SELECTION OF GOOD QUALITY ANTIVIRUS SOFTWARE

Sudhakar Singh[1], P.K. Khare[2], Prashant Mor[3]

[1] Research Scholar, Department of Physics and Electronics, RDVV, Jabalpur (M.P.), India and Associate Professor Department of Physics and Comp. Science , Sardar Patel College of Technology, Balaghat (M.P.), (India)

[2] Professor, Department of Physics and Electronics, RDVV, Jabalpur (M.P.), (India)

[3] Scientific Officer, Department of Physics and Electronics, RDVV, Jabalpur (M.P.), (India)

ABSTRACT

Antivirus software is the most commonly used technical control for malware threats mitigation, for operating systems and applications that are frequently targeted by malware. Antivirus software has become a necessity for preventing incidents. According to past experience with virus infection cases, most of them are related to operational practices when handling email or other IT security management issues. Antivirus products, Firewall products and other utility program are designed to protect computer system from Internet threats like hackers, viruses and worms by filtering out any suspicious communications sent to user computer. Current antivirus software also contains firewall and other utility program to protect computer system from malware related threats. Now in market there are many antivirus software available, therefore it is very important to know some tested result and parameter which help in selection of good quality antivirus software.

Keywords: Antivirus software, Antivirus engine, Antivirus parameter, Malware threats, Firewall

I. INTRODUCTION

Antivirus software often abbreviated as AV, sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software. Today enterprise networks are distributed to different geographical locations and applications are more centrally located. Every company's data is most valuable asset and must be treated as such. With the ever growing number of malicious threats such as Viruses, Spyware and Hackers, it has become mandatory to protect yourself against them. In order to prevent such data looses many organization came forward and designed network security tools and antivirus packages. Antivirus packages are mainly used to prevent and remove the viruses, Trojans, worms etc, where as firewalls are used to monitor incoming and outgoing connections. Computers are used extensively to process the data and to provide information for decision making therefore it is necessary to control its use. Due to organizational cost of data loss, cost of incorrect decision making, and value of computer software hardware organizations suffer a major loss therefore the integrity of data and information must be maintained. Antivirus packages are mainly used to safeguard. A specific component of the Antivirus and antimalware software commonly referred as the on-access or real time scanner, hooks deep into the operating systems core or kernel functions in a manner similar to how certain malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system accesses a file, the on-access scanner checks if the file is a legitimate file or not. If the file is considered a malware by the scanner, the access operation will be stopped, the file will be dealt by the scanner in pre-defined way i.e. how the Anti-virus program was configured during post installation and the user will be notified. This may considerably slow down the operating system depending on how well the scanner was programmed. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit bugs or trigger unexpected operating system behavior. Anti malware programs can combat malware in two ways**[1-3].**

(i) They can provide real time protection against the installation of malware software on a computer. This type of malware protection works the same way as that of antivirus protection in that the anti-malware software scans incoming network data for malware and blocks any threats it comes across.

(ii) Anti-malware software programs can be used solely for detection and removal of malware software that has already been installed onto a computer. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep or to compare this list to a list of known malware components, removing files that match.

There are number of venders providing antivirus packages which are differ in various features such as installation time, size, memory utilized, boot time, user interface launch time and full system scan time etc. We study in this paper to those parameter which are used to measure the performance of most commonly used antivirus products.

II. VARIOUS ANTIVIRUS ENGINE'S

The systems at highest risk are those that have internet access attached to their local retail network. Most viruses arrive through email attachments, but they can also arrive by downloading files, browsing the internet or simply using a diskette from home. More recently though, viruses have targeted Apple, Linux, handheld PDA, computers and cell phones. One of the few solid theoretical results in the study of computer viruses is Frederick B. Cohen's 1987 demonstration that there is no algorithm that can perfectly detect all possible viruses. However, using different layer of defense, a good detection rate may be achieved. There are several methods which antivirus engine can use to identify malware**[3-4].**

(i)Signature-based detection

It is the most common method. To identify viruses and other malware, the antivirus engine compares the contents of a file to its database of known malware signatures.

(ii)Heuristic-based detection:

It is generally used together with signature-based detection. It detects malware based on characteristics typically used in known malware code.

(iii)Behavioural-based detection

It is similar to heuristic-based detection and used also in Intrusion Detection System. The main difference is that, instead of characteristics hardcoded in the malware code itself, it is based on the behavioural fingerprint of the malware at run-time. Clearly, this technique is able to detect (known or unknown) malware only after they have starting doing their malicious actions.

(iv)Sandbox detection

It is a particular Behavioural-based detection techniques that, instead of detecting the behavioural fingerprint at run time, it executes the programs in a virtual environment, logging what actions the program performs. Depending on the actions logged, the antivirus engine can determine if the program is malicious or not. If not, then, the program is executed in the real environment. Albeit this technique has shown to be quite effective, given its heaviness and slowness, it is rarely used in end-user antivirus solutions.

(v)Datamining techniques

It is one of the latest approach applied in malware detection. Data mining and machine learning algorithms are used to try to classify the behaviour of a file as either malicious or benign given a series of file features, that are extracted from the file itself.

(vi)Digital Immune System

The digital immune system is a comprehensive approach to virus protection developed by IBM. The motivation for this development has been the rising threat of Internet based virus propagation. Traditionally, the virus threat was characterized by the relatively slow spread of new viruses and new mutations. Antivirus software was typically updated on a monthly basis and this has been sufficient to control the problem.

III. EVALUATION OF ANTIVIRUS ENGINE’S

When entering into an evaluation of antivirus engines the path to conclusive results requires patience and knowledge. Figure 1 shows simple flow chart of virus detection and table 1 shows comparison of some important virus detection methods according to their feature. Symbol √ means the method can support the property or may affect on the property positively. Actually, symbol √ □ dedicates an advantage for the method, while symbol **X** □ shows a weakness of the method. In scanning speed column, √□ denotes that the method can improve the scanning speed and reduce the time complexity. For example from the table it can be seen that hashing techniques in first generation scanners can improve the scanning speed and supports complete disinfection of the infected host, but it cannot used for detection of variants of a virus family or unknown viruses or macro viruses. It has no effects on the false negative or false positive alarm, as well in comparison to simple string signature scanning. Recently dynamic malware detection technology is mostly used in virus detection. The design of the testing process and the test files used will directly influence the outcome. Some important key point is given bellow**[5-7]**.

(i) Use a mixture of new and old files and a mixture of bad and good files

(ii) Do not just compare "number detected" but rather divide the detected files into categories like garbage /corrupted files, virus files and clean files in order to accurately compare detection rates of various engines

(iii) Consider turning off signature updates for a few days to a week, to test the engine's proactive capabilities

(iv) When using third party test results, it is important to understand how those results were achieved

(v) Besides testing virus detection levels, it is crucial to evaluate performance and/or system utilization, since this has the largest impact on cost and overall satisfaction levels from the system

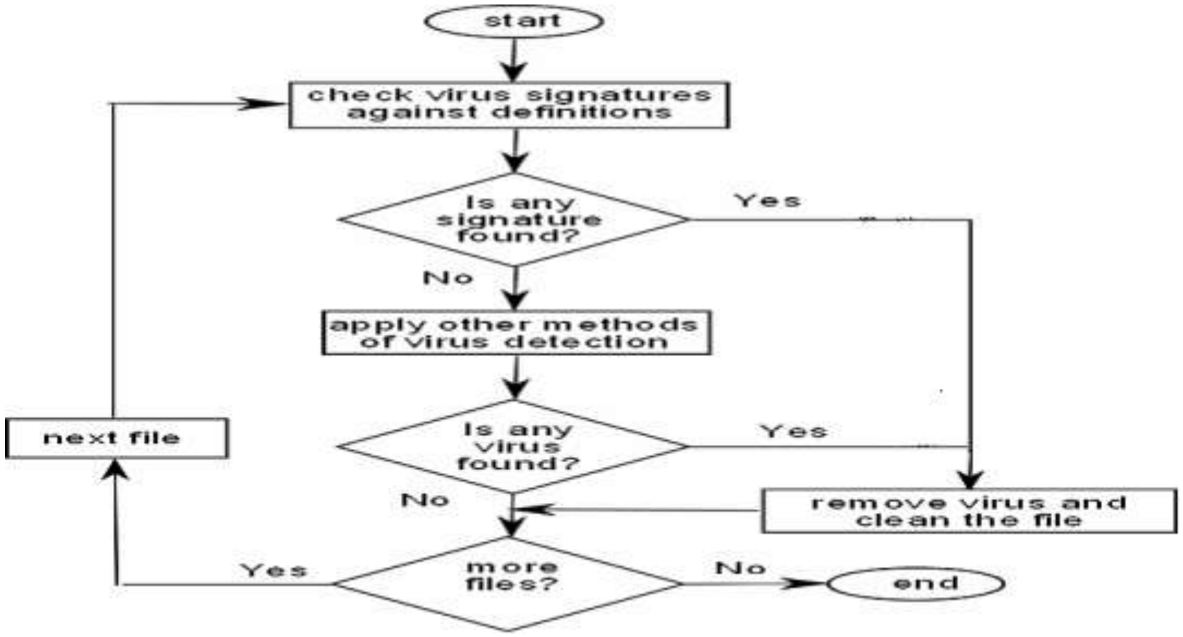
start
check virus signatures against definitions
Is any signature found?
Yes
No
apply other methods of virus detection
next file
Is any virus found?
Yes
No
remove virus and clean the file
Yes
more files?
No
end

Fig. 1: Virus Detection Process

Table 1: Comparison of virus detection methods according to their feature

Scanner Name	**Subcategories**	**Promise Perfect disinfection**	**Scanning speed improvement**	**Virus family detection**	**New or unknown Viruses detection**	**Encrypted/ polymorphic viruses**	**Metamorphic viruses**	**Macro viruses**	**False Positive**	**False Negative**

First generation Scanners [String Signature Scanning]	**Simple scanning**		√	x	x	x	x	x	x	Low	Low
	Optimizing Techniques	**wildcard**	√	x	√	x	x	x	x	Low	Low
		mismatch	√	x	√	x	x	x	x	Low	Low
		Generic degree	√	x	√	x	x	x	x	Low	Low
	Bookmark		√	x	x	x	x	x	x	Very low	low
	Speed up technique	**Hashing**	√	√	x	x	x	x	x	Low	Low
		Top and tail scanning	√	√	x	x	x	x	x	Low	High
		Entry point/Fixed point	√	√	x	x	x	x	x	Low	Low
Second generation scanning	**Smart scanning**		√	√	√	x	x	√	√	Low	Low
	Skeleton detection		√	x	x	x	x	x	√	Low	Low
	Nearly exact identification		√	x	x	x	x	x	x	Very low	Very low
	Exact identification		√	xx	√	x	x	x	x	Zero	Zero
	Heuristic analysis		x	x	√	√	x	√	√	Very high	Low

IV. VIRUS DEFENCE SOFTWARE

Common sense which are very useful for protecting computer system from virus infection given bellow.

(i) Keep your Internet browser up-to-date by ‘patching’ it regularly. Most browser updates include new security elements to meet newly identified virus threats. These updates can be obtained from Microsoft for Internet Explorer and other browser can be updated from their website also.

(ii) Purchase virus defense software. You should identify your individual requirements depending on your technical infrastructure, geographic spread and dependency on technology.

(iii) Suppliers offer many kinds of anti-virus program, some of which are downloadable from their web sites.

(iv) Use this software to scan e-mail attachments for viruses before you open them and also run an anti-virus program that scans files as they are opened. This type of scanning should take place constantly, automatically checking every file, programme or document each time it is opened or used. In network connected system Gateway virus checking, Server virus checking , Workstation virus checking etc. Performed by antivirus engine.

In present time various types of antivirus software are available. Some antivirus software support only windows, Some Linux/Unix and some Mac, Some software are also available which support two or more than two platforms. Table 2 shows list of Anti-virus Freeware, Table 3 shows list of Anti-virus Trialware, Table 4 shows Internet Security Suites Freeware which include anti-virus, firewall and other functions and Table 5 shows Internet Security Suites Trialware which include anti-virus, firewall and other functions**[8-9]**.

Table 2: Anti-virus Freeware

Name	Link	Platforms			
		Windows	Linux/Unix	Mac	Mobile
Android Antivirus	https://play.google.com/store/apps/details?id=and.anti				Y (Support Android)
Zoner Antivirus	http://www.zonerantivirus.com/	Y	Y		Y (Support Android)
Symantec iAnti Virus	http://www.iantivirus.com/product/			Y	
Sophos Antivirus	http://www.sophos.com/en-us/products/free-tools.aspx			Y	
Microsoft Security Essentials	http://www.microsoft.com/security_essentials/	Y			
Kingsoft AntiVirus	http://www.kingsoftsecurity.com/	Y			
Comodo Antivirus	http://www.comodo.com/products/free-products.php	Y	Y	Y	

Table 3: Anti-virus Trialware

Name	Link	Platforms			
		Windows	Linux/Unix	Mac	Mobile
BitDefender Antivirus Plus	http://www.bitdefender.com/Downloads/	Y			
F-Secure Anti-Virus	http://www.f-secure.com/en/web/home_global/anti-virus	Y		Y	
G Data AntiVirus	http://www.gdatasoftware.com/free-trial.html	Y			
McAfee AntiVirus Plus	http://home.mcafee.com/store/antivirus-plus	Y			
Panda Antivirus	http://www.pandasecurity.com/homeusers/downloads/	Y		Y	
Symantec Norton AntiVirus	http://hk-en.norton.com/downloads/	Y		Y	

Table 4: Internet Security Suites - Freeware (include anti-virus, firewall and other functions)

Name	**Link**	**Platforms**			
		Windows	**Linux/Unix**	**Mac**	**Mobile**
Avast Free Mobile Security	http://www.avast.com/free-mobile-security				Y (Support Android)
Avira Android Security	http://www.avira.com/en/avira-android-security				Y (Support Android)
BitDefender Mobile Security	http://www.bitdefender.com/toolbox/freeapps/mobile/				Y (Support Android)
Checkpoint ZoneAlarm Free Antivirus + Firewall	http://www.zonealarm.com/security/en-us/anti-virus-spyware-free-download.htm	Y			
Comodo Internet Security	http://www.comodo.com/products/free-products.php	Y			
360 SecuritySafe and MobileSafe (Chinese version)	http://www.360.cn/	Y			Y (Support Android, iOS, Symbian

Table 5: Internet Security Suites – Trialware (include anti-virus, firewall and other functions)

Name	**Link**	**Platforms**			
		Windows	**Linux/Unix**	**Mac**	**Mobile**
Panda Internet Security	http://www.pandasecurity.com/homeusers/solutions/internet-security/	Y			
Sophos Complete Security Suite	http://www.sophos.com/en-us/products/complete/complete-security-suite.aspx	Y	Y	Y	
Symantec Norton Internet Security	http://us.norton.com/downloads	Y		Y	
Kaspersky Internet Security	http://www.kaspersky.com/trials	Y		Y	Y (Support Android)
F-Secure Internet Security, Mobile Security	http://www.f-secure.com/en/web/home_global/support/installers	Y			Y (Support Android, Symbian)
BitDefender Sphere	http://www.bitdefender.com/Downloads/	Y		Y	Y (Support Android)
AVG Internet Security	http://www.avg.com/ww-en/internet-security	Y			
avast! Internet Security	http://www.avast.com/download-software	Y			
McAfee Internet Security, Mobile Security	http://home.mcafee.com/store/free-antivirus-trials	Y			Y (Support Android, Blackberry, Symbian

V. ANTIVIRUS SOFTWARE PERFORMANCE MEASUREMENT PARAMETER

Antivirus products are categorized into three parts such as Internet Security [IS], Total Security [TS] and Antivirus [AV]. Antivirus products are the products, which are primarily focused on detecting and remediation viruses and Spyware. Internet Security product provides all the virus and Spyware removal features of an antivirus (AV) as well as additional functions to provide greater Internet protection. These features may include protection against phishing, root kit detection, firewalls and scanning of web pages and HTTP data. Total Security products provide data migration and backup features on top of all security features common to internet security (IS) products. For the test performance of antivirus software following parameters were used **[10-11]**.

1. Installation Size [INS].
2. Installation Time [INT].
3. Boot Time [BT].
4. Scan Time [ST].
5. User Interface Launch Time [UILT].
6. Memory Usage During System Idle [MUDSI].
7. Browse Time [BwT].
8. File Copy, Move and Delete [FCMD].

(i) Installation Size

A products Installation Size was previously defined as the difference between the initial snapshot of the Disk Space (C: drive) before installation and the subsequent snapshot taken after the product is installed on the system. Although this is a widely used methodology, we noticed that the results it yielded were not always reproducible in Vista due to random operating system operations that may take place between the two snapshots. We improved the Installation Size methodology by removing as many Operating System and disk space variables as possible. This metric aims to measure a product’s total installation size. This metric is defined as the total disk space consumed by all new files added during a product's installation

(ii) Installation Time

This test measures the minimum installation time a product requires to be fully functional and ready for use by the end user. Installation time can usually be divided in three major phases **.** The speed and ease of the installation process will strongly influence the user’s first impression of the antivirus software. This test measures the minimum installation time required by the antivirus software to be fully functional and ready for use by the end user. Lower installation times represent antivirus products which are quicker for a user to install.

(iii) Boot Time

This metric measures the amount of time taken for the machine to boot into the operating system. Security software is generally launched at Windows startup, adding an additional amount of time and delaying the startup of the operating system. Shorter boot times indicate that the application has had less impact on the normal operation of the machine.

(iv) Scan Time

Scan Time is the time it took for each product to scan a set of sample files. The sample used was identical in all cases and contained a mixture of system files and Office files. All antivirus solutions have functionality designed to detect viruses and various other forms of malware by scanning files on the system. This metric measured the amount of time required to scan a set of clean files.

(v) User Interface Launch Speed

This metric provides an objective indication as to how responsive a security product appears to the user, by measuring the amount of time it takes for the user interface of the antivirus software to launch from Windows. To allow for caching effects by the operating system, both the initial launch time and the subsequent launch times were measured. Our final result is an average of these two measurements.

(vi) Memory Usage During System Idle

This metric measures the amount of memory (RAM) used by the product while the machine and antivirus software are in an idle state. The total memory usage was calculated by identifying all antivirus software processes and the amount of memory used by each process. The amount of memory used while the machine is idle provides a good indication of the amount of system resources being consumed by the antivirus software on a permanent basis. Better performing products occupy less memory while the machine is idle.

(vii) Browse Time

This metric measures the time taken to browse a set of popular internet sites to consecutively load from a local server in a user’s browser window.

(viii) File Copy, Move and Delete

This test measures the amount of time required for the system to copy, move and delete samples of files in various file formats.

VI. RESULTS AND DISCUSSION

On the basic of parameter, Performance of Internet security products and Antivirus software are given bellow.

(i) Products with lower boot times are considered better performing products.
(ii) Products with lower scan times are considered better performing products.
(iii) Products with lower User Interface launch times are considered better performing products.
(iv Products with lower memory usage during system idle (usage of RAM) are considered better performing products.
(v) Products with lower browse times are considered better performing Products.
(vi) Products with lower Internet explorer launch times are considered better performing products..
(vii) Products with lower installation times are considered better performing Products.
(viii) Products with lower installation sizes are considered better performing Products.

The one of most important parameter of antivirus, which is commonly known as the detection rate. The second is to know under which circumstances the software is able to see the virus. Can it see viruses if they come through a network share, via email or if they are already running in memory. There are three things you could do and should not do to get the assurance that your anti-virus software is indeed reliable. First user could be tempted to test the anti-virus yourself, to go on the net looking for virus libraries and throw them at the anti-virus. I would strongly discourage you from doing so, even if some vendors include such a methodology in their white papers. As EICAR (European Institute for Computer Ant-Virus Research) states: “Using real viruses for testing in the real world is rather like setting fire to the dustbin in your office to see whether the smoke detector is working”, You are not a virus expert and you never know what can happen. What if the anti-virus does not catch them all and they start deleting data on your hard drive or start spreading in your enterprise. That could cost you your job. Anti-virus experts themselves take all the precaution when dealing with viruses, ensuring, for example, that all infected media they handle are destroyed after being reviewed. Second, if you really want to know that the anti-virus is doing something, you can download at www.eicar.org a safe anti-virus test string. Most anti-virus software will detect the eicar file as being infected. That is a secure way to check the anti-virus ability to see viruses under different circumstances**[12-13].**

Finally, we can rely on external sources to verify the anti-virus detection rates. In order to understand what detection rates really mean, you need to know the difference between viruses in the wild and viruses In-The-Zoo. The In-The-Zoo viruses are lab viruses that have not been encountered in the real world. The In-The-Wild viruses are viruses that have been infecting computers worldwide. A list of the In-The-Wild viruses is kept by the WildList Organization International and can be found at www.wildlist.org.

□(i) The Virus Bulletin at www.virusbtn.com , for example, awards a 100% logo to products that pass their testing. It consists of testing anti-virus on-demand and real-time scanners against the list of the viruses found in the wild. The products able to detect a 100% of the in-the-Wild list are awarded.

□(ii)□□ The West Coast Lab offers two levels of checkmarks for anti-virus products. Vendors have to pay to have their products tested. The first level is passed if the product detects 100% of the virus listed in the WildList. To obtain the level 2 checkmark, the anti-virus has to pass level 1 and has to be able to repair all reparable viruses of the WildList without altering the system stability. The checkmarks can be found at www.check-mark.com/cgi-bin/redirect.pl. The West Coast Lab also provides test results for anti-virus software ability to catch Trojan horses.

□(iii) The ICSA (International Computer Security Association), division of TrueSecure, offer certification for On-Demand/On-Access anti-virus products, anti-virus products cleaning, anti-virus product for Internet Gateway E-mail, anti-virus products for Microsoft Exchange and Lotus Notes, anti-virus products for Security Service Providers, Internet Service Providers and anti-virus scanners. Anti-virus vendors also have to pay a fee to have their products tested. To be certified an On-Access or Real-Time scanner, for example, has to detect 100% of the viruses listed in the current In-The-Wild List, detect 100% of the viruses listed in the ICSA Labs Common Infectors Test Suite, detect 90% of macro viruses in the ICSA Labs Virus Collection and not cause false positives. An exhaustive list of the certification criteria for each type of anti-virus product can be found at:www.icsalabs.com/html /communities/antivirus/certification.shtml. A list of all testing results can be found at: www.icsalabs. com /html /communities/antivirus/index.shtml.

VII. CONCLUSIONS

As a member of the IT community, user face challenges every day in keeping servers and workstations up and running. These challenges are complicated by the demands of an increasingly complex IT environment, limited IT resources and often the requirements of a service level agreement as well. Yet the failure to meet these challenges can result in decreased IT credibility, unanticipated organizational changes, outsourcing of IT functions and diminished resource allocations all of which make it even harder for you to provide excellent service in the future. Computer viruses are among the most frustrating challenges faced by IT organizations today. They rob workers of productivity, divert IT personnel from more strategic corporate concerns and can even jeopardize company's information security. Yet there is no way which can keep every virus out of your company's computers. Employees unthinkingly launch executable email attachments that contain them. Newsreader programs pick up viruses attached to Usenet postings. Traveling employees bring them in on laptops after visits to customer sites.

Different tools are good at tackling different malware related threads or problems. Some are better at one or two than others. Some have better overall detection records than others and some are faster than others. There is no best unique anti-virus product. The choice of anti-virus solution should depend on user needs, user environment and user goals. Vendor information is always useful, but it is not wise to rely solely on them. In order to make the right choice of antivirus products, user should see yourself, look vendor information and see tested result released by different security company as well as other alternative sources.

REFERENCES

[1] OUCH, “Understanding Anti-Virus Software”, Newsletter, March 2011

[2] Singh Brijendra., “Network Security and Management”, Prentice Hall of India Private Limited, New Delhi- 110001, Published in 2007.

[3] Stalling, William., “Network Security Essentials application and standards”, Third Edition, Pearson Prentice Hall, Published in 2008

[4] http://en.wikipedia.org/Antivirus_software

[5] Anti-virus Product Evaluation Criteria, www.emory.edu/ITD/DESKNET/AV/criteria.htm

[6] SANS, “OUCH Monthly Security Awareness”, News Letter, March 2011

[7] Umakant Mishra, “An Introduction to Virus Scanners”, Available on http://www.trizsite.tk

[8] Peter Szor, “The Art of Computer Virus Research and Defense”, Addison Wesley Professional, edition First, February 2005.

[9] ICSA, http://www.icsalabs.com/html/communities/antivirus/index.shtml.

[10] www.passmark.com, Access on Oct. 2014.

[11] Gordon Sarah, "A Short Course in Antivirus Software Testing", White Paper, Available on www.symantec.com; Access on Nov. 2014.

[12] www.virusbtn.com, Access on Dec. 2014

[13] www.icsalabs. com /html /communities/antivirus/index.shtml. , Access on Dec. 2014