Agnieszka Cieplak[1], Mirosław Malec[2], Tomasz Cieplak[3]

THE ANALYSIS OF HARDWARE OPTIMIZATION METHODS FOR IMPROVING CAPABILITIES AND PERFORMANCE OF X-WAYS FORENSICS TOOLSET

Abstract. In this paper an attempt was made to identify optimal hardware configuration for a workstation designated to computer forensics expert, using X-Ways Forensics software. To achieve this objective a body of research data on different hardware setups was collected as a result of their performance examination while conducting diverse tasks during test simulations. With the complete research data, it was possible to determine the most optimal hardware configuration from all the setups prepared for the test.

Keywords: computer forensics, test simulations, hardware configuration.

INTRODUCTION

Computer Forensics is the branch of science dedicated to localizing, extracting, analysing and securing digital evidence in computer environment. It defines norms of correct forensic conduct and practice, combining the law with the tenets of computer technology. Naturally, it is closely interconnected with the position of Computer Forensics Investigator, who much like Criminal Investigator, is responsible for the entire investigation, starting from evidence recovery, through report, conclusions and presentation in the court. Computer Forensics Investigator must have knowledge and expertise to identify criminal activity within computer system and prepare the documentation necessary for court proceedings. For that purpose he should have access to an appropriate toolsets and software. Forensic experts have two groups of software to choose from – commercial and created in accordance with open source license. Among the commercial software the following enjoy greatest reputation: EnCase, FTK, X-Ways Forensics, Helix Pro, Nuix Desktop. On the other hand, to the category of the best open source products belong: pakiet TCT, SleuthKit + Autopsy, ProDiscover Basic, Deft/Caine and SIFT Workstation.

One undeniable advantage of open source tools is non-existent price tag. In contrast, commercial toolsets have producer's warranty, technical support and are characterise by overall better functionality.

[1] Specjalistka d/s informatyki śledczej, ASSECCO Lublin, e-mail: info@assecobs.pl

[2] Katedra Podstaw Techniki, Politechnika Lubelska, e-mail: m.malec@pollub.pl

[3] Katedra Organizacji Przedsiębiorstwa, Politechnika Lubelska, e-mail: t.cieplak@pollub.pl

Of these the most commonly used are: EnCase, FTK and X-Ways Forensics. Each of these applications has different features and strengths. For example, ExCase proves to be perfect solution in corporative environments for remote analysis of servers and workstations, whereas X-Ways Forensics excels at file examination. The choice of software often depends on price and investigator's area of expertise. When considering general reputation, X-Ways Forensics proves to be one of the most highly esteemed toolsets in its category. Due to reasonable balance between capabilities and its cost, it is very popular among Computer Forensics Investigators throughout the world. For this reason it was selected from among others and became the subject of this research.

X-WAYS FORENSICS AND ITS FUNCTIONALITY

X-Ways Forensics is an advance workflow environment for experts in Computer Forensics, and the flagship product of X-Ways Software Technology AG. This piece of software is used by American and German governmental agencies, Australian Department of Defence, technical universities in Vienna and Munich, and even private business, such as Microsoft, Hewlett Packard, Deloitte & Touche and Ernst & Young. The programme is closely integrated with WinHex disk editor (the forensics capabilities are available are available in the most advanced version of this software). Both WinHex and X-Ways Forensics feature the same base code. Launching WinHex editor with forensic license is the same as running X-Ways Forensics toolset, with just a few exceptions:

- the name of the software visible in the user interface varies;
- the WinHex executable is available to X-Ways Forensics users as a separate application to download;
- in X-Ways Forensics all kinds of operations on disks, virtual memory and physical memory are carried out in „read-only" mode. This is in order to ensure compliance with investigation procedures, which do not permit any changes in the content of secured evidence. In some cases disconnected from investigation procedures, one can take advantage of WinHex, which allows editing disk selectors or wiping clean its contents, its freespace and slackspace (the remains of files).

Here are the most significant features of X-Ways Forensics software:

- cloning disks and creating disk images;
- ability to read the inner structure of files in RAW (.dd), ISO and VHD images;
- full access to disks, matrix RAID, and disk images larger than 2TB (more than 232 sectors) whose single sector is bigger than 4KB;
- built-in capability to analyse matrix RAID type 0 and 5 and dynamic disks;
- active support for FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, CDFS/ISO9660/Joliet, UDF filesystems;

- ability to browse and clone the contents of RAM and virtual memory of running processes;
- a range of data recovery techniques;
- a data base of files headers, written in GREP elastic format;
- capacity to identify and obtain access to alternative datastreams in NTFS files;
- multiscale callculation of file checksums (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD, ...);
- the capacity for parallel, physical and logical keyword search;
- recursive view on all existing and deleted files in all subfolders;
- ability to create and read EnCase software disk images (*.e01*) with encoding capabilities (256 bit AES);
- automatic registration of all conducted activities (logging-in);
- security measures against data overwrite to ensure its authenticity;
- remote disk analysis in the network;
- Additional support for the following filesystems: HFS, HFS + / HFSJ / HFSX, ReiserFS, Reiser4, and many variants of UFS1 and UFS2;
- gallery view for image files, and Calendar view for all other data;
- File preview (using integrated component) for over 270 types of files;
- capabilities to analyze e-mail content recovered from Outlook (PST, OST), Outlook Express (DBX), Mozilla (including Netscape and Thunderbird), AOL PFC, mailbox (mbox, Berkeley, BSD, Unix), Eudora, PocoMail, Barca, Opera, Forte Agent, The Bat!, Pegasus, PMMail, FoxMail, maildir folders (local copies);
- Authomatic verification of file type by its signature and with the use of dedicated algorithms.
- ability to create own sets of file checksums.
- dynamic filters used to group data by file type, checksum sets, date of authentication/access/modification, size, comments etc.,
- ability to create report;
- ability to copy files from examined image or disk and preserve its directory path.
- automatic localization of image content in document files (for example in MS Office formats, PDFs etc.).
- ability to extract images from video files in the intervals set by the user;
- in-built component which allows examination of Windows register system files;
- elastic indexing algorithm;
- searching and indexing in Unicode standard and multiple other code pages at the same time.

RESEARCH BACKGROUND AND HARDWARE CONFIGURATION

As mentioned before the main objective of this research is to determine optimal hardware configuration for the range of the most common procedures in forensics investigation. The research involves a number of sampling tests on different hardware builds, in the course of which a number of factors were measured: the time required to complete the task as well as CPU and memory workload. The recorded data were used as the basis of selecting the most efficient solution. The research was conducted on 7 hardware configurations. In each case the task was executed on two prepared carriers: a hard drive and the image of USB flash drive. The producer of X-Ways Forensics software does not specify its minimal system requirements. This is due to the character of Forensics Investigator's work, who often finds himself working on diverse hardware configurations. Therefore, a common household computer set was selected for the minimal configuration. Apart from that, four laboratory class computers in seven different hardware builds were used in this research. Table 1 highlights the details.

Preparing workstations

Prior to commencing the actual research, each workstation was fit with SATA disk, as listed in table 1. Moreover, Microsoft Windows 7 Enterprise x64 was installed on each machine (with the exception of PC-1 where the research team installed x86 version of the OS). The OS was updated and retrofitted with Polish language pack. Next, the researchers installed, launched and patched trial version of Kaspersky Anti-Virus 9 software. The team also run AnalogXCapture application – which was used to make screenshots in order to document the achieved results. Furthermore, Process Explorer application was used on each machine so as to analyze the workload of the OS. Lastly, the researchers installed X-Ways Forensics 15.6 SR-10 software and applied xw_viewer component with it.

Preparing the test hard drive

The test hard drive was to emulate the real criminal evidence. A 40 GB (38164 KB) Seagate ST340014AS 7200.7 drive was selected for this purpose. The drive was wiped clean with HDD Erase 4.0. software. Next, using Computer Management tool (native to Windows 7) and parted application run from Ubuntu Linux Live CD two separate partitions were created: the first – 33 GB large with NTFS file system; and the second – EXT2 with the total free space of 5 GB. The NTFS partition drive became the host to Windows 7 Enterprise. Both partitions were partially filled with data (document, audio and video files). At this point, both partitions were removed with Computer Managment tool – two new ones were created in their place: an NTFS drive with 20GB of total size and another NTFS partition with 17 GB of initial space. Both of them were separated from each other by unformated space of 1 GB. Finally, Windows 7 Enterprise system was copied to the 20 GB partition.

RESEARCH PROGRESS

Each stage of the research was conducted with X-Ways Forensics software, following exactly the same procedure:

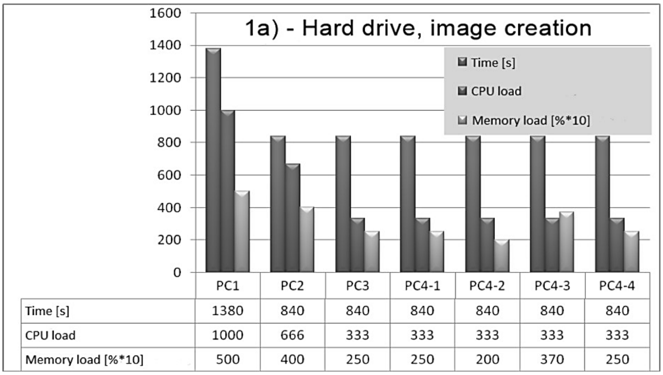
1. Test drive examination:
   - connecting the drive to laboratory machine with Tableau Seata Forensic Bridge blocker.
   - making a binary copy of the tested drive using X-Ways Forensics and moving its copy to the system drive.
   - creating the image of the copy volume.
   - calculating md5 checksums for all the files in the image.
   - creating index and its optimization using 3/4 of available RAM.
2. Examining tested Flash drive image:
   - creating an image of the volume (sector boundaries search).
   - calculating md5 checksums for all the files in the image.
   - creating index and its optimization using 3/4 of available RAM.
   - creating an image of the volume (byte-level search).
   - creating index and its optimization using 3/4 of available RAM.

Table 1. The listing of individual workstations

	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Mother board	Asus P5L-MX	Asus M4A78-EM	Asus P5Q SE	Asus M4A88TD-V Evo/USB3	Asus M4A88TD-V Evo/USB3	Asus M4A88TD-V Evo/USB3	Asus M4A88TD-V Evo/USB3
CPU	Intel Celeron D 336	DualCore AMD Phenom II X2 Black Edition 550	Intel(R) Core(TM)2 Duo E7400	AMD Phenom(tm) II X6 1055T	AMD Phenom(tm) II X6 1055T	AMD Phenom(tm) II X6 1055T	AMD Phenom(tm) II X6 1055T
Number of cores	1	2	2	6	6	6	6
CPU clock	2800 MHz	3100 MHz	3150 MHz	2800 MHz	2800 MHz	2800 MHz	2800 MHz
RAM (in GB)	1 GB	4 GB DDR2	4GB DDR2	8GB DDR3	6GB DDR3	4GB DDR3	8GB DDR3
RAM clock speed	800 MHz	800 MHz	800 MHz	1600 MHz	1600 MHz	1600 MHz	1600 MHz
Hard drive	Seagate ST380811AS (80 GB, 7200 RPM)	WDC WD10EALS-00Z8A0 (931 GB, 7200 RPM, SATA), WDC WD800JD-23LSA0 (80GB, 7200 RPM)	Seagate ST3750528AS (698 GB, 7200 RPM)	2 connected RAID0 drives: WD1002FAEX (1 TB, 7200 RPM)	2 connected RAID0 drives: WD1002FAEX (1 TB, 7200 RPM)	2 connected RAID0 drives: WD1002FAEX (1 TB, 7200 RPM)	Seagate ST380811AS (80 GB, 7200 RPM)

RESEARCH DATA AND ITS ANALYSIS

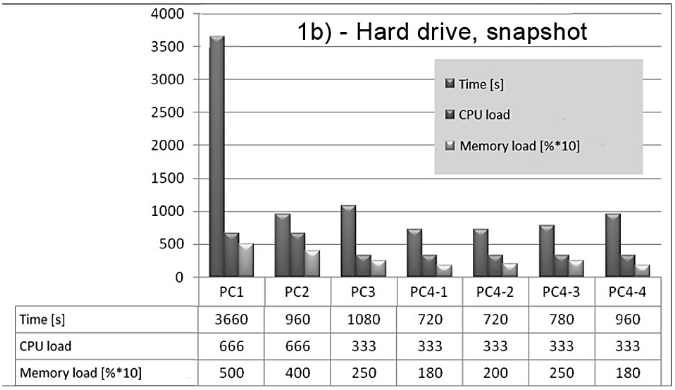
The research procedures were carried out on all workstations which are listed in table 1. During its proceedings the time required to complete the tasks as well as CPU and RAM workload were closely followed. The results of the research are presented in the following data charts. Each chart refers to individual stage of the research.



	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]	1380	840	840	840	840	840	840
CPU load	1000	666	333	333	333	333	333
Memory load [%*10]	500	400	250	250	200	370	250

Fig. 1. Test hard drive examination – creating disk image

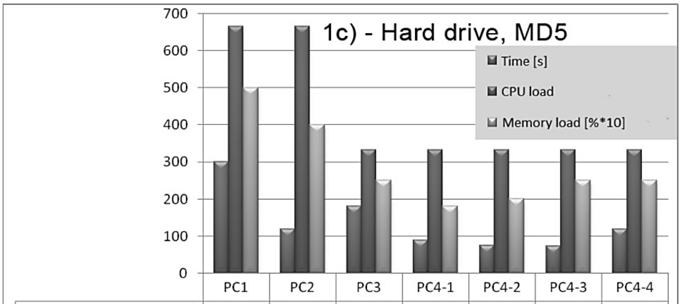
As Figure 1 shows, the process of creating the drive image takes equal amount of time on all tested machines, except for PC1.



	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]	3660	960	1080	720	720	780	960
CPU load	666	666	333	333	333	333	333
Memory load [%*10]	500	400	250	180	200	250	180

Fig. 2. Test hard drive examination – creating disk image

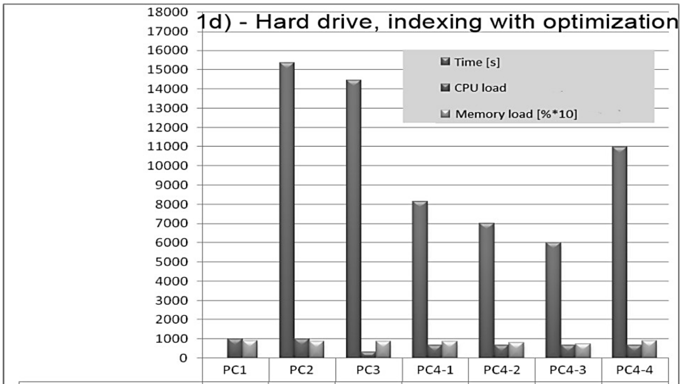
Figure 2 indicates that taking hard drive snapshot take much more time on PC1 in comparison with other machines. It's worth noting that both CPU and memory stress are the lowest on PC4 configuration. In spite of having more RAM at the disposal it takes more time to complete the task on PC4-4 build than on PC4-2 and PC4-3 configurations.



	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]	300	120	180	90	75	74	120
CPU load	666	666	333	333	333	333	333
Memory load [%*10]	500	400	250	180	200	250	250

Fig. 3. Hard drive examination, calculating md5

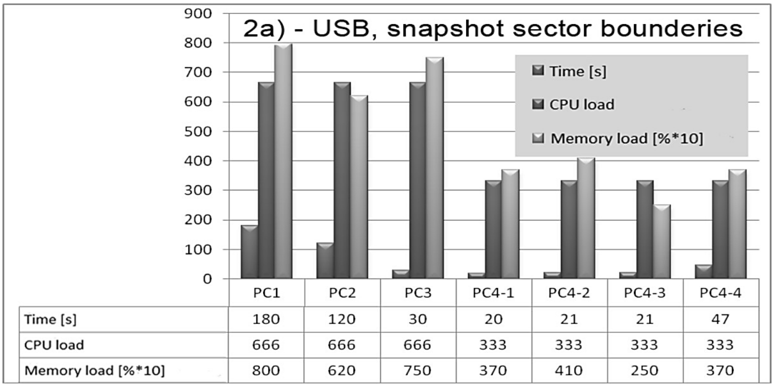
Figure 3 shows that the process of calculating checksums overburdens neither memory nor CPU. The procedure requires more time on PC1 and PC3 setups. The time discrepancy on other builds is negligible.



	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]		15360	14460	8160	7020	6000	10980
CPU load	1000	1000	333	666	666	666	666
Memory load [%*10]	900	870	870	870	800	750	900

Fig. 4. Hard drive examination – indexing with optimization

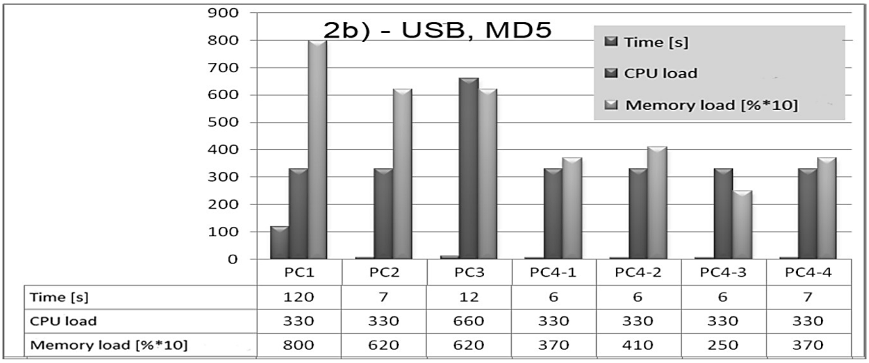
The PC1 configuration was exempted from the Figure 4 because the results diverged significantly from the research sample. In all configurations the memory and CPU load varies slightly. However, one should note the performance drop on PC4-1, PC4-2 and PC4-3 workstations. Contrary to the expectations – the more RAM computer has the more time it takes to complete this stage. This phenomenon stems from the way optimization process works. The memory is used to store search „trees". The bigger the memory size is, the larger the data „trees" become which affects the pace of search and insert operations. One should take into account that once the process is over the files take up less space on hard drive and their indexing is much more efficient.



	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]	180	120	30	20	21	21	47
CPU load	666	666	666	333	333	333	333
Memory load [%*10]	800	620	750	370	410	250	370

Fig. 5. Flash drive examination, creating a snapshot and sector boundaries

Figure 5 shows that taking hard drive snapshot takes much more time on PC1 and PC2 in comparison with other machines. It's worth noting that the workload for memory and CPU is the lowest again on PC4 configuration. Once more the task completion speed is marginally slower on PC4-4 configuration in comparison with PC4-2 and PC4-3 setups.



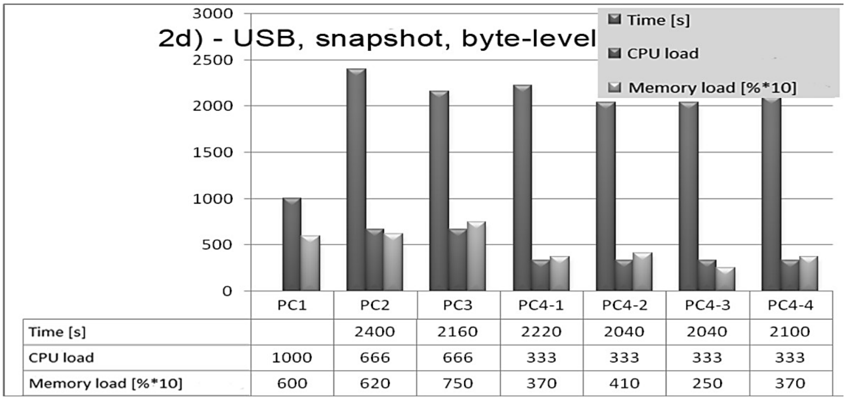
	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]	120	7	12	6	6	6	7
CPU load	330	330	660	330	330	330	330
Memory load [%*10]	800	620	620	370	410	250	370

Fig. 6. Flash drive examination, calculating md5

Figure 6 indicates that the checksum calculation heavily burdens the memory on PC1, PC2 and PC3 builds. The operation lasts the longest on PC1 machine whereas on all other computers the difference in time is minimal.

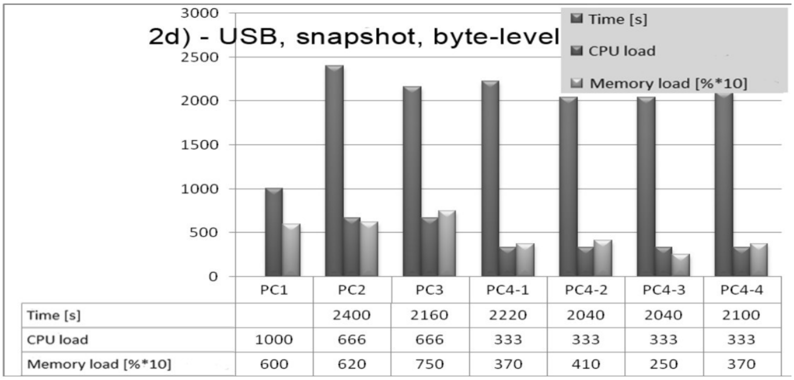
As shown in Figure 7, the PC1 again falls behind the other machines in terms of component performance and task completion speed. The CPU and memory workload in other configurations differs only slightly.

PC1 configuration for time was once again excluded from Figure 8 as they went off the scale. Likewise, same as before, the completion time for this operation varies insignificantly on the other configurations. Note that the stress of RAM and CPU is the lowest on PC4 configuration.



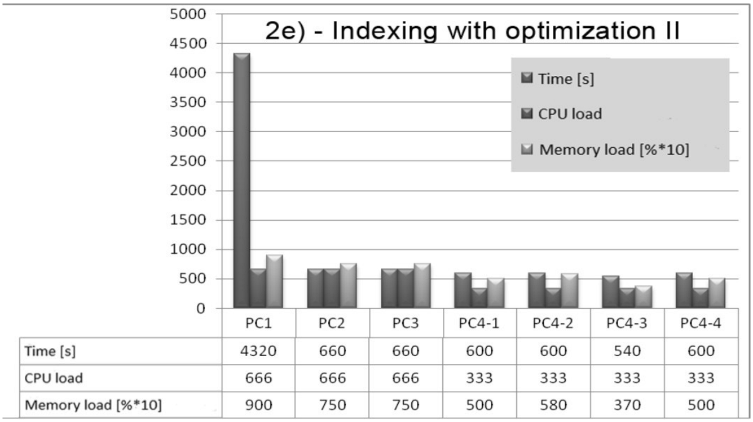
	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]		2400	2160	2220	2040	2040	2100
CPU load	1000	666	666	333	333	333	333
Memory load [%*10]	600	620	750	370	410	250	370

Fig. 7. Flash drive examination, indexing with optimization



	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]		2400	2160	2220	2040	2040	2100
CPU load	1000	666	666	333	333	333	333
Memory load [%*10]	600	620	750	370	410	250	370

Fig. 8. Flash drive examination, snapshot creation and byte-level analysis



	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Time [s]	4320	660	660	600	600	540	600
CPU load	666	666	666	333	333	333	333
Memory load [%*10]	900	750	750	500	580	370	500

Fig. 9. Flash drive examination, indexing with optimization – method II

Figure 9 indicates that the time constraint for PC1 decisively diverges from the results of other hardware platforms. The CPU and memory workload in other configurations hardly varies. In order to improve the legibility of all the presented charts the following assumptions were made:

- The units time are seconds.
- The levels of CPU stress belong to the subset of {1000, 666, 333} which means heavy, medium and small workload respectively.
- On the other hand the values of memory load are given in percentages multiplied by 10 which allows for better representation on charts.

Having collected the data, the next step was to create point chart in order to determine the most optimal configuration set. During each stage of the research the configuration, which had the best results in one category received 1 point. This means a single computer build could acquire the maximum of 3 points in any stage. All the points received by particular configurations were summed up to be presented in table 2.

In conclusion, the research data clearly shows that PC4-3 setup, which received the largest number of points, is the most optimal hardware configuration for X-Ways Forensics software.

Table 2. Research data – conclusions

Operation	PC1	PC2	PC3	PC4-1	PC4-2	PC4-3	PC4-4
Hard drive							
Creating an image	0	1	2	2	3	2	2
Snapshot	0	0	1	2	3	1	2
MD5	0	0	1	2	2	2	1
Indexing with optimization	0	0	1	0	0	2	0
Flash memory							
Snapshot sector level	0	0	0	1	2	3	1
MD5	1	2	0	2	2	2	2
Indexing with optimization	0	0	0	1	1	3	1
Snapshot	0	0	0	1	2	3	1
Indexing with optimization II	0	0	0	1	1	3	1
Results	1	3	5	12	16	21	11

CONCLUSIONS

The work of a Computer Forensics Investigator is intrinsically interwoven with the investigation proceedings and the future of the convicts. Consequently, access to appropriate hardware and software is an imperative, necessary to achieve desired levels of performance and detail. This work presented a body of research whose ultimate goal was to find an optimal hardware configuration necessary for the work of Computer Forensics Investigator who uses X-Ways Forensics Software. The research was conducted on 7 computer configurations whose examination required 77 different tests. In the course of the first stage, the researchers assumed minimal hardware specification, which was to reflect the most common household computer workstations. Next, six other, more advanced setups were assembled to be used in the research.

The performance results of the builds dedicated to work with X-Ways Forensics software are up to ten times better, the results of the minimal configuration. A special note should be taken at the way the amount of RAM affects the results of the tests. As it turned out machines with 8 GB of RAM perform worse by a few percent than their counterparts, which use only 4 GB of memory. It can be concluded that this unexpected behaviour stems from the way the operating system or the software itself uses the memory resources available on the machine. The examined data indicates that from all tested configurations the PC4-3 setup proves to be most optimal to work with X-Ways Forensics toolset. This research ought to be continued in the future to adequately reflect the technological changes, which result from dynamically developing computer hardware and forensic software markets.

BIBLIOGRAPHY

1. Anderson A., Mohay G.: Computer and intrusion forensics. Artech House Inc., 2003.
2. Królikowski P.: ComputerForensics Best Practices. Conference materials “II All-Poland Computer Forensics Conference”, Katowice 2010.
3. Fleischmann S.: X-Ways Forensics/WinHex Manual. X-Ways Software Technology AG, 2009.
4. Ganster Björn: email correspondence concerning X-Ways Forensics software features.
5. Metzger P.: Anatomia PC. Wydanie XI, Helion, Warszawa 2007.
6. Prosise C., Mandia K., Pepe M.: Incident Response and Computer Forensics. The McGraw-Hill Companies, 2003.
7. Casey E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Second Edition, Academic Press, 2004.
8. Marcella A.J., Greenfield R.S.: Cyber Forensics – A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. CRC Press LCC, 2002.

ANALIZA MOŻLIWOŚCI OPTYMALIZACJI SPRZĘTOWEJ DLA UZYSKANIA POPRAWY WYDAJNOŚCI PRACY PROGRAMU X-WAYS FORENSICS

Streszczenie

W pracy podjęto próbę ustalenia optymalnej konfiguracji sprzętowej dla stanowiska informatyka śledczego z wykorzystaniem aktualnego, specjalistycznego oprogramowania programu X-Ways Forensics. Aby zrealizować postawiony cel przeprowadzono badania różnych konfiguracji sprzętowych podczas wykonywania wcześniej określonych zadań – symulacji testowych. Po zakończeniu tego etapu prac dokonano analizy wyników badań i przeprowadzono wybór najbardziej optymalnej konfiguracji sprzętowej spośród przygotowanych do testów.

Słowa kluczowe: informatyka śledcza, symulacje testowe, konfiguracja sprzętowa.