# Performance Investigation of Antivirus-
# A Comparative Analysis

## REMYA THOMAS and NACHAMAI.M*

Department of Computer science, Christ University, Bangalore, India.
*Corresponding author E-mail: nachamai.m@christuniversity.in

### Abstract

Antivirus as name implies preventthe devices such as computers, mobiles and pen-drive from viruses. All gadgets which interact with open network are prone to virus.Virus is a malicious software program which replicates by copying its code multiple times or by infecting any computer program(like modifying the existing program) which can affect its process. Virus perform harmful task on affected host computer such as possessing on hard disk, CPU time, accessing private information etc. This paper specifies the performance of(McAFee, Avast, Avira, Bitdefender, Norton)antivirus and its effectiveness on the computer. The performance is tested based on the time acquired by each antivirus to act on a computer. The parameters used to analyze the performance are quick scan, full scan and custom scan with respect to time. Through the analysis Bitdefender performance is better than other selected antivirus.

**Keywords**: Antivirus, Computer scan, Virus, Performance Testing.

## INTRODUCTION

The explosion with World Wide Web is always prone to the interaction of unknown threat which can ruin the computer. Antivirus software plays an active role towards the prevention of hidden threats in web which can affect the computer. The infection can be of different types such as Droppers, Trojans, root-kits, worms, viruses, and so on. Antivirus is security software that focuseson providing better protection. The physical view of an antivirus is shown in fig1. Antivirus software is used to disinfect the infected program or to completely immaculate malicious software from the system.

Antivirus software uses different techniques to identify malicious software, which often self-protect and mask deep in an operating system. Advanced virus may use undocumented operating system functionality and hidden techniques in order to prevail and avoid being detected. Because of the huge malware attack these days, Antivirus software is designed to handle all kinds of malignant payloads attacking from both trusted and un-trustedsources.

Antivirus software consists of different types of scan like full scan, quick scan and customscan.

**Full Scan**

Full scan[1] is performed to ensure that the computer is free from viruses. It helps to scan files, local drive, folders on thesystem. Full scan can be performed on external devices likedigital camera, USB drivers and many others.

**Quick Scan**

Quick scan is used to scan the most infected area in a computer. A quick scan checks only the common areas for viruses available in a computer. Scanned areas include common areas of the hard drive, including the temporary files, computer memory and the operating system directory. Basically quick scan take less than 20-30 minutes to complete. Full scan checks every folder available, and hence takes longer time to perform the scan. Depending on the hard drive and memory space a computer, it could take 40 minutes to several hours to accomplish a full scan.

**Custom Scan**

Custom scan as name implies allows the user to customize which files and folders are to be scanned. This scan is useful when the user likes to perform a scan for a particular folder, or if the user likes to scan an entire drive. Customscan helps to remove unknown viruses, spyware, tracking cookies, potential threats and stealth programs, which can exploit and alter Windows system files. For the performance study of different antivirus, parameters like full, custom and quick scan are performed on the basis of time.

**Literature Review**

In research paper" A Comparative Study of Virus Detection Techniques"[2] determines that, to model the behavior of virus the use of "logic formulae" is one of the most recent developments
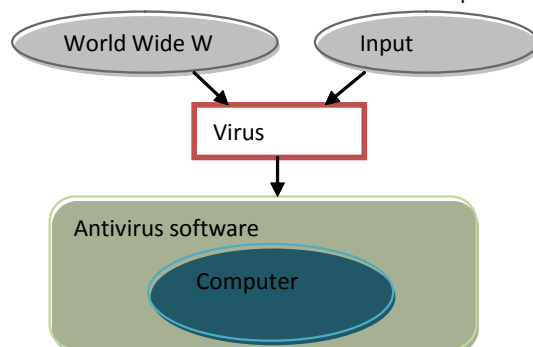


**Fig. 1: Physical view of an antivirus**

in computer virus research. Logic formulae are an alternative to basic virus detection technique. Behavior based virus detection is used to overcome the issues related with traditional signature based virus identification. Signature based virus detection is explained with pros and cons.

In research paper" Study and Comparison of Virus Detection Techniques "[3] determines that, as the characteristics of different viruses are different, the detection approaches should be different. Viruses of the different types cannot be detected by single method. Viruses are classified as simple virus,Encrypted Viruses, Polymorphic Viruses, Oligomorphic virus, Metamorphic Viruses. The virus detection methods specified are Signature based virus detection, Anomaly Based Detection, Code Emulation. Signature scanning is concluded as the easy and economical method for detecting majority of current available viruses and it causes less impact on existing hardware and codes.

In research paper" Antivirus Software Testing for the New Millenium"[4] determines about the antivirus system of next generation are discussed. The organization testing the antivirus is ICSA Certification, Westcoast Labs Checkmark, University of Hamburg VTC malware tests etc. Network aware viruses like Melissa have proven that virus specified techniques are not sufficient enough to prevent infection by new viruses. The inherent backlog of post-infection generic methods and pre-infection heuristics make virus detection more powerful way to prevent and remove viruses. Antivirus products that consist of hybrid approach are likely to evolve.

The performance study of different antivirus is described in detail for computer in [5]. The classification is based on three groups (ranks) of antivirus i.e. AV Test,VB, AV comparative. According to the survey,no antivirus engine consistently holds the top place in each year across all testing organization.

The performance and protection of antivirus is described in detail in[6,7] where different antivirus are compared based on scanning methods like on-demand and on-access malware scan ,website rating,malicious URL blocking, Phishing protection, Behavior based detection and vulnerability scan.

## MATERIALS and METHODS

Anti-malware software also known as Antivirus, is computer software that is usedto detect, prevent and remove malicious software[8].

To study the performance of the different antivirus in a computer system full scan, custom scan, and quick scan parameters/methods are considered.

Basically four levels of malware products are available in the market:
• Free
• Paid antivirus
• Suites
• Premium suites

Moving from free to premium suits the features gets added such as identity theft protection, parental controls, firewalls and system performance tools. Free antivirus software basically provides a bare low level of protection. It will scan for virus, and often can perform automatic virus scans as well. Few free apps have additional protection tools such as a browser add-on that checks for harmful links and premium suites consist of firewall[9]. Usually these features are limited to paid antivirus software products.

Paid antivirus lies as a middle ground between the basic free and the feature-packed antivirus security suites. Paid antivirus offers overall security tools like parental controls, identity theft protection and hence more flexibility than a free antivirus package available, usually paid antivirus consist of few additional features than suites, which are designed to be one-stop protections hops.The biggest issue faced while going with free antivirus products is the lack of technical support, free antivirus users usually must assist by themselves.

Anti-viruses selected for the analysis in this research work are:

### Norton

Norton is one of the well-known antivirus software. One of its key features is that it updates every 10 to 15 minutes to ensure that the system is up to date.

### McAfee

McAfee Antivirus is software that protects the computer from spyware and viruses, and includes a firewall that helps in preventing hacker attacks to the computer.

### Bit defender

Bit Defender give protection from spyware, viruses, root-kits, provides anti-phishing service, and offers a laptop and gamer mode.

### Avira

Avira introduced Avira Protection Cloud (APC) whichtakes the information available through internet (cloud computing) to enhance the detection and effect on system performance less. APC was initially used only during a manual quick system scan but later it was extended to real-time protection.

### Avast

Avast is the popular antivirus available in the market, and it has the largest share of the market for malware applications. Avast free antivirus product's features include antivirus with Avast Passwords, antispyware, streaming updates, Secure HTTPS scanning, Home Network Security scanner, Site Correct, Do Not Track, anti-malware, Smart Scan, Rescue Disk, anti-phishingand Software Updater (manual).

For the comparative performance analysis of antivirus, time consumed by different anti-viruses for different scans like full, quick and customized are considered. Analysis is performed on a laptop consisting of intel i3 core processor with 2 GB RAM, 64 bit operating system and windows 8.1 single language version. The common steps carried out for the entire antivirus are:

Step 1: Install antivirus in the computer.
Step 2: Double click/right-click on the Antivirus System Tray icon and navigate to antivirus software.
Step 3: Click on scan tab
Step 4: Select the type of scan available in provided option (i.e. full scan, quick scan, custom scan).
Step 5: If custom scan is opted, user will be able to select the folders, drivers and software available on the system.

Step 6: Click on "Start" scan.

Step 7: The user will be prompted with the alert box with option "View results" after the scan gets completed

Step 8: The scan result will be displayed on the screen.

Step 9: The user will be able to repair the errors.

Antivirus programs are essential as they are powerful pieces of software for windows computers. For smart computer users there will be virus through plug-in and browsers. Hence multi-layer security strategy is required. Antivirus protection provides multilayer security strategy for computer. Installed antivirus will be continuously run in background checking all the files which user accesses. When software I installed the antivirus software compares the software for known worms, virus or malwares. Antivirus also checks for the new or unknown virus based on the bad behavior of the software. Antivirus detects security holes in the program that has infected the computer.

The comparison study performed for the performance analysis of antivirus (Norton, Avast, Avira, Bit Defender, McAfee) is tested by the basic manual testing using the antivirus and its different types of scans. This paper focuses mainly on three type of scan i.e. full, quick and custom with respect to the time taken by the antivirus to complete the scan. The scan analysis made for each antivirus is represented in the table 1, table 2 and table 3 respectively. As the observation, full scan takes more time as it scan whole computer folders, drivers and software. Custom scan is performed in the entire antivirus selecting the C drive of the computer. In the observation quick scan scans the virus prone areas only hence less time compared to full scan and custom scan. The time consumed to complete the custom scan is based on the user folder selection. The protection and performance of all the three antivirus is tabulated in table 4.

**System Information:**

System Type: 32- bit Operating System.
RAM: 2 GB.
Processor: Intel(R) Core(TM) i3.
No. of files scanned in Full scan: 800114 files
No. of files scanned in Quick scan:55672 files
No. of files scanned in Custom scan: 413234 files

**Table1. Time based analysis on antivirus using full scan**

| Parameters | Full scan | |
|---|---|---|
| Antivirus | Time(mins) | Files |
| McAfee | 176 | 772887 |
| Avira | 175 | 795699 |
| Avast | 170 | 795678 |
| Bitdefender | 166 | 799891 |
| Norton security | 178 | 789887 |

**Table 2.Time based analysis on antivirus using quick scan**

| Parameters | Quick scan | |
|---|---|---|
| Antivirus | Time(mins) | Files |
| McAfee | 63 | 55332 |
| Avira | 76 | 55112 |
| Avast | 60 | 49195 |
| Bitdefender | 65 | 55672 |
| Norton security | 50 | 55682 |

**Table 3: Time based analysis on antivirus using custom scan**

| Parameters | Custom Scan | |
|---|---|---|
| Antivirus | Time(mins) | Files |
| McAfee | 127 | 334232 |
| Avira | 130 | 328605 |
| Avast | 124 | 343234 |
| Bitdefender | 133 | 345783 |
| Norton security | 139 | 337832 |

**Table 4: Antivirus performance and protection percentage[10]**

| Antivirus | Protection | Performance |
|---|---|---|
| McAfee | 58 | 83 |
| Avira | 92 | 100 |
| Avast | 100 | 75 |
| Bitdefender | 100 | 100 |
| Norton security | 100 | 92 |

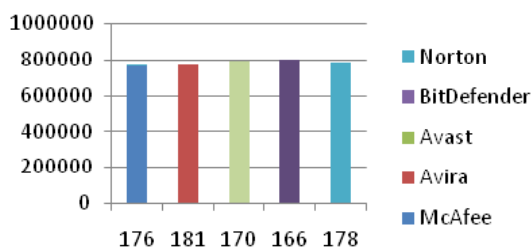**Fig. 2: Full scan graph(x axis: time, y axis: No. of files)**



**Fig. 3: Quick scan graph(x axis: time, y axis: No. of files)**

## RESULTS and DISCUSSIONS

### Full scan

McAfee antivirus scanned less files with more time than Avira. Avast scanned less files with less time compared to Avira. Bitdefender scanned more files in less time compared Norton. Hence Bitdefender antivirus performed better than other antivirus by scanning more files in less time. Hence the data fetched by top ten reviews.com looks good in full scan as the top ten reviews mention Bit Defender to have 100 percent performance and protection. The full scan results are plotted in figure 2.

### Quick Scan

In Quick scan Avira scanned less files consuming more time than McAfee. Avasta scanned less files in less time than Avista.Norton scanned more files in less time than Bitdefender. Hence the data fetched by top ten reviews.com looks good in Quick scan as the top ten reviews mention Bit Defender to have 92 percent performance and 100 percent protection. The quick scan analysis is plotted in figure 3.

### Custom scan

In custom scan performed for C drive, Avira scanned less files consuming more time than McAfee.Avasta scanned more files in less time compared to McAfee. Bitdefender scanned more files than Norton in less time. Hence Bitdefender performance is more than any other antivirus. The custom scan analysis is represented in the form abar chart in fig 4.

As per the top ten reviews.com bitdefender has 100% performance and protection which is the same case of the analysis performed based on this
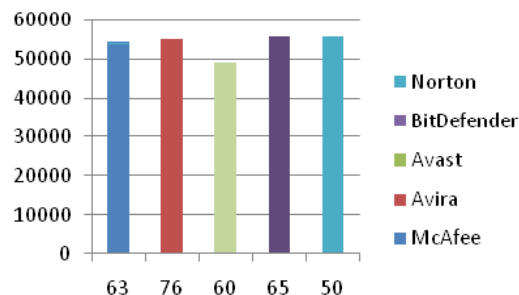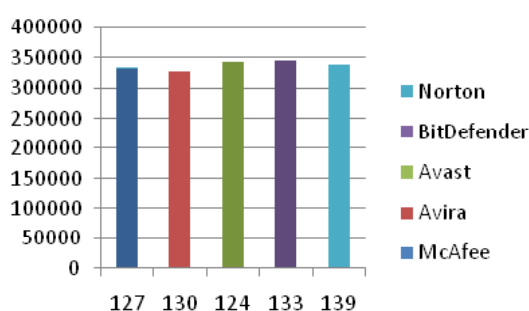


**Fig. 4: Custom scan graph(x axis: time, y axis: No. of files)**

paper. But comparing the performance of Avira to other antivirus, it has less performance as Avira took more time to scan the less number of files. But in the toptenreviews McAfee performance is tagged to below compare to other antivirus. Hence according to the analysis, Bitdefender has more performance compared to other antivirus and Avira has less performance.

## CONCLUSION

Antivirus is a powerful program which protects and removes viruses from computer. Antivirus download new and updated definition files which contains the signature of viruses. When antivirus scans a file and identifies that the file matches a known piece of malware, antivirus stops the file from running further and put them into "quarantine". In the performance study of different antiviruses, Bitdefender have high performance as bitdefender scans more files in less time. Norton can be rated second high performer as Norton as well scans more files in less time. Performance of Avira is low as it takes more time to executed limited files.

## REFERENCES

1. https//www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/
2. Sulaiman Al Amro and Ali Alkhalifah," A Comparative Study of Virus Detection Techniques".
3. Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad and Vinayak N Malavade," Study and Comparison of Virus Detection Techniques".
4. Sarah Gordon," Antivirus Software Testing for the New Millenium".
5. https://www.opswat.com/blog/antivirus-performance-study-shows-diversification-key
6. http://in.pcmag.com/antivirus-from-pcma/37090/guide/the-best-free-antivirus-protection-of-2016
7. http://thinhlong.vn/upload/download/avc_report25.pdf
8. https://www.raymond.cc/blog/test-the-effectiveness-of-your-antivirus-firewall-and-hips-software/
9. https://www.sans.org/readingroom/whitepapers/commerical/anti-virus-software-challenge-prepared-tomorrows-malware-today-782
10. http://www.toptenreviews.com/software/security/best-antivirus-software/