discover some suspicious line. Based on parser file on Fig.9 there was a file, named "etc.php" which is a suspicious file as an attacker.

Fig. 9. Suspicious File on Parser

TABLE III. RESULT ANALYSIS OF SESSION HIJACKING

Parameter	Describe of information
Victim's Operating System	Windows XP SP2x86 and Windows XP SP3x86
Victim's PHPSESSID	1eerlridi5n06nobd8nkhpatg6
Attacker's IP Address	192.168.25.102
Attacker's Operating System	Linux x86_64
Attacker's Browser	Firefox/38.0, iceweasel/38.8.0
XSS Script	<script>document.location=http://192.168.25.102/?+document.cookie;</script>
Security gaps	DVWA Security=low
Port	80
Protocol	TCP
File upload	Etc.php
Method of attacker	Session hijacking
Time of intrusion	unknown

The simplest treatment to prevent the system from session hijacking is to perform the filtering of user input, so that the user can not insert HTML tags into the comment field or others. The result in table III will be announced as an evidence.

- FTP attack

Information file of FTP attack can be seen at table IV, while the summary record result analysis of FTP Attack can be seen in table V below.

After doing analysis on timeline mac-time file, we discover some suspicious line. Based on parser file on Fig.10 there was a file, named "penting.exe" which is a suspicious file as an attacker.

TABLE IV. INFORMATION FILE OF FTP ATTACK

Parameter	Dump Memory	Packets.pcap	Timeline Mac-time
File name	14juli2016-FTP.mem	Packets.pcap	Timeline-mactime.txt
File size	536805376	306421	3728513
MD5sum	/media/cyber/ 3C0A072C0A06E 2AE/ capture\memory/ 14juli2016-FTP.mm	/home/cyber/ out-bulk/ 14juli2016-FA/packets.pcap	/home/cyber/ timeliner/FA/ timeline-mactime.txt
MD5sum	84dee785935268c 161d612be2affbfc 4	D92108805ce72 625a78bb928cb e267a7	B6799857922f a2a558b6d0a9 cefcf6b9
Image Local date and time	2016-07-14 23:15:35 +0700	-	-
Last Modify	2016-07-14 23:16:17.4860240 0000 +0700	2016-07-16 22:23:35.07028 7482 +0700	2016-07-17 19:18:07.8618 33909 +0700
Last Change	2016-07-14 23:18:22.6052751 00 +0700	2016-07-16 22:23:35.07028 7482 +0700	2016-07-17 19:18:07.8618 33909 +0700

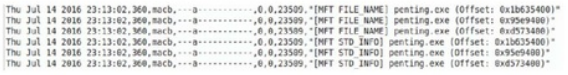

Fig. 10. Suspicious File on Parser FTP Attack

The simplest handling to avoid brute force is using passwords by combining capital letters, number, and special character. Besides that, don't forget to use the password with more than 8 characters, use the limited login attempt, and install the firewall on your network. The result in table V will be announced as an evidence.

TABLE V. RESULT ANALYSIS OF FTP ATTACK

Parameter	Describe of information
Victim's Operating System	Windows XP SP2x86 and Windows XP SP3x86
Attacker's IP Address	192.168.25.102
Security Gaps	FTP Server
Port	21
Protocol	FTP
User name	Root
File Upload	Penting.exe
Method of Attacker	Brute Force
Time of intrusion	unknown

- Illegal Access

Information file of Illegal Access can be seen at table VI, while the summary record result analysis of Illegal Access can be seen in table VII below.

TABLE VI. INFORMATION FILE OF ILLEGAL ACCESS

Parameter	Dump Memory	Plugin dlllist	Timeline Mac-time
File name	14juli2016-IA.mem	dllist-IA.txt	Timeline-mactime.txt
File size	536805376	4876	4961351
MD5sum	/media/cyber/3C0A072C0A06E2AE/capture\memory/14juli2016-IA.mem	/home/cyber/Volatility\File/14juli2016-dlllist-IA.txt	/home/cyber/timeliner/FA/timeline-mactime.txt
MD5sum	931933c6aaf338087742871432	13783bbfe8a418cd81d2719e96ad3502	Ea9834fcdc80ceabd6f136f758fadab4
Image Local date and time	2016-07-14 23:51:23 +0700	-	-
Last Modify	2016-07-14 23:51:57.21286 1000 +0700	2016-07-18 00:59:56.706287554 +0700	2016-07-18 01:25:37.650321639 +0700
Last Change	2016-07-14 23:56:50.70223 88 00 +0700	2016-07-18 00:59:56.706287554 +0700	2016-07-18 01:25:37.650321639 +0700

The information file of illegal access a little bit different from FTP attack and Session hijacking. We use plugin dlllist to make an investigation in order to get timeline-mactime.txt. Next, investigator will look at the history of the use of the console. However, after repeated iteration there was not found any suspicious thing. The result in table VII will be announced as an evidence.

TABLE VII. RESULT ANALYSIS OF ILLEGAL ACCESS

Parameter	Describe of information
Victim's Operating System	Windows XP SP2x86 and Windows XP SP3x86
Attacker's IP Address	192.168.25.102
Port	4444
Protocol	TCP
Backdoor	Penting.exe
The enhance of the priviledge	Done by Penting.exe
Dll file yang diakses	Dlllist-IA.text
Method of intrusion	Exploit Backdoor
Time of intrusion	unknown

The simplest handling to avoid brute force is using firewall software, perform regularly update antivirus, use software that can detect the anomaly in the network like snort.

V. CONCLUSION

Based on the result of investigator and analysis system, we can give a conclusion that live forensics using dump memory has been successfully done by giving an evidence as the result of investigator to the system which is attacked by three attacked methods in the cyber network. This evidence can be responsible and proven. Besides that, in order to avoid those all intrusion, we should to perform the filtering user input, use the passwords by combining capital letters, number, special character, and should be more than 8 characters. Otherwise, use the limited login attempt, install the firewall on your network, perform regularly update antivirus, and use software that can detect the anomaly in the network like snort.

ACKNOWLEDGMENT *(Heading 5)*

This Publication is financed by Directorate Research and Community Services of Telkom University.

REFERENCES

[1] M. H. Ligh, A. Case, J. Levy and A. Walters, The Art of Memory Forensics : Detecting Malware and Threats in Windows, Linux,and Mac Memory, Indianapolis,: John Wiley & Sons, Inc., 2014.

[2] F. Adelstein, "Live forensics: diagnosing your system without killing it first," *Communications of the ACM,* vol. Volume 49 , no. Issue 2, February 2006

[3] Stover S., Dickerson M. Using Memory Dumps in Digital Forensics. ;Login:magazine. Volume 30, Issue 5 December 2005. In press.

[4] Vidas, Timothy. Starting a Framework for analysis of Volatile Data Stores. Third Annual ifip WG 11.9 International Conference on Digital Forensics. Orlando, Florida. Jan 28-31, 2007.

[5] Asrizal, "Digital Forensik Apa dan Bagaimana," 30 December 2010.[online]. Available: e-dokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf. in.press

[6] Tanembaum, Andrew S. "Structured Computer Organization ". 4th edition. Prentice Hall. 1999. Pp.200-201.

[7] Gross Christie., " Digital Forensics RAM Analysis" http://nest.unm.edu/files/7114/1392/6819/USCyberCrime-CG.pdf. [online]

[8] Stalling, William. " Operating Systems". 4th edition. Prentice Hall. 2015. Pp. 30-35

[9] M.Lessing and B.v.Solms, "Live Forensic Acquisition as Altmative to Tradisional Forensic Processes," 2008.

Digital Forensics Random Access Memory Using Live Technique Based On Network Attacked

ORIGINALITY REPORT

7%

SIMILARITY INDEX

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

★nest.unm.edu
Internet
2%

EXCLUDE QUOTES ON
EXCLUDE BIBLIOGRAPHY ON
EXCLUDE MATCHES OFF