Live Digital Forensics: Windows XP vs Windows 7

Fenu Gianni
University of Cagliari
Dept. of Computer Science
Cagliari, Italy
Email: fenu@unica.it

Fabrizio Solinas
University of Cagliari
Dept. of Computer Science
Cagliari, Italy
Email: fabrizio.solinas@unica.it

***Abstract*—Over the last few years, analysing a computer or a digital device has become a necessity in the field of criminal investigations. Traditional digital forensics analysis includes static analysis, which concerns data that are permanently stored in devices, and live analysis, which regards data that are temporarily stored in equipments or that transit in networks. This paper proposes a live forensics analysis on two different operating systems: Windows XP and Windows Seven. The case study focuses on some common applications such as Skype, Google Talk and the browser Internet Explorer. The last software involves only those cases in which the browser is surfing on Facebook, Yahoo, Hotmail and Gmail. In addition, although many types of applications are payment software, one of the main objectives of this work has been the only use of the free software in order to prove the possibility to obtain the same results minimizing the costs.**

***Index Terms*—live forensics, RAM forensics analysis, computer forensic investigation, cybercrime, investigation**

I. Introduction

Whichever organization, businesses or government is actually making efforts to contrast cybercrime. Moreover, although digital forensics has recently faced new challenges [1], it still remains the main way to investigate digital evidences and to answer questions in relation to previous digital states and events [2]. Indeed, the Internet is one of the main means to attack an organisation. Nowadays, governments and organisations are increasingly reinforcing their reliance on cyber technologies, such as cloud computing, on-line banking and social networks. In tandem, the rate of innovation in new technologies is expanded and organisations are struggling to keep up with the risks of introducing and using new technologies. Cyber activities have provided both a new type of economic crimes and new vectors to facilitate existing economic crimes [3].

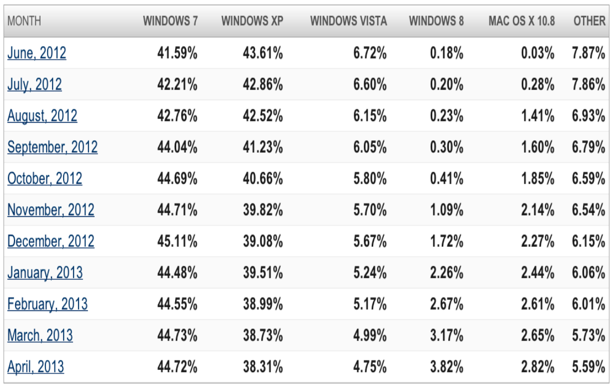
Today, cybercrime has interested governments, business and private citizens for different issues. First of all, governments has faced this issue because it represents a social problem (child trafficking, child pornography, etc.) and, at the same time, a security challenge (espionage, terrorism, etc.). Subsequently, in this specific field, business risk concerns business espionage and therefore financial problems. Finally citizens risk theft identity, frauds and so on. In addition, Symantec (2010) argues that during the 2008-2010 reference period, the threat landscape, once dominated by worms and viruses created by irresponsible hackers, is now ruled by a new type of criminal. The cybercrime is typically a scam that is perpetrated by bogus emails, sent by ”phishers”, which are designed to steal confidential information. Moreover, in the black market, different tools are used for attacks, such as the so-called crime ware programs: bots, Trojan horses, and spyware [4].

In this scenario, computer security and digital forensics analysis are both correct solutions in order to prevent and to search evidences in relation to: data theft, industrial espionage, unauthorized access to computer systems company, damage to information and to answer any potential litigation. All governments and businesses are increasingly being targeted by waves of attacks from criminals and countries, looking for an economic or military benefit. So numerous and advanced are the attacks that many organizations are tackling problematic issues, such as the identification of the greatest risk in terms of threats and vulnerabilities and the allocation of resources in order to stop the most probable and damaging attacks in advanced. In addition, although digital forensics is increasingly becoming important for society and in the scientific debate, the regulations that govern this type of crime are constantly evolving, representing a new field in the legislative scenarios. Moreover, not only does the legislature often fail in dealing with this kind of crimes, but these violations also involve several countries with different legal systems. In this reference context, it is necessary to consider the offences that every citizen commits. They go from tax evasion to on-line banking fraud, terrorist operations, phishing or child pornography , juvenile pornography.

From this conceptual framework, the research work describes a case study of Live Digital Forensics (LDF) on the two most popular operating systems: Windows XP and Windows 7. For the last several months, Microsoft has emphasized the importance of migrating from Windows XP to Windows 7, but even now more than 30 percent of computers are equipped with this OS as showed in fig. 1 [5].

The rest of this paper is organized as follows. The first section discusses what LDF is in order to provide a clear and comprehensive definition of this concept. The second part describes the main differences between Windows XP and Windows 7. The third section presents some tests. Finally, the last part completes the paper through conclusions and future works.

ISBN: 978-1-4673-5256-7/13/$31.00 ©2013 IEEE



MONTH	WINDOWS 7	WINDOWS XP	WINDOWS VISTA	WINDOWS 8	MAC OS X 10.8	OTHER
June, 2012	41.59%	43.61%	6.72%	0.18%	0.03%	7.87%
July, 2012	42.21%	42.86%	6.60%	0.20%	0.28%	7.86%
August, 2012	42.76%	42.52%	6.15%	0.23%	1.41%	6.93%
September, 2012	44.04%	41.23%	6.05%	0.30%	1.60%	6.79%
October, 2012	44.69%	40.66%	5.80%	0.41%	1.85%	6.59%
November, 2012	44.71%	39.82%	5.70%	1.09%	2.14%	6.54%
December, 2012	45.11%	39.08%	5.67%	1.72%	2.27%	6.15%
January, 2013	44.48%	39.51%	5.24%	2.26%	2.44%	6.06%
February, 2013	44.55%	38.99%	5.17%	2.67%	2.61%	6.01%
March, 2013	44.73%	38.73%	4.99%	3.17%	2.65%	5.73%
April, 2013	44.72%	38.31%	4.75%	3.82%	2.82%	5.59%

Fig. 1. Desktop Top Operating System Share Trend (June, 2012 to April, 2013) [5].

II. Live digital forensics

Digital forensics or digital forensic science concerns evidences from any digital device. Digital forensic branches are: computer forensics, forensic data analysis, database forensics, mobile device forensics, network forensics, forensic video and forensic audio. All the discovered evidences should be convincing and sufficiently reliable to stand up in court. This concept is strongly highlighted in the work of Sivaprasad and Jangale [6], where they define digital forensics as the science of locating, extracting and analysing differently types of data from different devices.

Moreover, data have to be interpreted by specialists in order to be used as legal evidence [6]. Digital evidences can be found in computer (hard disks, RAMs or graphics cards RAM), mobile phones, iPods, pen drives, digital cameras, CDs, DVDs, floppies, computer networks, the Internet etc. [7] or they can be hidden in pictures (Steganography), deleted files, formatted hard disks, deleted emails, encrypted files, chat transcripts, password protected files and so on. In a nutshell, digital evidences represent information, stored or transmitted in binary form, that has to be reliable in court. Digital evidences can relate to source code theft, on-line banking frauds, on-line share trading fraud, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling and so on. As a consequence, digital forensics focuses on finding digital evidences after a computer security breach has occurred. It consists in the analysis of information that is contained and created with computer systems and computing devices, typically in the interest of figuring out what happens, when it happens, how it happens and who is involved. Therefore, digital forensics is the process of investigating a computer system to determine the cause of the incident. A calculator or, more in general, a capable digital device for digital investigations could have three distinct roles within the computer crime:

- A computer can be the aim of the crime;
- It can be the means by which you make the crime;
- It can serve as repository storing of information that contains criminal acts.

LDF is the branch that focuses on the analysis of volatile memory. Volatile memory is the work memory and it requires power to maintain the stored information, in other words it needs power to reach the computer memory. Hence the analysis of this memory is extremely sensitive to whatever happens. The idea is to make a dump of a volatile memory for off-line analysis.

An investigator can then build the case through the analysis of the memory dump in an isolated environment that does not alter original evidences. This approach addresses some of the issues to live digital forensics analysis. First of all, this approach limits impact on the compromised system. Secondly, the analysis is repeatable and it is possible to ask new questions later. In addition, off-line volatile memory analysis does not allow to compromise machine on operating system. This enables detection of hidden processes through installation of rootkit or a similar tool [8]. Few years ago, copying memory from an external storage device without modifying the memory's contents was possible thanks to a special pre-installed hardware [9]. Today, different tools for memory analysis are proposed such as FATKit [10], Volatools [11], FACE [12] and bodySnatcher [13].

III. Overview of main differences between Windows XP and Windows 7

Windows XP has represented a crucial point in the successful period of economic and technological expansion of Windows. After Windows XP, different operating systems have alternated in the international scenario such as Windows Vista and most recently Windows 7 and Windows 8. Each operating system is unique in its own way. Windows XP was released the 31 of December of 2001. In May 2012, XP still had a 44.26% share of the entire operating system market [14] whereas in April 2013 XP had 38.31 % and 7 44.72% [15]. Many users think that Windows XP is still sufficient for their needs and they do not understand the value of upgrading at this time. However, Windows 7 is four to five times less vulnerable to malware infections than Windows XP [16]. Overall, as the fig. 2 shows, the study has emphasized how the more recent Microsoft operating systems, which have the latest service packs, have a lower infection rates in relation to the older ones. Indeed, Windows 7 and Windows Server 2008 R2 have the highest marks for security [16]. On the other hand, XP still has an important slice of trade and for this reason Microsoft is going to continue supporting it until April 2014, while XP can no longer be purchased.

In relation to XP, Microsoft has introduced many new features and improvements. Some of these are improvements in security and overall performance, other ameliorations are connected with better compatibility with other programs. However, despite these improvements, different reasons should make upgrading to Window 7 tempting. First of all, Microsoft Windows 7 aims at accommodating the new emerging trends, such as the constant development of hardware (monitor touch,

ISBN: 978-1-4673-5256-7/13/$31.00 ©2013 IEEE

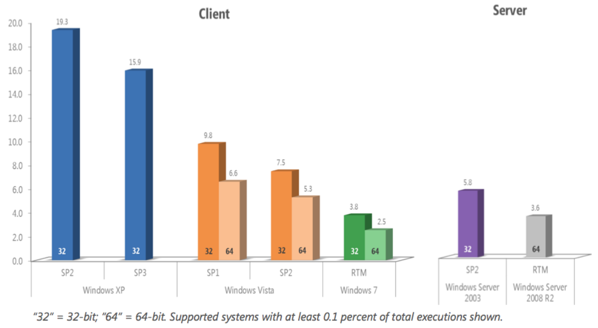


Fig. 2. Average quarterly infection rate (CCM) by operating system and service pack in 2010 [16].

spread of 64-bit processors, solid state drives, multicore processors, etc..), the increasing popularity of mobile computing devices (Netbook, Tablet, Smart Phone), the use of home networks and the deployment of Media Center. Logically, all these functionalities need higher minimum requirements. Indeed for 7 it is necessary:

- at least a 1Ghz 32 bit processor;
- 1 GB of RAM (32-bit version) or 2GB of RAM (64-bit version);
- 16 GB of Hard Drive (32-bit version) or 20 GB (64-bit version).

Overall, Windows 7 is faster than Windows XP. Networking computers together is easier and more streamlined than in XP or Vista. Moreover, in Windows 7 the upload and download speeds for data are improved. This includes increased speeds for browsing the internet and downloading files. XP has never been known for having good security. Indeed, User Account Control (UAC) has been introduced with Vista and later it has been kept in Windows 7 but with additional controls and improved functionalities. UAC is simply a security feature that helps to block viruses and malware. Although, it is not infallible, it certainly limits the damages that certain types of malware can do to PC. In addition, even if XP performs well, playing computer games in Windows 7 takes gaming to a new level. Microsofts Direct X 10 technology offers better graphics and sound. Additionally, it provides better performance even with a mid-range PC.

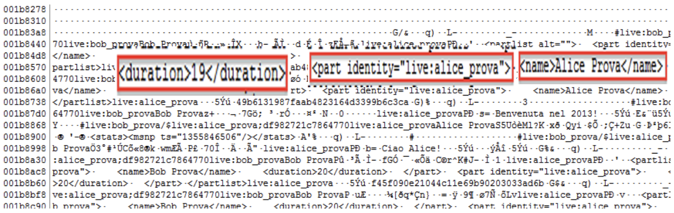
However, in order to ease the transition to Windows 7, Microsoft has included what it is well-known as XP Mode. This feature is available with the Professional, Enterprise, and Ultimate versions of Windows 7. XP Mode is a way of installing and running programs that are not compatible with 7. It is a great, cost effective tool that can allow you to go on and back between XP and 7. In addition, Microsoft is also suggesting that organizations can save money by moving from Windows XP to Windows 7 [17]. Microsoft clearly wants to wrest the venerable 10-year-old Windows XP from the grip of organizations that have depended on it. Windows XP has been embraced by the commercial world in a surprising way. IDC's report, "Mitigating Risk: Why Sticking With Windows XP Is a Bad Idea," [17] is a financial analysis based on interviews with nine "large" organizations (an average of 3,680 employees). The study quantified the costs associated with staying on Windows XP, including lost user productivity time, as well as IT support and help desk costs. On the other hand, the study does not analyse an important and fundamental factor that is represented by the costs associated with updating applications to run on Windows 7. Of course, security should be a principal concern for those organizations that still use Windows XP. Indeed, the OS is going to lose security-patch support by April 8, 2014 in accordance with Microsoft's product life cycle schedule. Windows XP is moving out of its "extended support" phase, which means "the end of security updates, (paid) hot fix agreement support, and per-incident support services," according to IDC's report [17]. An alternative option for organizations might be to pay Microsoft for "custom support," but this can be an expensive option. According to IDC study,it estimated that the annual cost for organizations to maintain a Windows XP-based PC is $870. The same cost for a Windows 7-based PC is $168, as a consequence, organizations potentially can save about $701 per PC per year by moving to Microsoft's newer OS, according to the report. The report breaks down Windows XP user productivity costs into six categories, including time lost to malware, time taken to reimage a PC, reboot waits, downtime and time waiting for help desk support. Reboots and malware constitute the top two productivity time drainers among users. Finally according to the report "Moving to Windows 7 will reduce the time invested in patch management by 82%," [17].

IV. The case study

The research analysis has been conducted in different virtual machines. First of all, it is necessary to explain the configuration of the host systems and secondly the configuration of the virtual machines. The host system configuration is a MacBook Pro 15-inch, late 2008 with OS X Lion 10.7.5 equipped with:

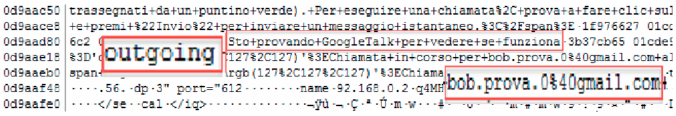
- Processor: 2.93 GHz Intel Core 2 Duo;
- Memory (RAM): 8GB of RAM;
- Graphics: NVIDIA GeForce 9400M 256MB.

The virtualization system is VMware Fusion Professional 5.0.3. Two different virtual machines are used to run tests. The first is equipped as follows: Windows XP Professional service pack 2 with 512 MB and 15 GB of HD, while the second is equipped with Windows 7 Professional 32 bit with 1 GB of RAM and 15 GB of HD. In both systems, the following software are installed: Skype 6.0.0.126, Google Talk 3.7.1.9330, Internet Explorer 8.0.7600.16385 (IE). Moreover, the following accounts are created to make the use of these software possible: two Facebook accounts (Alice Prova, Bob Prova), two Hotmail accounts (alice_prova@hotmail.com, bob_prova@hotmail.com), two Gmail accounts (alice.prova.0gmail.com, bob.prova.0gmail.com), one Yahoo account (alice_prova@yahoo.it). Google Talk needs the use of the Gmail account, while Skype requires the use of Hotmail account. Indeed, Windows Live Messenger accounts are switched into Skype account in April 2013. The tests are divided into steps, that are:



```
001b8278 ···························································································
001b8310 ···························································································
001b83a8 ···········································G/&···q)··L-··········_-·············M····#live:bob_
001b8440 70live:bob_provaBob_Provai·õR··»·ÎX···b-·ÃÌ··d·É·Î·zEÅ·ã·'live:alice_provaPÐ··'···<partlist alt="">·  <part identity=
001b84d8 </name>·                                    >·
001b8570 partlist>li <duration>19</duration> ab4 <part identity="live:alice_prova"> <name>Alice Prova</name>
001b8608 4770live:bob                         øó·l
001b86a0 va</name>·                           rt>·   <part identity="live:alice_prova">·    <name>Alice Prova</name>·
001b8738 </partlist>live:alice_prova···5Ýú·49b6131987faab4823164d3399b6c3ca·G)$···q)··L-·········3··················#live:bo
001b87d0 64770live:bob_provaBob Provaz+···¬·7Gö; ³·rÓ···¤²·N··0······live:alice_provaPÐ·s=·Benvenuta nel 2013!···5Ýú·E&¨ü5Ýu
001b8868 Y····#live:bob_prova/$live:alice_prova;df982721c7864770live:alice_provaAlice ProvaS5UòèMl?K·xð·Qyi·$Õ·;Ç+Zu·G·Þ²þ6
001b8900 ·® '-®·<stats><msnp ts="1355846506"/></stats>·A'$···q)··L-·········#···················#live:bob_prova/$live:alice_
001b8998 b ProvaÖ3°#¹ÚCõ«8®k·wmÆÃ·P£·70Î··Ä··Ã"·live:alice_provaPÐ·b=·Ciao Alice!···5Ýú···ýÅî·5Ýú··G$&···q)··L-·········_-·
001b8a30 :alice_prova;df982721c7864770live:bob_provaBob ProvaPû·³Ã·Ì-·fGÓ·¯·«Õä·C®r^K#J-·Ì·1·live:alice_provaPÐ··'··<partlis
001b8ac8 prova">·    <name>Bob Prova</name>·    <duration>20</duration>·  </part>·  <part identity="live:alice_prova">·
001b8b60 >20</duration>·  </part>·</partlist>live:alice_prova···5Ýú·f45f090e21044c11e69b90203033ad6b·G$&···q)··L-·········_-
001b8bf8 ve:alice_prova;df982721c7864770live:bob_provaBob ProvaP·uÆ····¼[ðq*Çn}··=·ÿ·9¶·ø7Ñ·õLvlive:alice_provaPÐ·v···<part
001b8c90 b prova">·    <name>Bob Prova</name>·    <duration>20</duration>·  </part>·  <part identity="live:alice prova">·
```

Fig. 3. Dump RAM: Skype focus.



```
0d9aac50 trassegnati+da+un+puntino+verde).+Per+eseguire+una+chiamata%2C+prova+a+fare+clic+sul
0d9aace8 +e+premi+%22Invio%22+per+inviare+un+messaggio+istantaneo.%3C%2Fspan%3E·1f976627 01cc
0d9aad80 6c2 outgoing Sto+provando+GoogleTalk+per+vedere+se+funziona·3b37cb65 01cde
0d9aae18 %3D'                127%2C127)'%3EChiamata+in+corso+per+bob.prova.0%40gmail.com+al
0d9aaeb0 span+               rgb(127%2C127%2C127)'%3EChiama bob.prova.0%40gmail.com
0d9aaf48 ····.56.·dp·3" port="612········name·92.168.0.2·q4MH
0d9aafe0 ····</se··cal·</iq>··············¬ÿù·¬·Ç·ª·Ú·m·w···#
```

Fig. 4. Dump RAM: Google Talk focus.

- Starting up the virtual machine;
- Use of the analysed service;
- Acquisition of the dump;
- Dump analysis.

The software FTK Imager is used to do the acquisition. FTK Imager is present, by default, on the live CD of DEFT. The Dump is saved in a external drive, connected by the USB.

A. *Skype*

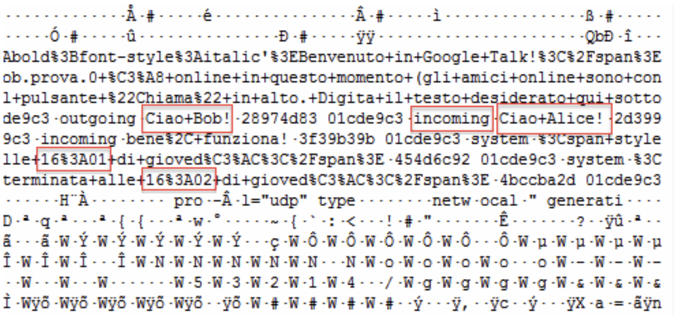
After the starting up, in each virtual machine Skype runs. As a consequence, it is logged with alice_prova and it is added Bob's account (bob_prova). After that bob_prova is showed in contact list, first of all a chat starts and then a skype call, secondly Alice signs out from the Skype. Nothing about the history of skype account will be saved because it is setted. The fourth step is showed in the fig. 3, where through the dump analysis it is possible to find information about the chat, the source's account and destination's account. Therefore, by the RAM's dump it is possible to find all the communications of Skype activities.

B. *Google Talk*

After the preliminary operation of starting up (run VM and run Google Talk), from the account alice_prova.0@gmail.com it is added bob_prova.0@gmail.com. After the presence of bob_prova.0@gmail.com on the list of contacts, a chat starts and after this a call of few seconds. From the analysis, it is possible to find evidences in relation to both actions. First of all, it has been recovered the entire chat conversation and information about the start date and end date of the conversation. However, the two considered operating systems do not show significant differences. In the pictures 4 and 5 some frames of chat and the date of the start and of the end of a brief conversation are highlighted.

C. *Internet Explorer*

IE is tested on Facebook, Gmail, hotmail and Yahoo. The choice of this browser is related to the fact that it is the more used browser in the web. The fig. 6 [18] proves this thesis. For each of the virtual machines, Windows XP and Windows 7, the browser applications have been verified using the portals Facebook, Yahoo, Hotmail and Gmail, which are some of the most used in the world. The tests are made using Internet Explorer in two ways: normal mode and private mode. The second does not record your browsing history, and, at least in theory, it should not leave traces on your computer, in the form of cookies, when you close the window or Tab[1].



```
··············Å·#·····é················Â·#·····ì·················ß·#·····
·····Ó·#·····û················Ð·#·····ÿÿ·······················QbÐ·î···
Abold%3Bfont-style%3Aitalic'%3EBenvenuto+in+Google+Talk!%3C%2Fspan%3E
ob.prova.0+%C3%A8+online+in+questo+momento+(gli+amici+online+sono+con
l+pulsante+%22Chiama%22+in+alto.+Digita+il+testo+desiderato+qui+sotto
de9c3·outgoing·Ciao+Bob!·28974d83 01cde9c3·incoming·Ciao+Alice!·2d399
9c3·incoming·bene%2C+funziona!·3f39b39b 01cde9c3·system·%3Cspan+style
lle+16%3A01+di+gioved%C3%AC%3C%2Fspan%3E·454d6c92 01cde9c3·system·%3C
terminata+alle+16%3A02+di+gioved%C3%AC%3C%2Fspan%3E·4bccba2d 01cde9c3
······H¨À·········pro·-Â·l="udp" type·········netw·ocal·" generati····
D·ª·q·ª···ª·{·{···ª·w·°·····~·{·`·:·<···!·#·"·······Ê········?··ÿû·ª··
ã···ã·W·Ý·W·Ý·W·Ý·W·Ý·W·Ý···ç·W·Ô·W·Ô·W·Ô·W·Ô·W·Ô···Ô·W·µ·W·µ·W·µ·W·µ
Î·W·Î·W·Î···Î·W·N·W·N·W·N·W·N·W·N···N·W·o·W·o·W·o·W·o···o·W·–·W·–·W·–
··W···W···W·······W·5·W·3·W·2·W·1·W·4···/·W·g·W·g·W·g·W·g·W·&·W·&·W·&
Ì·Wÿõ·Wÿõ·Wÿõ·Wÿõ·Wÿõ··ÿõ·W·#·W·#·W·#·W·#··ý···ÿ,··ÿc··ý···ÿX·a·=·ãÿn
```

Fig. 5. Dump RAM: Google Talk focus.

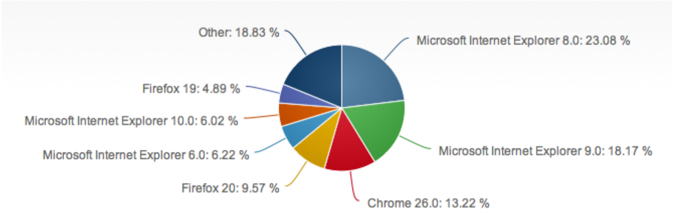


Fig. 6. Desktop top browser share trend [18].

The scenario for each sub-section is the same. For each VM, first of all, after that the system is ready, Internet Explorer runs. By default, IE opens www.google.it web page, the correct url is typed and logged to web portal with alice_prova account. In the case of tests in private mode, after IE runs it is necessary to start the private mode and to type the correct url. Dump of RAM is done for each single test. When the browser is opened, it is necessary to logout first and then to do the dump.

1) Facebook: The Facebook tests focus on the chat activities. After that alice_prova is logged, bob_prova account is added to the list of friends and after the friend acceptance, a chat starts. The chat lasts for 5 minutes. The tests are split in chat with browser in normal mode an private mode and, as a result, the RAM dump is done in the two cases: closed and opened browser. However, in those cases the logout is always done. As it can be seen on the table I and II, there is only one different result between XP and 7. This concerns the case in which the browser works in normal mode and when the browser is opened during the dump. Logically, the logout from Facebook is guaranteed. In this specific case on the Windows XP, it is possible to find the no encrypted account's

[1] In the area of graphical user interfaces (GUI), a tabbed document interface (TDI) or a Tab is one that allows multiple documents to be contained within a single window, using tabs as a navigational widget for switching between sets of documents. It is an interface style most commonly associated with web browsers, web applications, text editors, and preference panes.

password; whereas on Windows 7 the password is not present in the dump. The research keywords used on the dump are: *Facebook*, *_prova*, *alice*, *bob*.

2) Yahoo,Hotmail and gmail: The Yahoo and Hotmail tests focus on the mail activities. The results are identical, therefore they are analysed in the same section. The scenario of tests is login on the web mail with the browser in normal or private mode at the url https://login.yahoo.com for Yahoo and https://login.live.com/ for Hotmail. After that an email is composed, it is sent from the alice_prova@yahoo.it or alice_prova@hotmail.it to bob_prova@hotmail.it. Finally, logout from the web mail and the RAM dump can start. The same operation is repeated changing surfing mode (normal or private) or operating system. However in these cases, there are not differences in relation to the variables: OS, browser in private o normal mode and browser open or close during dump. The research keywords used on the dump are: *%40hotmail.it*, *hotmail.it*, *_prova*, *alice*, *bob*, *%40gmail.it*, *gmail.it*, *%40yahoo.it*.

D. Summarized of Internet Explorer tests

The table I summarizes the Internet Explorer tests on Windows XP, whereas the table II sums up the tests on Window 7.

As the tables show, there is not significant difference; however some details are evident. First of all, in the first row of both tables, it is possible recognize a dissonance in relation to Yahoo and Hotmail. Indeed, in XP it is possible discover sender and recipient that are not feasible in 7. Looking the second row, when the browser is opened, there is only one but extremely important difference. It can be viewed the account's password decrypted as well as the chat. In the third row, the email recipient is identifiable on XP and in relation to Yahoo and Hotmail, meanwhile in the other cases it is not possible. Finally in the last row, still in Yahoo and Hotmail web site, there is a difference. This is the only case in which Windows 7 provides more information than XP. Indeed, the sender's user-name can be discovered.

TABLE I
SUMMARIZED OF INTERNET EXPLORER TESTS ON WINDOWS XP

Type of surfing	**Dump with browser closed/ opened**	**Facebook (Chat)**	**Yahoo (Mail)**	**Hotmail (Mail)**	**Gmail (Mail)**
Normal mode	Closed	User-name (sender and recipient) and chat's body	User-name (sender and recipient) , subject and email's body	User-name (sender and recipient), subject and email's body	User-name of sender, sender, recipient, subject and email's body
Normal mode	Opened	User-name (sender and recipient), account's password not encrypted and chat	User-name (sender and recipient), subject and email's body	User-name (sender and recipient), subject and email's body	User-name of sender, sender, recipient, subject and email's body
In Private Browsing	Closed	Nothing	User-name (sender and recipient), Subject and email's body	User-name (sender and recipient), Subject and email's body	User-name of sender, sender, recipient, subject and email's body
In Private Browsing	Opened	User-name (sender and recipient) and chat's body	Subject and email's body	Subject and email's body	User-name of sender, sender, recipient, subject and email's body

V. CONCLUSIONS AND FUTURE WORKS

The aim of this work has been to find differences in Live Digital Forensics between Windows XP and Windows 7 in a few, but extremely permeated, software. The research shows as there is not importance differences between Windows XP and Windows 7 during live forensic analysis. The only one is due to the use of Facebook. Indeed using Facebook by IE in normal mode and leaving the browser opened, though logout is done, in Windows XP it is possible to find the not encrypted password, whereas in Windows 7 the password cannot be found. Probably Microsoft does not implement any function to remove evidences from the RAM, and this task could be implemented by each installed software. Certainly, this is good in relation to the investigation of police, but the private and public organizations probably do not appreciate any unauthorized access at the own machine. However, the dump analyses are simplified because the content of research has been known. In general, the work of a computer forensics investigator can be very stressful because although different information are available, only some of them are useful for investigation. From this research, it is possible to notice as Facebook use *email=user-name&pass=password*, therefore they can be used in general as keywords, whereas *[”msg”:”text”* is always present for the message parts. In Skype there is always *part identity=*, *name* or *duration*, the first and the second are always followed by information about account of sender or recipient, while the third is followed by the seconds of call if the evidence is a call and not a chat. Using Google Talk *incoming* and *outcoming* mean respectively an input to the sender and a message sent by the sender. In this work, the analysis on the two common Operating System of Microsoft, Windows Xp and Windows 7 has been presented. In the future, it is scheduled to complete the analysis with Widows 8, which represents the new Operating System. This possible implementation is not the only. Indeed, forensics analysis is extremely interested in knowing dissimilarities among different browser. Indeed, smart

TABLE II
SUMMARIZED OF INTERNET EXPLORER TEST ON WINDOWS 7

Type of surfing	**Dump with browser closed/opened**	**Facebook (Chat)**	**Yahoo (Mail)**	**Hotmail (Mail)**	**Gmail (Mail)**
Normal mode	Closed	Username (sender and recipient) and chat's body	Subject and email's body	Subject and email's body	Username of sender, sender, recipient, subject and email's body
Normal mode	Opened	Username (sender and recipient) and chat's body	Username of sender, sender, recipient, subject and email's body	Username of sender, sender, recipient, subject and email's body	Username of sender, sender, recipient, subject and email's body
In Private Browsing	Closed	Nothing	Username (sender), Subject and email's body	Username (sender), Subject and email's body	Username of sender, sender, recipient, subject and email's body
In Private Browsing	Opened	Username (sender and recipient) and chat's body	Username (sender), Subject and email's body	Username (sender), Subject and email's body	Username of sender, sender, recipient, subject and email's body

users unlikely use IE, but they usually use Chrome or Firefox. From this viewpoint, the work will evolve through Windows 8 and other browsers in order to complete the scenario on Windows. Moreover, the study could be completed through the correlations with other operating systems such as Mac OS X and the common Linux distribution (Ubuntu, Red Hat).

REFERENCES

[1] M. Caloyannides, "Forensics is so "yesterday"," *Security Privacy, IEEE*, vol. 7, no. 2, pp. 18–25, 2009.

[2] B. Carrier, "Digital forensics works," *Security Privacy, IEEE*, vol. 7, no. 2, pp. 26–29, 2009.

[3] K. Cheater and D. Harley, "Cybercrime: Out of obscurity and into reality," 6th PwC Global Economic Crime Survey, Tech. Rep., March 2012.

[4] M. Merritt, "Cybercrime exposed," http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/norton_cybercrime_exposed_booklet.pdf, 2010, [Online; accessed 04-March-2013].

[5] "Desktop top operating system share trend," http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=11qpcustomb=0, [Online; accessed 04-May-2013].

[6] A. Sivaprasad and S. Jangale, "A complete study on tools amp; techniques for digital forensic analysis," in *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, 2012, pp. 881–886.

[7] J. R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*. Charles River Media, 2005.

[8] C. Waits and J. A. et al, "Computer forensics: Results of live response inquiry vs. memory image analysis," CERT, Tech. Rep., 2008.

[9] B. D. Carrier and J. Grand, "A hardware-based memory acquisition procedure for digital investigations," *Digital Investigation*, vol. 1, no. 1, pp. 50 – 60, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287603000021

[10] N. L. P. Jr., A. Walters, T. Fraser, and W. A. Arbaugh, "Fatkit: A framework for the extraction and analysis of digital forensic data from volatile system memory," *Digital Investigation*, vol. 3, no. 4, pp. 197 – 210, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287606001228

[11] A. Walters and N. P. Jr, *Volatools: integrating volatile memory forensics into the digital investigation process*. Black Hat DC, 2007.

[12] A. Case, A. Cristina, L. Marziale, G. G. Richard, and V. Roussev, "Face: Automated digital evidence discovery and correlation," *Digital Investigation*, vol. 5, Supplement, no. 0, pp. S65 – S75, 2008, ¡ce:title¿The Proceedings of the Eighth Annual {DFRWS} Conference¡/ce:title¿. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287608000340

[13] B. Schatz, "BodySnatcher: Towards reliable volatile memory acquisition by software," *Digital Investigation*, vol. 4, pp. 126–134, Sep. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.diin.2007.06.009

[14] "Desktop operating system market share may, 2012 to june, 2012," http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10qpcustomd=0qpsp=160qpnp=2qptimeframe=M, [Online; accessed 01-May-2013].

[15] "Desktop operating system market share april, 2013," http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10qpcustomd=0qpsp=171qpnp=1qptimeframe=M, [Online; accessed 01-May-2013].

[16] J. F. e. a. Doug Cavit, "Microsoft security intelligence report," Microsoft, Tech. Rep., 2010.

[17] N. S. Al Gillen, Randy Perry, "Mitigating risk: Why sticking with windows xp is a bad idea," http://www.microsoft.com/en-us/download/details.aspx?id=29883, Microsoft, Tech. Rep., 2012, [Online; accessed 01-03-2013].

[18] "Desktop browser version market share april, 2013," http://marketshare.hitslink.com/browser-market-share.aspx?qprid=2qpcustomd=0, [Online; accessed 01-May-2013].