School of Computer Science and Engineering

COURSE TITLE: OPERATING SYSTEMS

COURSE CODE: CSE2005

Slot: F2

PROJECT TITLE: RELATIVE STUDY OF UEFI AND BIOS WITH THEIR TECHNICAL SPECIFICATIONS

SUBMITTED TO:

PROF. MEENAKSHI SP.

SUBMITTED BY:

S. No	Name	Reg. No	Lab slot
1	ADITYA ROHILLA	18BCE0929	L19+ L20
2	KHWAAB THAREJA	18BCE0930	L19+ L20
3	SHRESTH SRIVASTAVA	17BEC0340	L19 + L20

ABSTRACT:

New computers use UEFI code rather than the standard BIOS. each are low-level software that starts once we boot your pc before booting your OS, however UEFI may be an additional trendy solution, supporting larger hard drives, quicker boot times, additional security measures, and handily higher graphics and mouse cursors. However, this ancient BIOS is currently outdated. Of course, the BIOS has evolved and improved over time. Some extensions were developed, as well as ACPI, the Advanced Configuration and Power Interface. this permits the BIOS to more simply configure devices and perform advanced power management functions, like sleep. however, the BIOS hasn't advanced and improved nearly as much as alternative computer technology has since the times of Microsoft disk operating system. UEFI replaces the standard BIOS on PCs. There's no way to switch from BIOS to UEFI on an existing laptop. we'd like to shop for new hardware that supports and includes UEFI, as most new computers do. Most UEFI implementations give BIOS emulation thus we will prefer to install and boot old operating systems that expect BIOS rather than UEFI, thus they're backwards compatible. **The new specification (UEFI) addresses many limitations of BIOS, as well as restrictions on magnetic disc partition size and therefore the quantity of time BIOS takes to perform its tasks.**

I) INTRODUCTION:

i) FIRMWARE:

Firmware is a pc software package that has a control over the system hardware to that it's been connected. It's one among the foremost vital softwares that run on any kind of system. It's a built-in software package that runs on any system which may neither be modified nor removed however in rare cases will be updated.

Considering the firmware of the modern computers that we tend to use, from the past once the pc came into use the sole firmware interface that was used was BIOS (Basic input-output system).

ii) BIOS:

BIOS is the low-level software that is present on a chip on the motherboard of computer. It initializes all the hardware components of the computer when the computer starts up. Apart from initializing, it also ensures their proper functionality. After the initialization it runs the boot loader which boots the windows or any other OS that any computer has.

Settings like computer's boot order, hardware configuration, system time etc can be configured using the setup screen of BIOS when the BIOS is loaded.

It's highly important that the system's firmware is working properly and efficiently as it's the component that connects hardware and software by initializing the hardware along with OS.

iii) UEFI:

Unified Extensible Firmware interface (UEFI) is a specification for a software program that connect computer's firmware to OS.

UEFI is expected to replace BIOS.

BIOS limitations:

- Doesn't support larger disk spaces.

Often BIOS is programmed with a disk space limitation.

II) RELATED WORKS and DETAILS:

i) BACKGROUND:

The UEFI firmware will boot from drives of 2.2 TB or larger—actually, the theoretical limit is 9.4 zettabytes. That's roughly thrice the calculable size of all the information on the net. That's because UEFI uses the GPT partitioning theme rather than MBR. It additionally boots in a more standardized way, launching EFI executables instead of running code from a drive's master boot record.

UEFI will run in 32-bit or 64-bit mode and has a lot of available address space than BIOS, which implies your boot method is quicker. It additionally implies that UEFI setup screens may be slicker than BIOS settings screens, together with graphics and mouse pointer support. However, this isn't necessary. several PCs still ship with text-mode UEFI settings interfaces that look and work like a recent BIOS setup screen.

UEFI is filled with different options. It supports Secure Boot, which implies the software may be checked for validity to confirm no malware has tampered with the boot method. It will support networking options right within the UEFI firmware itself, which might aid in remote troubleshooting and configuration. With a conventional BIOS, we've got to be sitting in front of a physical pc to tack it.

It's not simply a BIOS replacement, either. UEFI is actually a small software that runs on top of the PC's firmware, and it will do tons over a BIOS. it should be kept in non-volatile storage on the motherboard, or it should be loaded from a hard drive or network share at boot. PCs with UEFI can have different interfaces and options. It's all up to your computer manufacturer, however the fundamentals are going to be identical on every computer.

III) WORK FLOW, DISCUSSION AND EVALUATION:

i) UEFI VS BIOS

BIOS is widely used throughout the world instead of UEFI and major reason is lack of knowledge among people.

ii) DESIGN WISE:

In BIOS we cannot use mouse at all while in UEFI we have the freedom of using mouse because it is optimized for the pointing device.

BIOS page looks more or same to that of a QBASICS or TURBOC++ design while the design of UEFI can be made dynamic by adding animations which is only limited till adding images in the BIOS.

iii) MEMORY:

BIOS uses the MBR (Master Boot Recorder) system for partitioning of data while UEFI uses GUID partitioning table. So now let’s see what these are and why do we need them?

So MBR portioning restricts us to use a hard-disk of size 2TB. So, if we insert a hard-disk of size greater than 2TB then it will only count the space of 2TB and the rest will be wasted. While the GUID can read memory up to 7 zeta bytes (7*1024 TB) making it the future of next booting system.

Now as we have seen about the portioning size, now let’s see about no. of partitions. So just imagine that you have a hard disk of 4TB and you managed to get GUID on your legacy mode but you want to make a partition drives of music, movies, games, documents, OS and various other things but you got to know that you can have maximum of 4 partitions. Now in this scenario UEFI saves your day because it allows you to have 128 different partitions.

BACKUP’S MEMORY: The UEFI is vested with a great functionality. It creates two copies of the same data, one at the beginning of the disk and another at the end. If the one data gets corrupt then it automatically retrieves the data from the backup. This is the biggest plus point of UEFI.

iv) SPEED AND PERFORMANCE: -

Since UEFI is stage free, it might have the capacity to upgrade the boot time and speed of the PC. This is particularly the situation when you have extensive hard drives introduced in your PC. This improvement relies on how UEFI is designed to run. UEFI can perform better while introducing the equipment gadgets. Regularly this speed improvement is a small amount of the aggregate boot time, so you won't see a colossal distinction in general boot time. Designers can make utilization of UEFI shell condition which can execute order from other UEFI applications improving the execution of the framework further.

(FIRMWARE: A low- level software that provides control over the system hardware. There may be different types of firmwares.)

MALWARES IN FIRMWARE:

Initially in olden days when such malwares or codes written for criminal purposes were used, software developers improved their capacity of increasing the ability to defend such attacks. So, attackers had targeted the firmware in order to do their unfair activities. They started focusing on the time space between firmware and the OS start. Such kind of attacks in this time space is usually referred as “boot kit” or “rootkit” attacks.

Rootkit attack:

It’s a collection of softwares which are intentionally created to harm or cause a damage to computer. An attacker can either directly insert the rootkit into the computer (This can be a result of direct attack to the computer like getting the password by false means etc) or can be automated. Once a rootkit is installed in the computer it’s very difficult to detect even the intrusion of rootkit as it has control over the system software and hence can even manage the system software such that its intrusion is not detected.

Once if the malware is injected into the system, it gets direct access to the hardware without the knowledge of the user or the OS. It’s practically not possible to directly detect the malware in the firmware unless a search is performed which targets the malware.

Sometimes the malware may directly settle in the ROM which can’t be removed even by the reinstalling of OS or swapping the hard drive.

Firmware rootkits inject exploit code into the system, either by fixing or substituting the default firmware image. Boot-kits inject malicious code at the purpose wherever the microcode hands management over to the operating system, usually by modifying the operating system bootloader package. Rootkits and Boot-kits use numerous ways to avoid detection, typically targeting firmware as a result of which it's liable for loading the operating system kernel.

UEFI’S SPECIFICATIONS FOR BOOTING:

UEFI’s digital signature method to secure the booting process:

As mentioned above the malware creators started focusing the booting process for the malware injection it’s necessary to secure the booting process by some means. BIOS has been subjected to numerous malware attacks as it doesn’t employ any boot securing procedures.

The main concept here to secure the booting process is to avoid the execution of compromised booting code, by which the malware entry can be avoided (i.e injection of malware implies that there has been some change in the boot code or it can be said that the boot code has been compromised). So, by avoiding the execution of compromised code one can stop the injection of malware into the system and also the control of malware over OS can be avoided.

One of the techniques that UEFI follows to secure the booting process is through digital signatures. In this technique every executable part is embedded with a digital signature signed by a trusted code creator. A digital signature is basically hash of the code to which the sign is to be embedded. In order to create the digital signature, the creator may use any of the cryptographic techniques like public/private key cryptography. Once the sign has been embedded, during execution the code is converted to the hash using public or apt key and compared to the sign embedded. If the code has been compromised the hash obtained at the execution time and the embedded sign won’t match and hence the code is either not allowed to execute. At this point the system may take an alternate booting path or prompt the user for further actions. It is vital to notice that a compromised system is often not allowed to finish the bootstrap method in a compromised state.

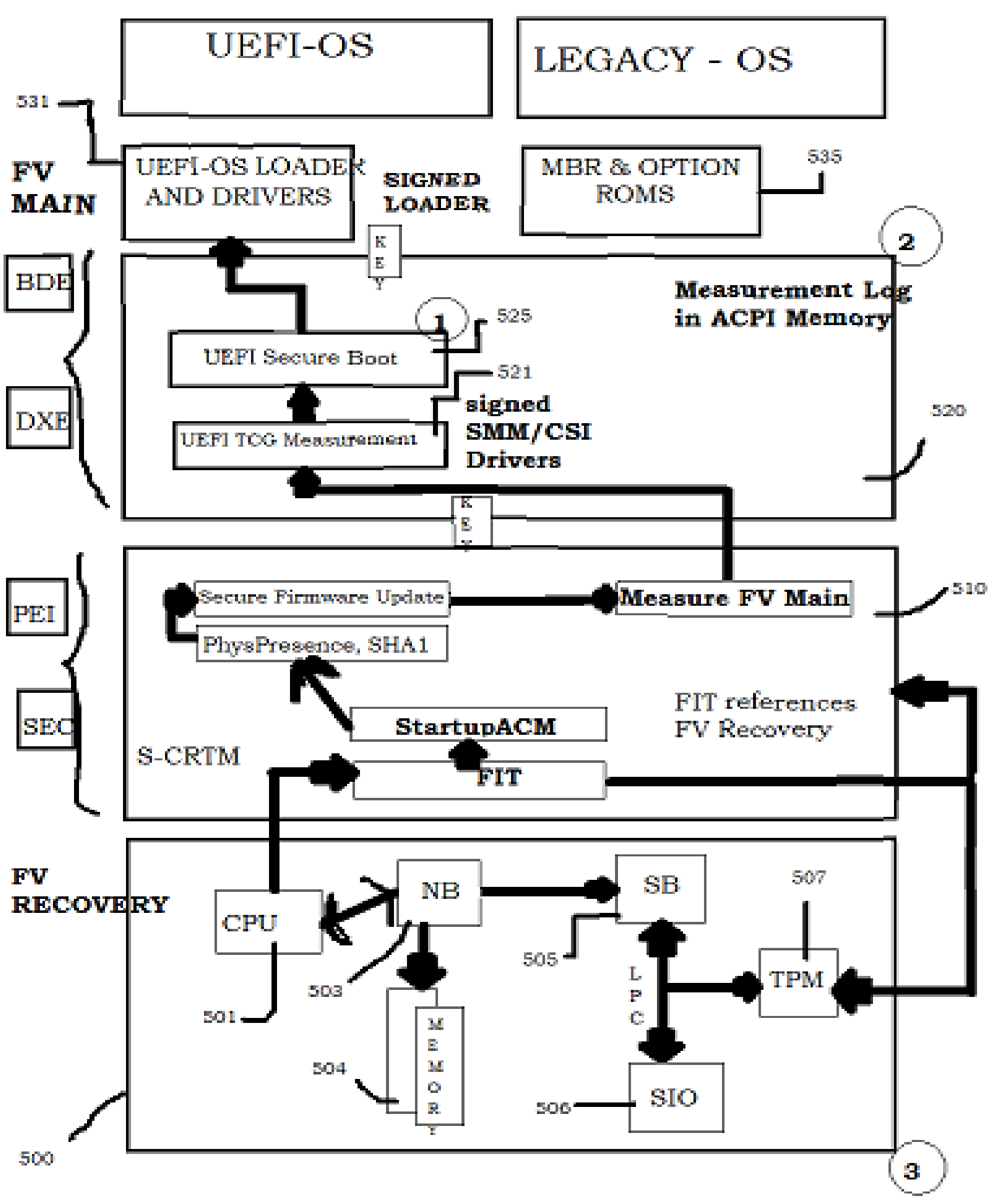
SYSTEM METHOD TO SECURE BOOT BOTH UEFI AND LEGACY OPTION ROMS

WITH COMMON POLICY ENGINE:

An embodiment of the present invention relates generally to booting a platform and, more specifically, to protecting against malware in third party drivers and executables using a policy engine to ensure that the images are authenticated. Various mechanisms exist for checking platform status. In some existing systems, the Trusted Platform Module (TPM) and the techniques promulgated by the Trusted Computing Group entail the use of the TPM as a Root-of-Trust for Storage (RTS) and Reporting (RTR) via the Platform Configuration Registers (PCRs) and Storage Root Key (SRK), respectively. The TPM is a passive piece of hardware. The platform firmware (or microcode) is the Root of Trust for Measurement (RTM). The unified extensible firmware interface (UEFI). Secure Boot adds a Root of Trust for Enforcement of Validation (RTE/RTV), which enables the “Secure Boot.” However, the TPM merely records the status, and on its own does not provide a method for ensuring boot integrity. Currently, there is only standardization of measured boot, e.g., record but run the image regardless of the status. This scheme is akin to auditing from a security perspective, rather than protection. From a product perspective, it may be acceptable, because a challenger can assess the security posture. However, from a malware perspective, this scheme is unacceptable since the malware was “measured and run.” Once the malware runs, even if it is later detectable, the damage has been done. Thus, there is a need to proactively prohibit the execution of unauthorized code.

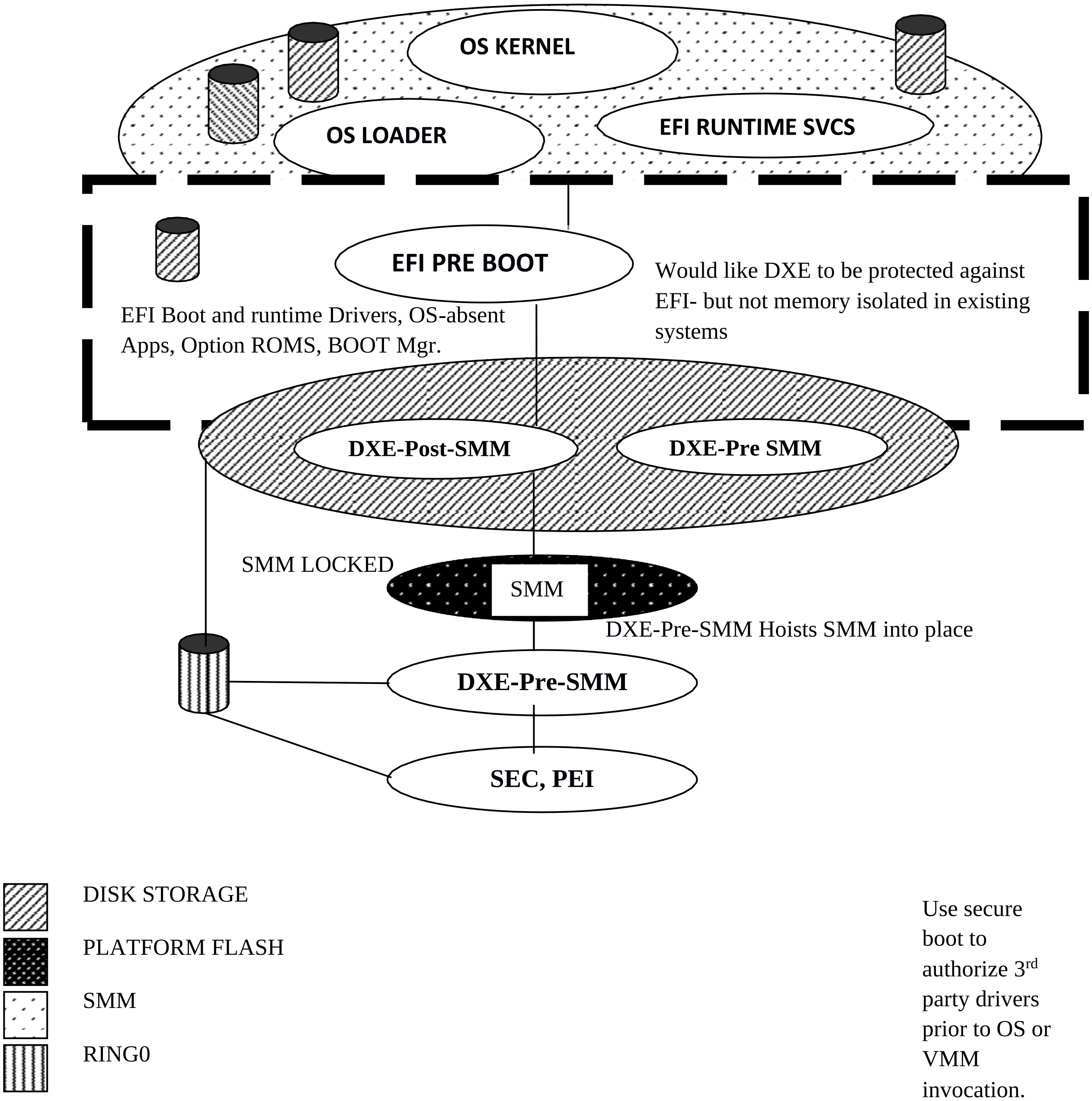
IV) WORKING LAYOUT OF UEFI (FV RECOVERY SECTION)

FV recovery it checks mostly about the hardware components of the system and make sure that all data for startup is recovered. The main difference between the UEFI and legacy mode is the UEFI loader and drivers in UEFI and MBR in Legacy boot mode.



1. Measured Boot
2. Secure Boot

3. FIT Boot



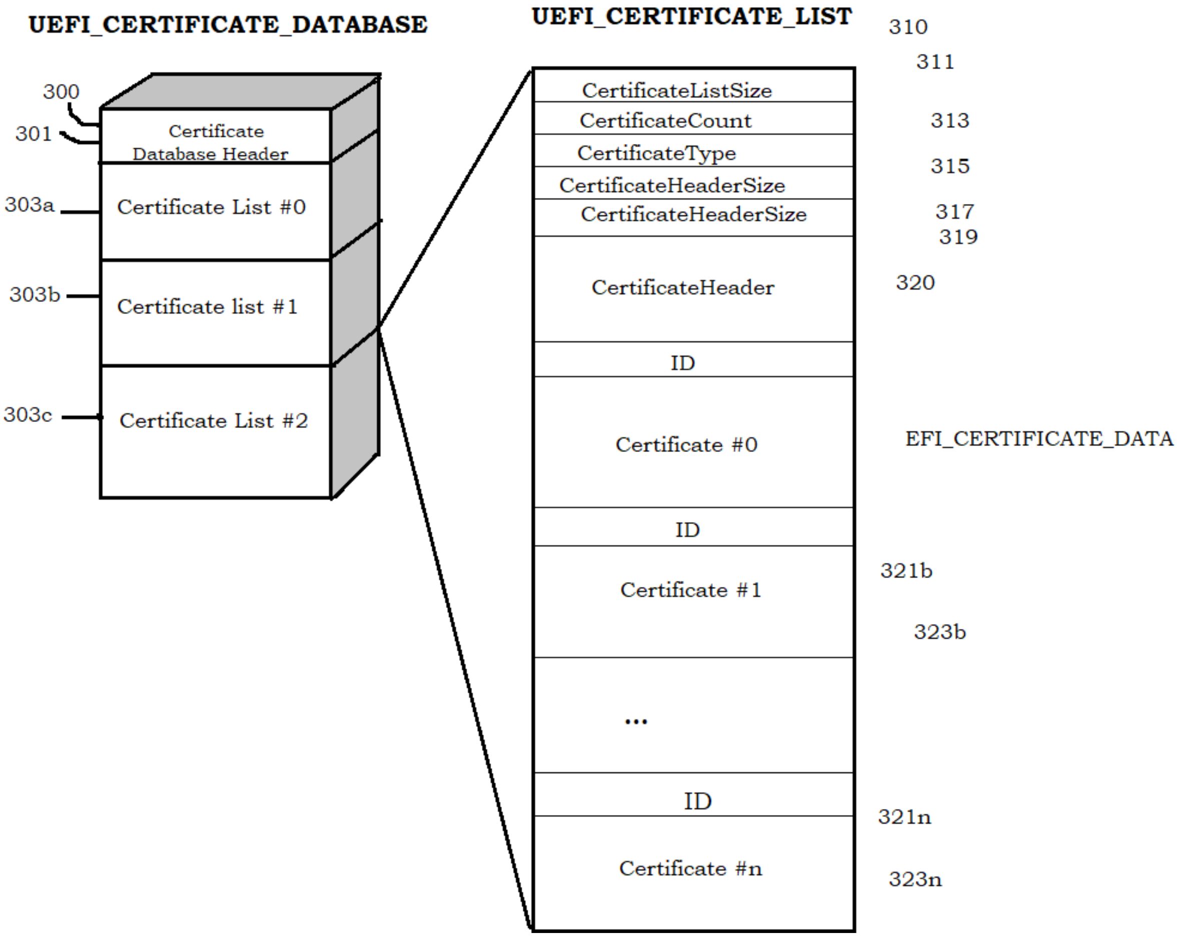
EFI Boot and runtime Drivers, OS-absent Apps, Option ROMS, BOOT Mgr.

Would like DXE to be protected against EFI- but not memory isolated in existing systems

DXE-Pre-SMM Hoists SMM into place

Use secure boot to authorize 3rd party drivers prior to OS or VMM invocation.

Each time if the third-party application needs permission to enter our system then it has to pass the secure boot feature which has the power to authorize any incoming file. This feature helps to stop us from getting attacked by any outside malware. Each time during loading, a key is to be generated which allows secure boot. This key cannot be seen by the user as it is completely system governed process and if there’s any malware attack then this key is not generated until this process is not resolved.

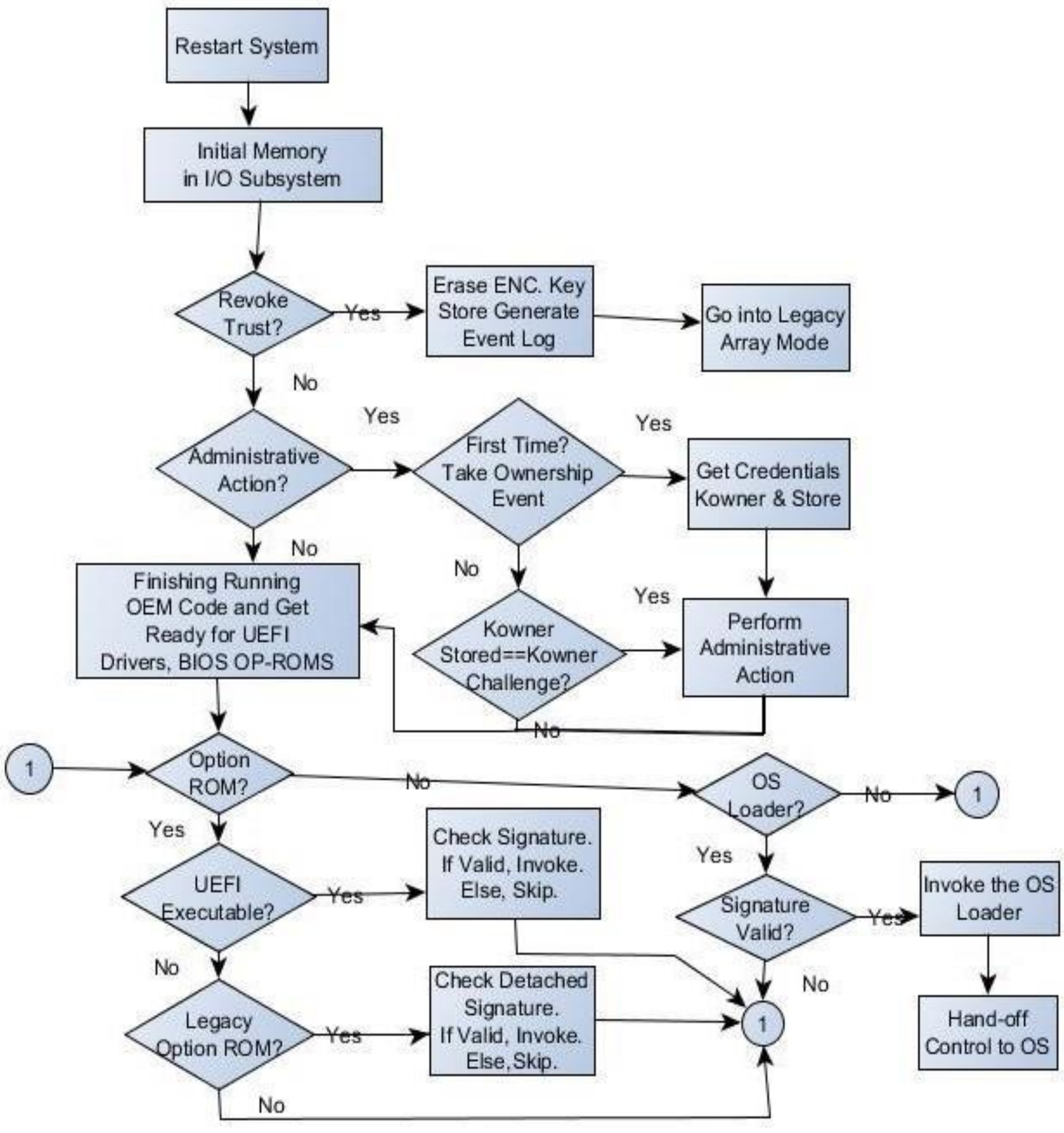


UEFI has a very classified database which ensures that each Certificate list has all the details contained inside it in a unified manner. UEFI certificate database contains the main certificate header which is similar to the address/label followed by the blocks of memory named as Certificate list #x. This list has various information which is shown in the above diagram.

V) ALGORITTMS FOR IMPLEMENTATION OF UEFI_CERTIFICATE_DATABASE:

```
Typedef struct_EFI_CERTIFICATE_DATABASE
{
VINT32 DatabaseSize;
VINT32 CertificateListCount;
VINT8 CertificateListDate[ANYSIZE];
} EFI_CERTIFICATE_DATEBASE;
Typedef struct_EFI_CERTIFICATE_LIST
{
VINT32 CertificateListSize;
VINT32 CertificateCount;
EFI_GUID CertificateType;
VINT32 CertificateHeaderSize;
VINT32 CertificateSize;
//vint8 CertificateHeader[CertificateHeaderSize];
//VINT Certificate[...][CertificateSize];
} EFI_certificate_list;
Typedef struct_EFI_CERTIFICATE_DATA
{
EEFI_GUID ID;
VINT8 Data[ANYSIZE];
}EFI_CERTIFICATE_DATA
```

FLOW CHART

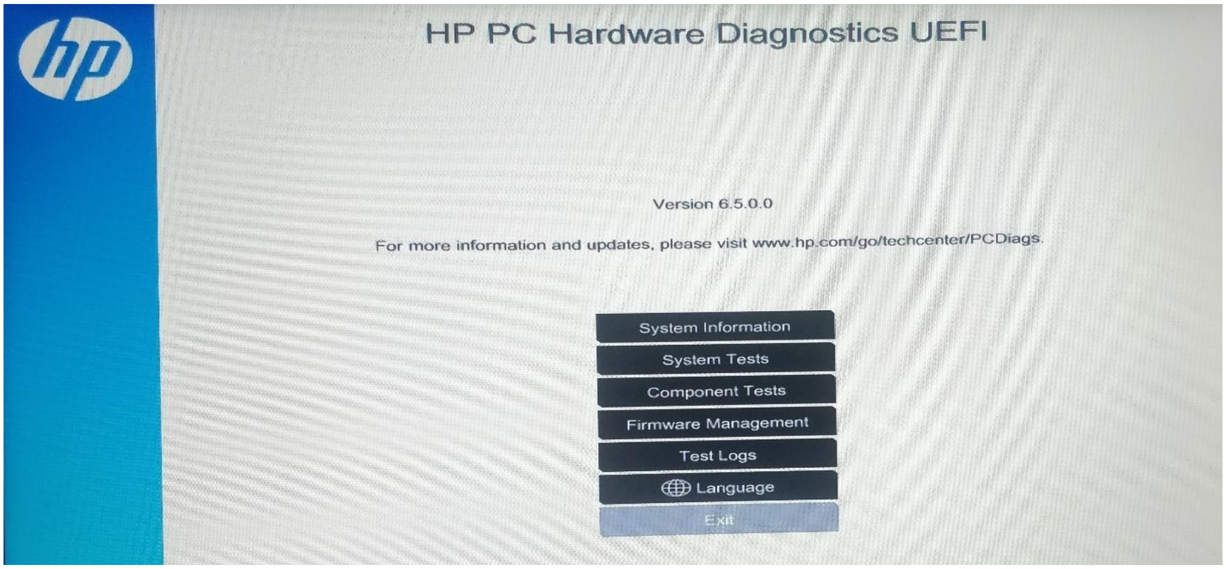

Restart System
Initial Memory in I/O Subsystem
Revoke Trust?
Yes
Erase ENC. Key Store Generate Event Log
Go into Legacy Array Mode
No
Yes
Administrative Action?
First Time? Take Ownership Event
Yes
Get Credentials Kowner & Store
No
No
Finishing Running OEM Code and Get Ready for UEFI Drivers, BIOS OP-ROMS
Yes
Kowner Stored==Kowner Challenge?
Perform Administrative Action
No
1
Option ROM?
No
OS Loader?
No
1
Yes
Check Signature. If Valid, Invoke. Else, Skip.
Yes
UEFI Executable?
Yes
Signature Valid?
Yes
Invoke the OS Loader
No
No
Check Detached Signature. If Valid, Invoke. Else,Skip.
Legacy Option ROM?
Yes
1
Hand-off Control to OS
No

VI) RESULTS:

Booting process of both BIOS and UEFI have been used and the following results and conclusions were drawn:

i) INTERFACING OF UEFI:

UEFI provides a graphical user interface for its boot manager which simplifies the job of user.



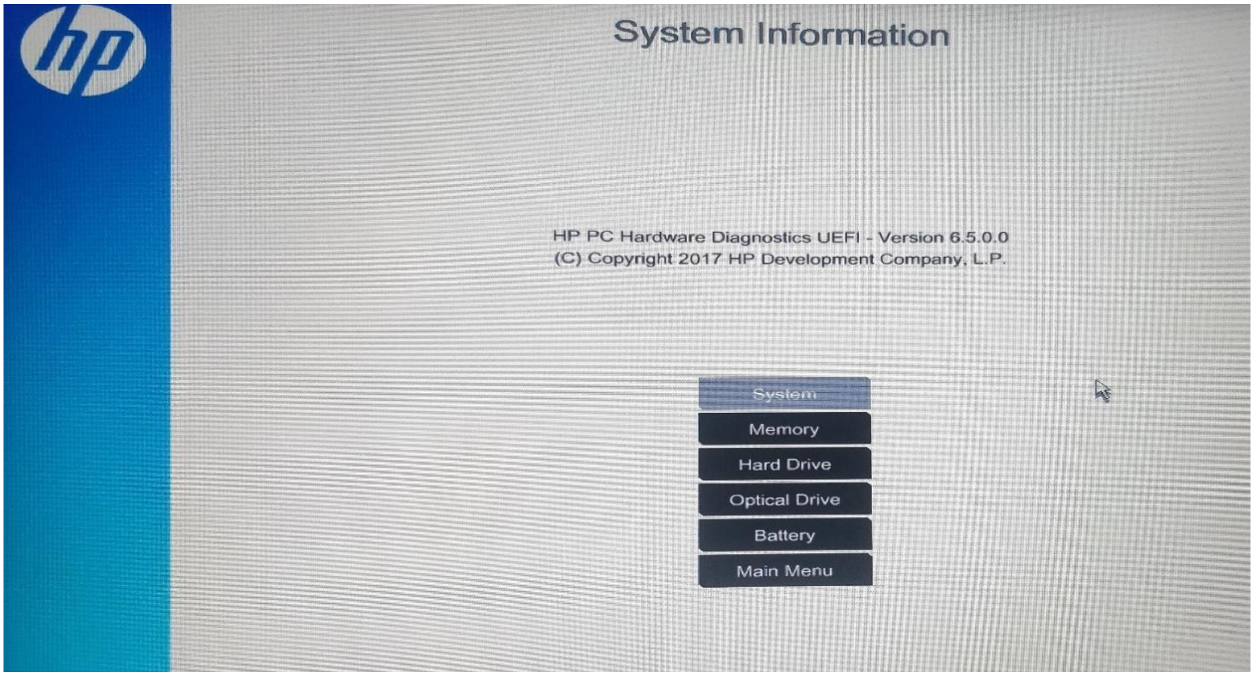
HP PC Hardware Diagnostics UEFI

Version 6.5.0.0

For more information and updates, please visit www.hp.com/go/techcenter/PCDiags.

ii) MOUSE POINTER:

UEFI provides mouse pointer option which is not available in BIOS.



System Information

HP PC Hardware Diagnostics UEFI - Version 6.5.0.0
(C) Copyright 2017 HP Development Company, L.P.

PROPERTIES	SPECIFICATION
Model	HP Pavilion Notebook
System ID	8216
Product ID	Z4Q39PA#ACJ
Born on Date	07/21/2017
Processor Type	Intel(R) Core™ i5_7200U CPU@2.50GHZ
Current processor speed	2400 MHz
Memory size	8129 MB RAM
BIOS Date	12/12/2016
BIOS Revision	F.25
Serial Number	5CD712943C
Keyboard Controller Revision	83.14
Operating System Image	16WW3DRT602#SACJ#DACJ

iii) SYSTEM INFORMATION

iv) MEMORY INFORMATION

PROPERTIES	SPECIFICATION
DIMM: Device Locator Not installed	Bottom-slot 1(left)

DIMM: Device Locator	Bottom-slot 2(right)
Manufacture	A-DATA
Serial Number	CB720200
Part Number	A01P24HC8T1-BQXS
Memory Size	8129 MB
Maximum Memory Speed	2133 MHz
Memory Clock Speed	2133 MHz
Memory Type	DDR4
Type Detail	Synchronous

v) MEMORY INFORMATION

PROPERTIES	SPECIFICATION
DIMM: Device Locator Not installed	Bottom-slot 1(left)

DIMM: Device Locator	Bottom-slot 2(right)
Manufacture	A-DATA
Serial Number	CB720200
Part Number	A01P24HC8T1-BQXS
Memory Size	8129 MB
Maximum Memory Speed	2133 MHz

Memory Clock Speed	2133 MHz
Memory Type	DDR4
Type Detail	Synchronous

vi) HARD DRIVE INFORMATION

PROPERTIES	**SPECIFICATION**
HDD1: Type	ATA
Model	WDC WD10JPVX-60JC3T0
Firmware, Version	01.01A01
Serial Number	WD-WXK1AC6H6843
Capacity	1000 GB
LBA48	Supported
SMART	Enabled
Sector Type	4k/512e

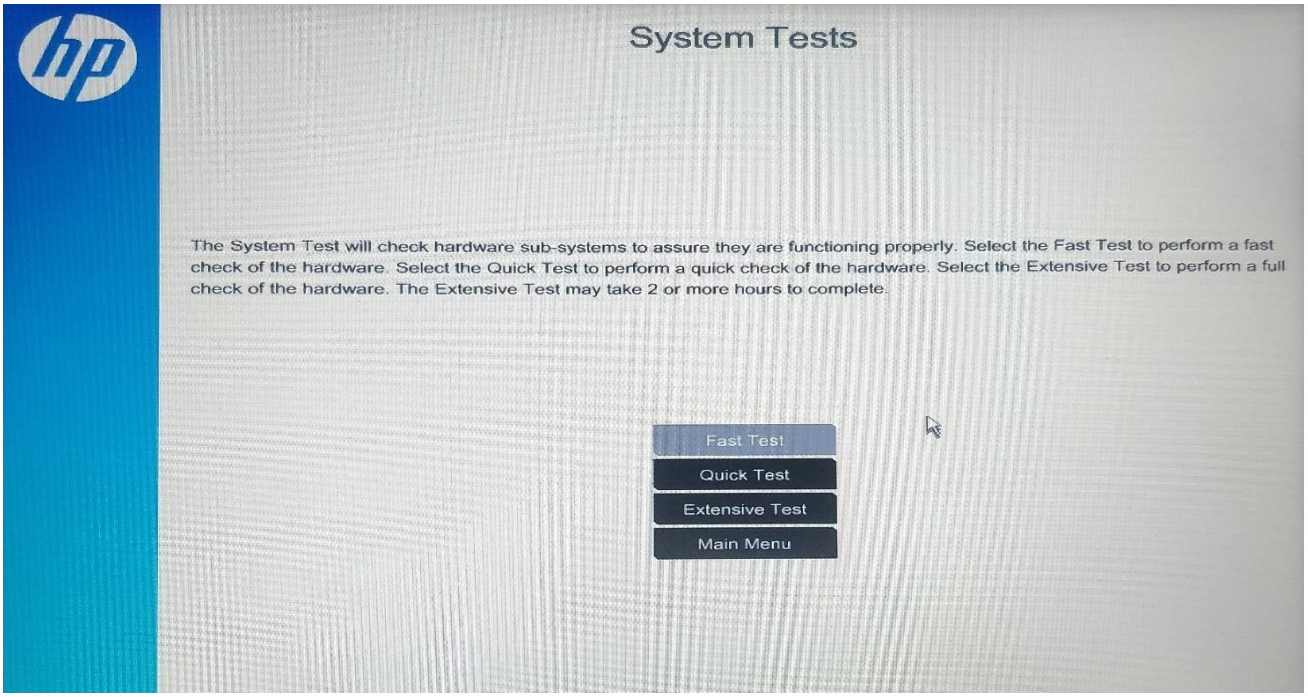
vii) OPTICAL DRIVE INFORMATION

PROPERTIES	**SPECIFICATION**
ODD 1: Type	ATA
Model	hp DVDRW GUE1N
Firmware Version	UE00
Serial Number	KL5H2J31515
Read Support	CD.DVD
Write Support	CD.DVD

viii) BATTERY INFORMATION

PROPERTIES	**SPECIFICATION**
Battery1: Location	PRIMARY
Device Name	BP02041
Manufacture	313-54-31
Serial Number	01275 02/05/2017
Capacity	41195 m.Hour
Voltage	7700 mV
Chemistry	LION

ix) SYSTEM TESTS:

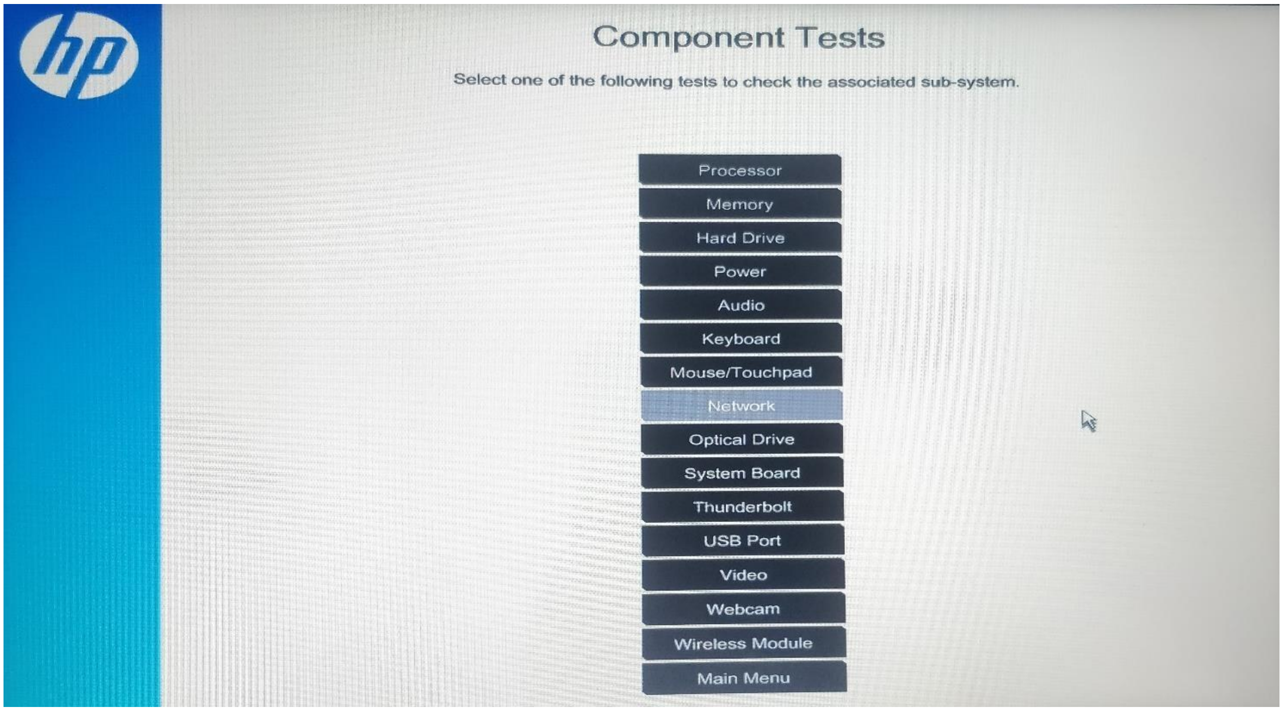

System Tests

The System Test will check hardware sub-systems to assure they are functioning properly. Select the Fast Test to perform a fast check of the hardware. Select the Quick Test to perform a quick check of the hardware. Select the Extensive Test to perform a full check of the hardware. The Extensive Test may take 2 or more hours to complete.

a) COMPONENT TEST:

In UEFI there is a specification which allows us to test the hardware components individually. This allows us to identify the component which is not functioning properly and can be rectified.

Where as in BIOS the boot loader the hardware test is not component specific. It only identifies the presence of a failure in functionality of hardware but not the component in which failure is identified.



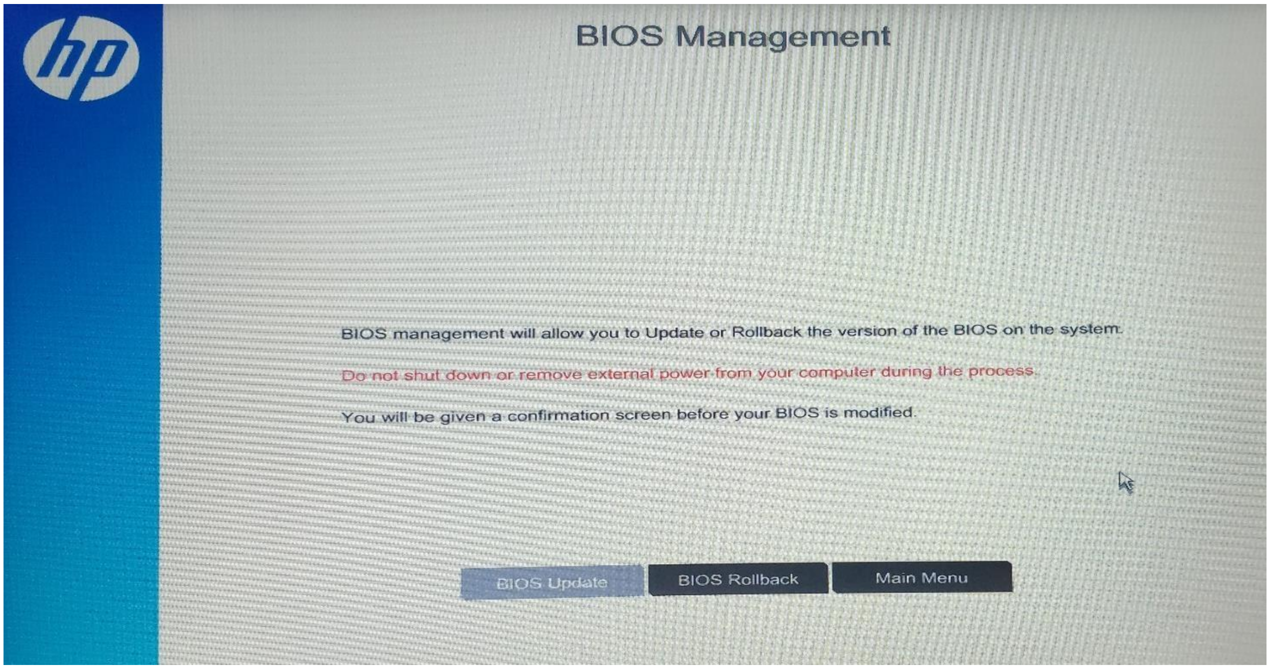
Component Tests

Select one of the following tests to check the associated sub-system.

x) BACKWARD COMPATIBILITY:

As discussed earlier, any system that employees UEFI can be converted to BIOS any time. Whereas systems that support BIOS and not UEFI can’t be converted to UEFI without any additional hardware support.

This feature of UEFI is called **“Backward Compatibility”**.

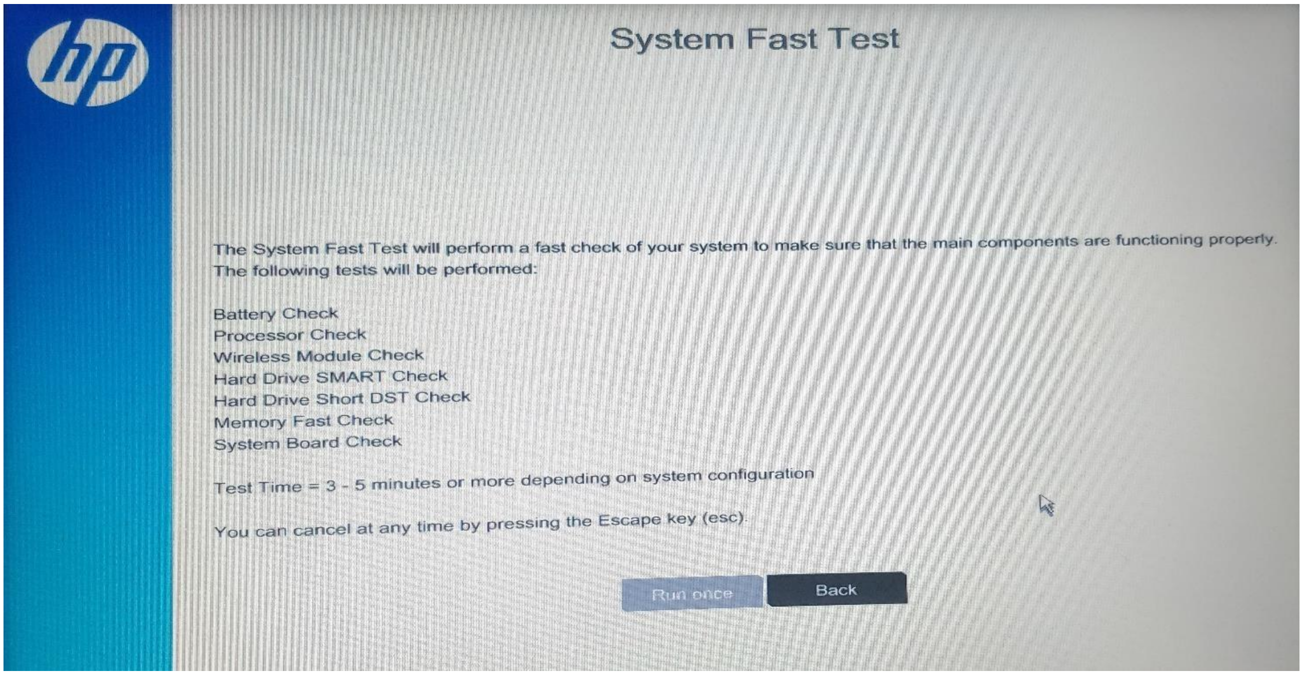


BIOS Management

BIOS management will allow you to Update or Rollback the version of the BIOS on the system.

Do not shut down or remove external power from your computer during the process.

You will be given a confirmation screen before your BIOS is modified.



System Fast Test

The System Fast Test will perform a fast check of your system to make sure that the main components are functioning properly.
The following tests will be performed:

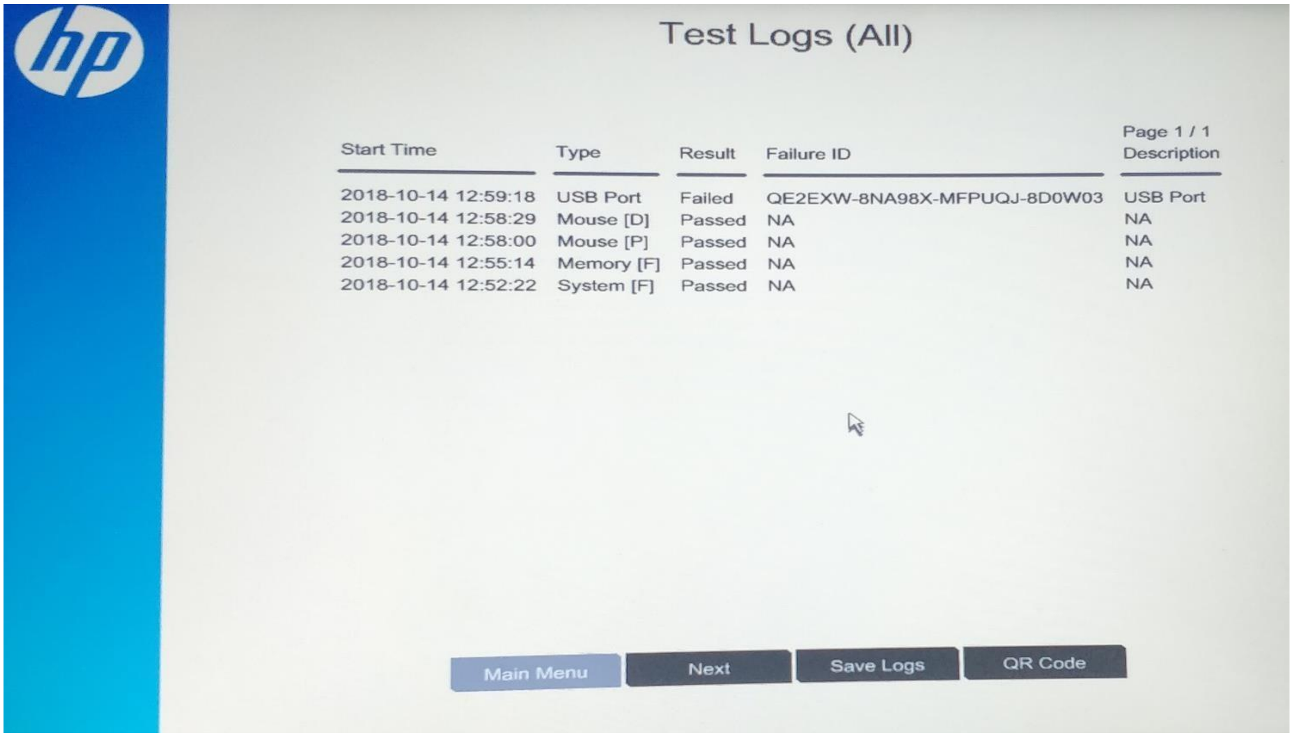
Battery Check
Processor Check
Wireless Module Check
Hard Drive SMART Check
Hard Drive Short DST Check
Memory Fast Check
System Board Check

Test Time = 3 - 5 minutes or more depending on system configuration

You can cancel at any time by pressing the Escape key (esc).

xi) TEST LOGS:

UEFI gives the test logs as a summary to easily find the error.

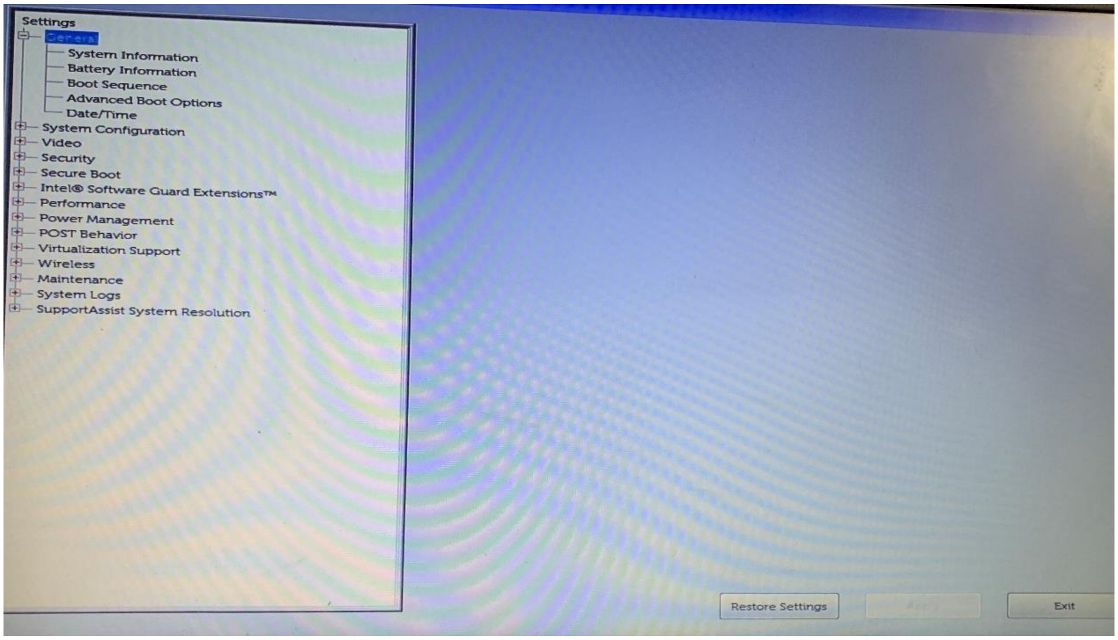


Test Logs (All)

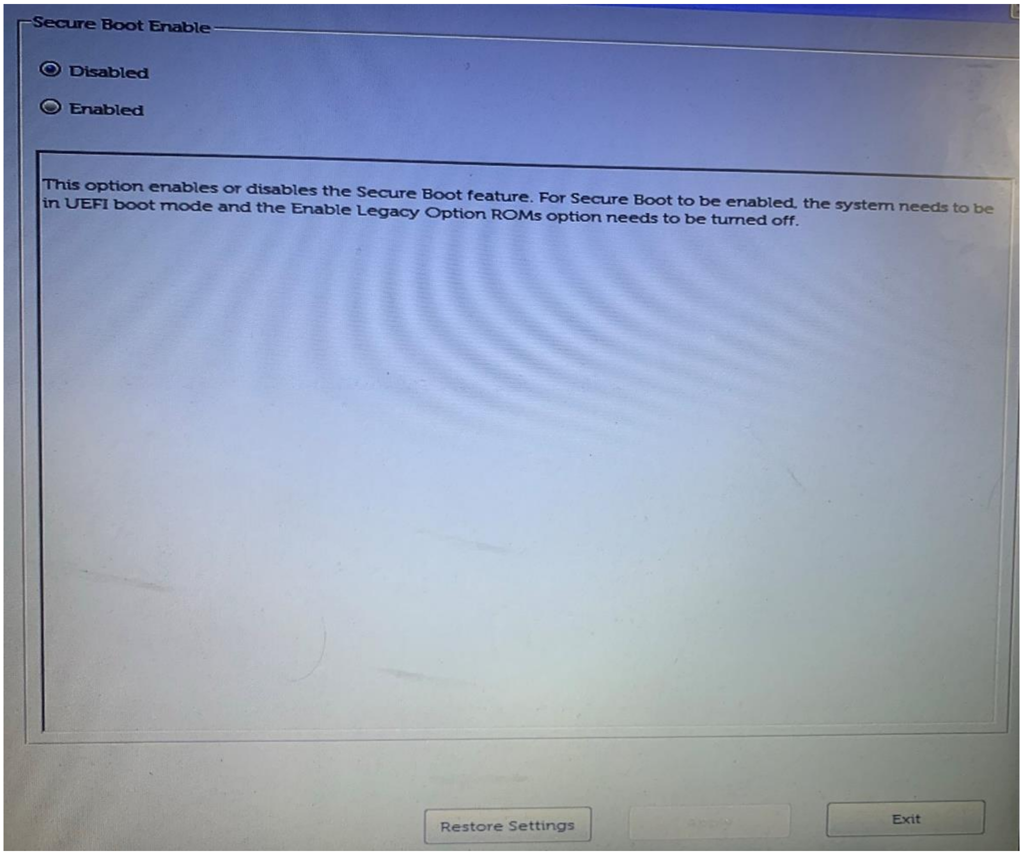
Page 1 / 1

Start Time	Type	Result	Failure ID	Description
2018-10-14 12:59:18	USB Port	Failed	QE2EXW-8NA98X-MFPUQJ-8D0W03	USB Port
2018-10-14 12:58:29	Mouse [D]	Passed	NA	NA
2018-10-14 12:58:00	Mouse [P]	Passed	NA	NA
2018-10-14 12:55:14	Memory [F]	Passed	NA	NA
2018-10-14 12:52:22	System [F]	Passed	NA	NA

BIOS BOOT INTERFACE:



System needs to support UEFI in order to have secure boot



Secure Boot Enable

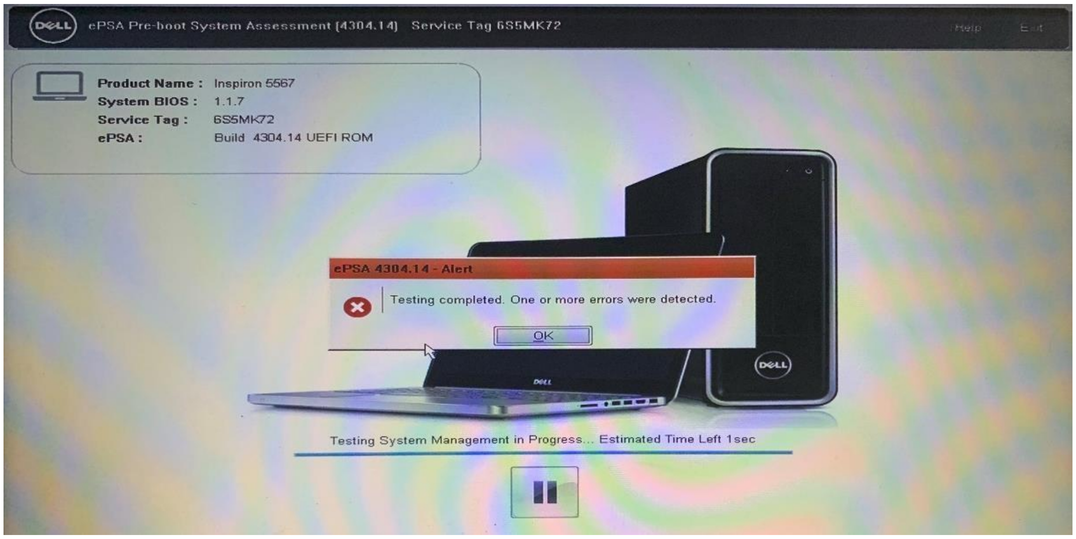
● Disabled

○ Enabled

This option enables or disables the Secure Boot feature. For Secure Boot to be enabled, the system needs to be in UEFI boot mode and the Enable Legacy Option ROMs option needs to be turned off.

i) HARDWARE TESTING IN BIOS:

It doesn’t give any result specific to component.



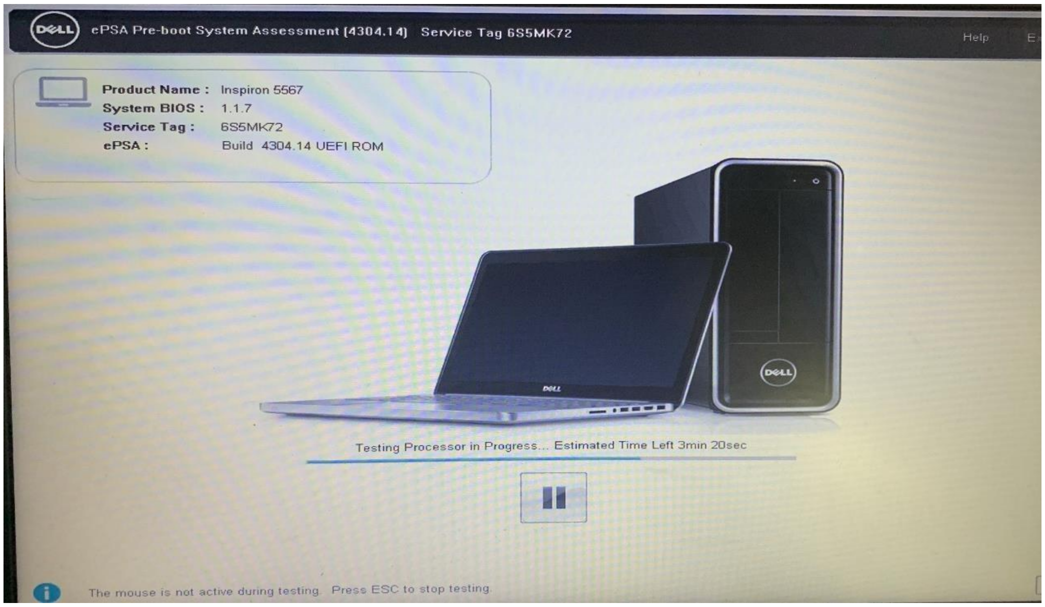
ePSA Pre-boot System Assessment [4304.14]   Service Tag 6S5MK72

Product Name : Inspiron 5567
System BIOS : 1.1.7
Service Tag : 6S5MK72
ePSA : Build 4304.14 UEFI ROM

ePSA 4304.14 - Alert

Testing completed. One or more errors were detected.

Testing System Management in Progress... Estimated Time Left 1sec



ePSA Pre-boot System Assessment [4304.14]   Service Tag 6S5MK72

Product Name : Inspiron 5567
System BIOS : 1.1.7
Service Tag : 6S5MK72
ePSA : Build 4304.14 UEFI ROM

Testing Processor in Progress... Estimated Time Left 3min 20sec

The mouse is not active during testing. Press ESC to stop testing.

VII) CONCLUSION: -

Let’s start with the type of memory used by the UEFI mode. It uses the GUID Partition Table (GPT) which has a better partitioning technique than the MBR (Master Boot Reader) technique used by LEGACY as GPT provides us with file recovery benefits by making a copy of the data at the end partition of the hard-disk, in case the data gets corrupt then we can get back the data from it. This is not there in LEGACY. In design part, UEFI again beats the LEGACY mode. This was obvious because UEFI was built years after DOS and thus had a better technological advancement in that field. All the layouts of the UEFI have privileges of using the mouse cursor which LEGACY mode can use it only at some places. Now let’s focus on the major thing that is the secure boot feature provided by the UEFI mode. This feature alone handily takes down the old LEGACY boot mode. The secure boot in UEFI checks the digital signature appended with the executable parts of the OS code with the hash generated by the UEFI during booting. This process continues until the operating system is completely started. UEFI security features are designed to prevent boot-kits (malware) from being installed. Now let’s move to the hardware checking procedure in which LEGACY mode diagnose the whole system at once and does not specify the error as shown it pictures above while in UEFI one can find that each hardware component is checked separately. Thus, we can understand what to fix. If it just says something is wrong then it’s of no use. UEFI has a much-classified database which ensures that each Certificate list has all the details contained inside it in a unified manner.

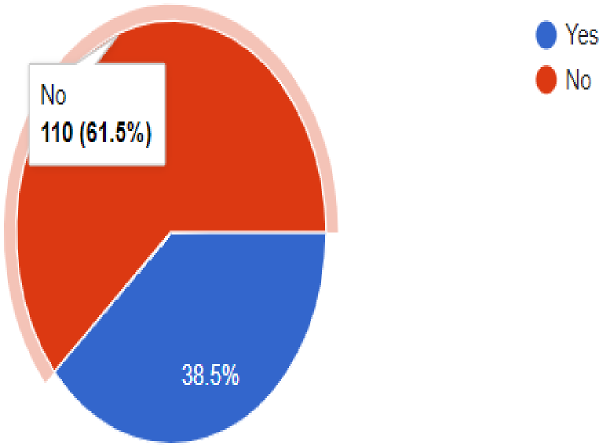
REFERENCES

- J.-F. Agneessens. (2012, Analysis of the building blocks and attack vectors associated with the Unified Extensible Firmware Interface (UEFI). Available: https://www.sans.org/reading_room/whitepapers/services/analysis-building-blocks-attack-vectors-unified-extensible-firmware_34215.
- UEFI, "Unified Extensible Firmware Interface Specification, Version 2.3.1c," ed, 2011.
- P. P. Swire, "A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Agencies," *Houston Law Review*, vol. 42, January 2006.
- U.S. PATENT DOCUMENTS
  5,421,006 A 5, 1995 Jablon et al.
  5,919,257 A 7, 1999 Trostle
  6,401.208 B2 * 6/2002 Davis et al. T13, 193
  6,463,535 B1 * 10/2002 Drews............................713, 176

SURVEY ON UEFI

Opinion of VIT students

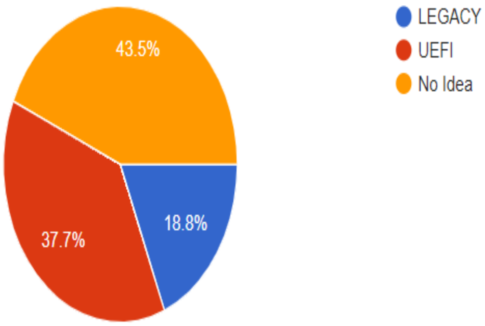
- **Have you ever re-installed an OS in your PC?**



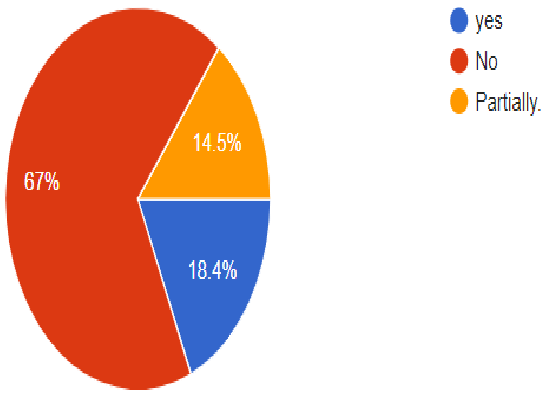
IF “YES”

- **In which mode have you re-installed it?**

A shocking result again because 44% people have no idea about it.

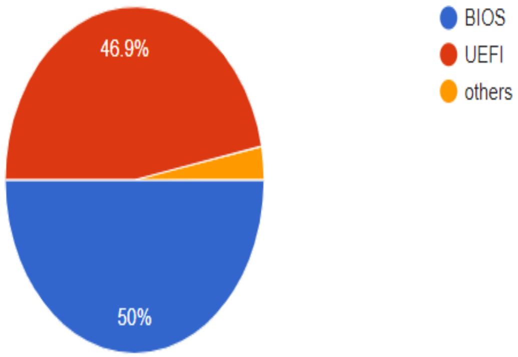


- **Do You know what UEFI is?**
  This was the response



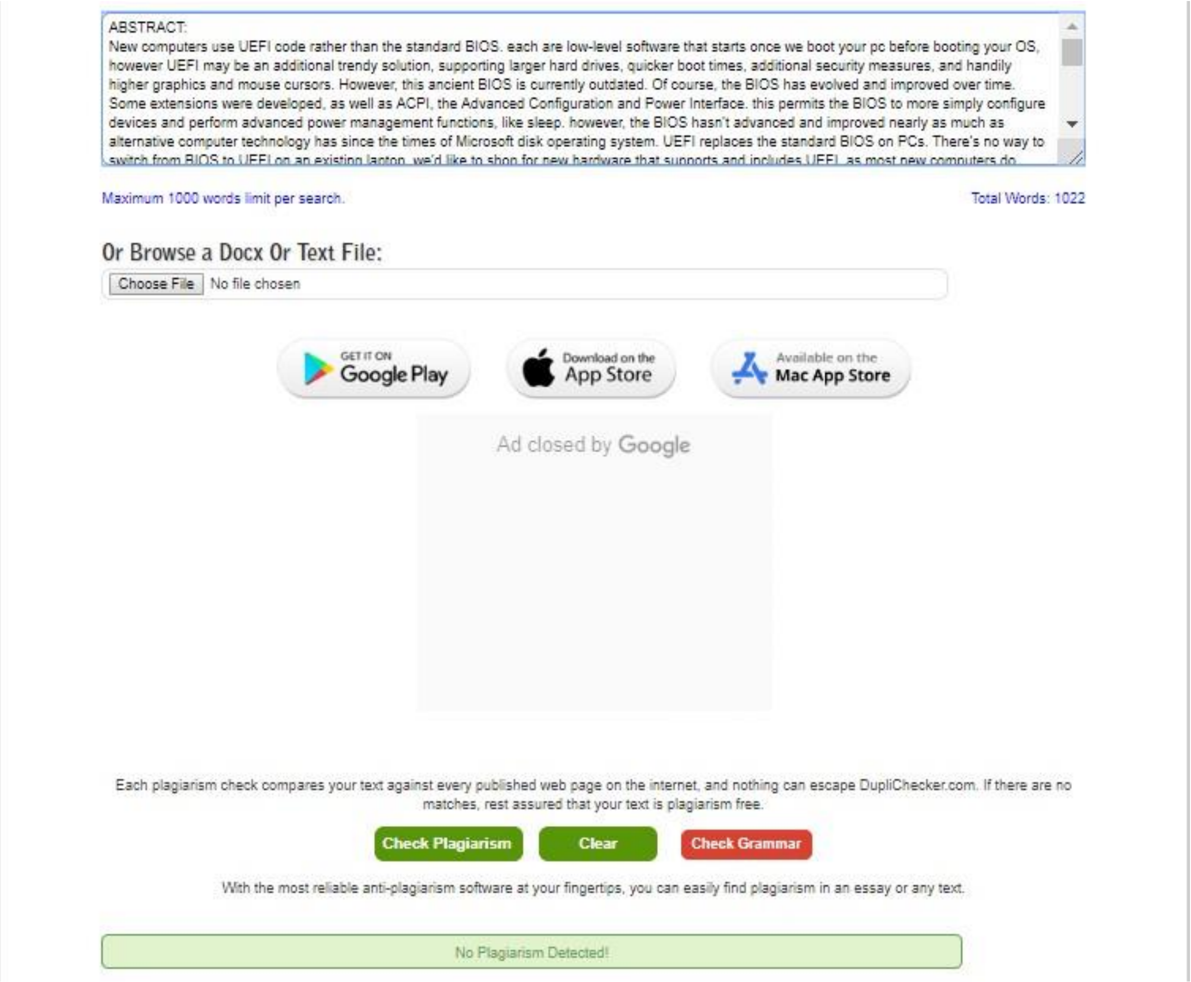
IF "YES"

- **Which firmware interface does your PC have?**



Even after knowing about UEFI and its benefits, 50% people are still going for BIOS.

PAGE 1-4:



ABSTRACT:
New computers use UEFI code rather than the standard BIOS. each are low-level software that starts once we boot your pc before booting your OS, however UEFI may be an additional trendy solution, supporting larger hard drives, quicker boot times, additional security measures, and handily higher graphics and mouse cursors. However, this ancient BIOS is currently outdated. Of course, the BIOS has evolved and improved over time. Some extensions were developed, as well as ACPI, the Advanced Configuration and Power Interface. this permits the BIOS to more simply configure devices and perform advanced power management functions, like sleep. however, the BIOS hasn't advanced and improved nearly as much as alternative computer technology has since the times of Microsoft disk operating system. UEFI replaces the standard BIOS on PCs. There's no way to switch from BIOS to UEFI on an existing laptop. we'd like to shop for new hardware that supports and includes UEFI, as most new computers do

Maximum 1000 words limit per search.

Total Words: 1022

Or Browse a Docx Or Text File:

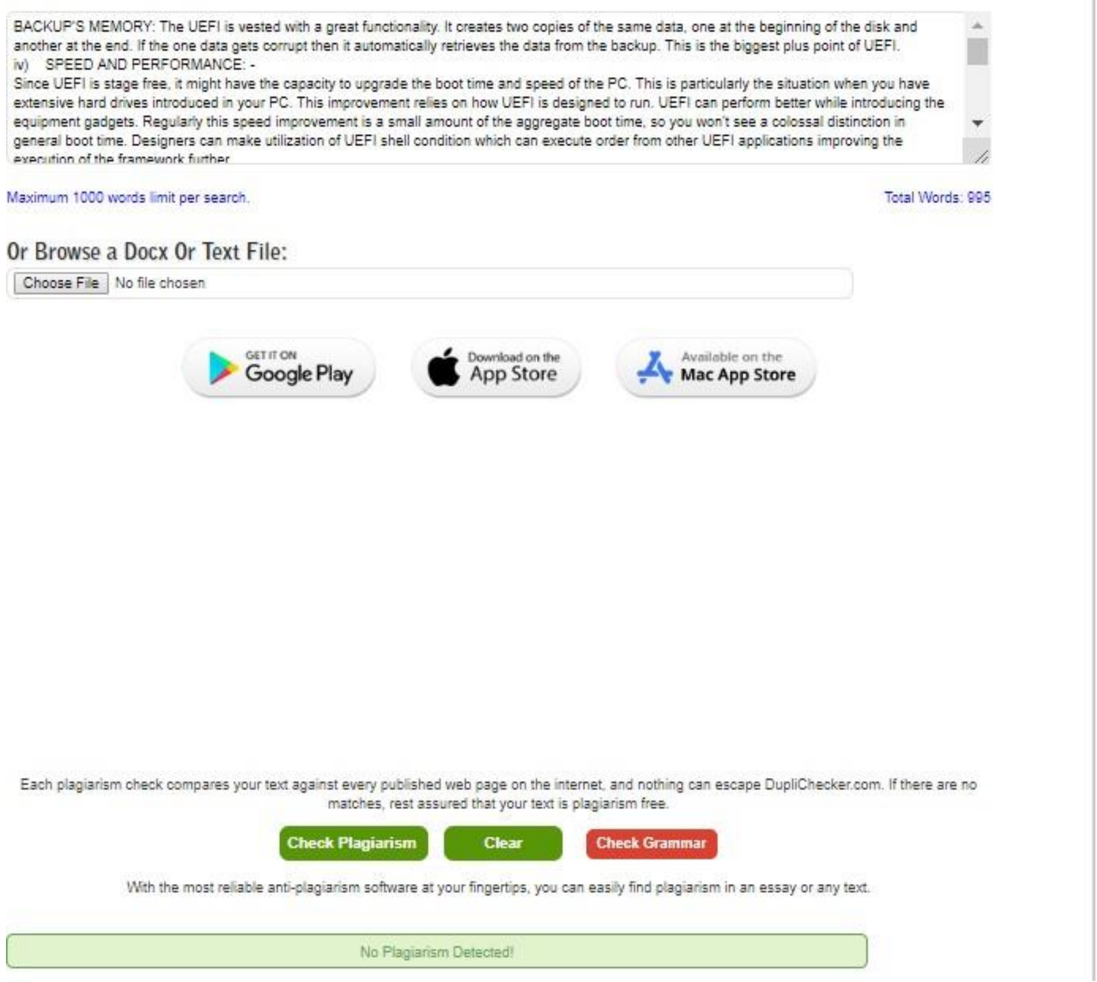
Choose File No file chosen

Each plagiarism check compares your text against every published web page on the internet, and nothing can escape DupliChecker.com. If there are no matches, rest assured that your text is plagiarism free.

With the most reliable anti-plagiarism software at your fingertips, you can easily find plagiarism in an essay or any text.

No Plagiarism Detected!

PAGE 4,5:



BACKUP'S MEMORY: The UEFI is vested with a great functionality. It creates two copies of the same data, one at the beginning of the disk and another at the end. If the one data gets corrupt then it automatically retrieves the data from the backup. This is the biggest plus point of UEFI.
iv) SPEED AND PERFORMANCE: -
Since UEFI is stage free, it might have the capacity to upgrade the boot time and speed of the PC. This is particularly the situation when you have extensive hard drives introduced in your PC. This improvement relies on how UEFI is designed to run. UEFI can perform better while introducing the equipment gadgets. Regularly this speed improvement is a small amount of the aggregate boot time, so you won't see a colossal distinction in general boot time. Designers can make utilization of UEFI shell condition which can execute order from other UEFI applications improving the execution of the framework further

Maximum 1000 words limit per search.

Total Words: 995

Or Browse a Docx Or Text File:

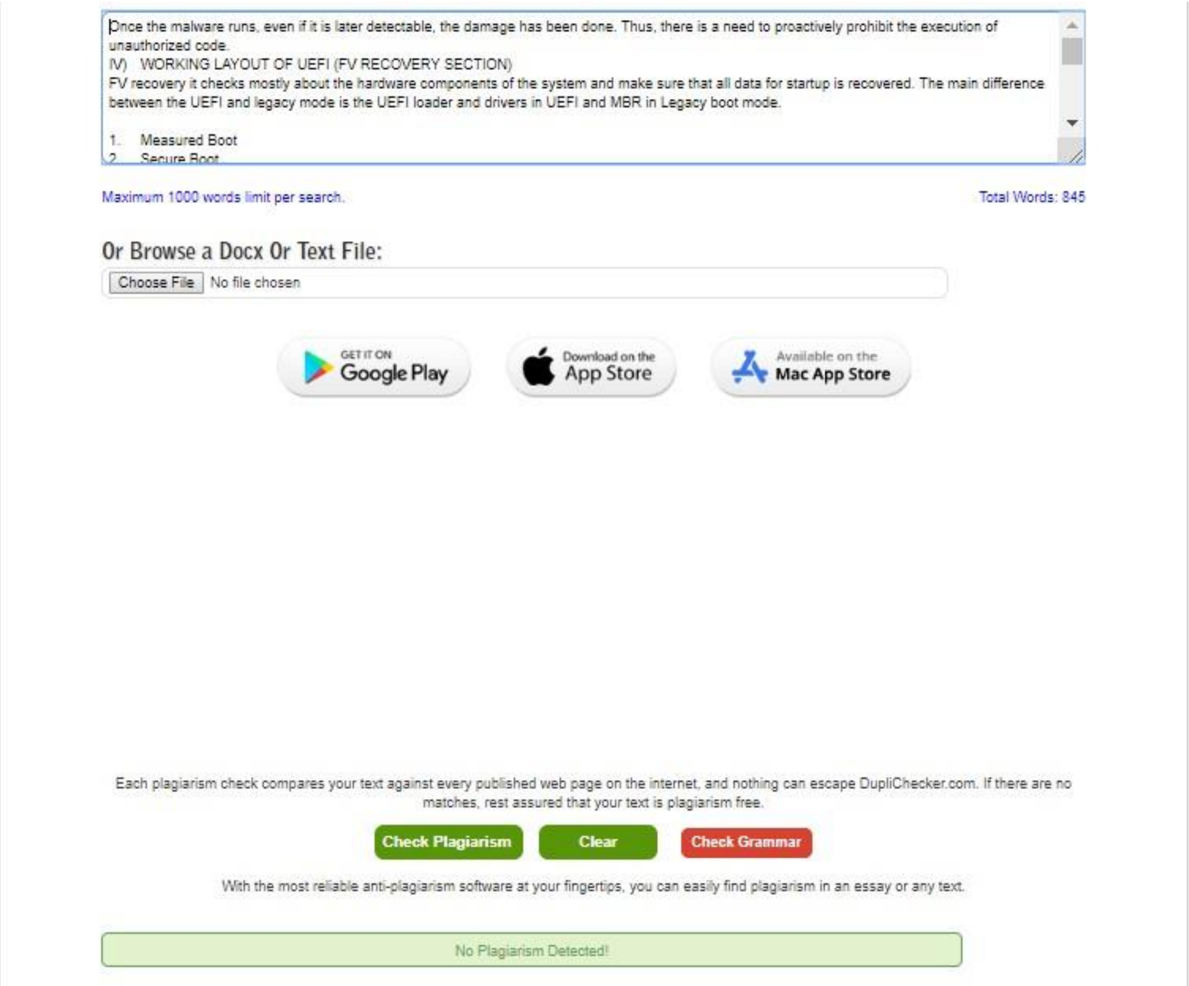
Choose File No file chosen

Each plagiarism check compares your text against every published web page on the internet, and nothing can escape DupliChecker.com. If there are no matches, rest assured that your text is plagiarism free.

With the most reliable anti-plagiarism software at your fingertips, you can easily find plagiarism in an essay or any text.

No Plagiarism Detected!

PAGE 6-19:



Once the malware runs, even if it is later detectable, the damage has been done. Thus, there is a need to proactively prohibit the execution of unauthorized code.

IV) WORKING LAYOUT OF UEFI (FV RECOVERY SECTION)

FV recovery it checks mostly about the hardware components of the system and make sure that all data for startup is recovered. The main difference between the UEFI and legacy mode is the UEFI loader and drivers in UEFI and MBR in Legacy boot mode.

1. Measured Boot
2. Secure Boot

Maximum 1000 words limit per search.

Total Words: 845

Or Browse a Docx Or Text File:

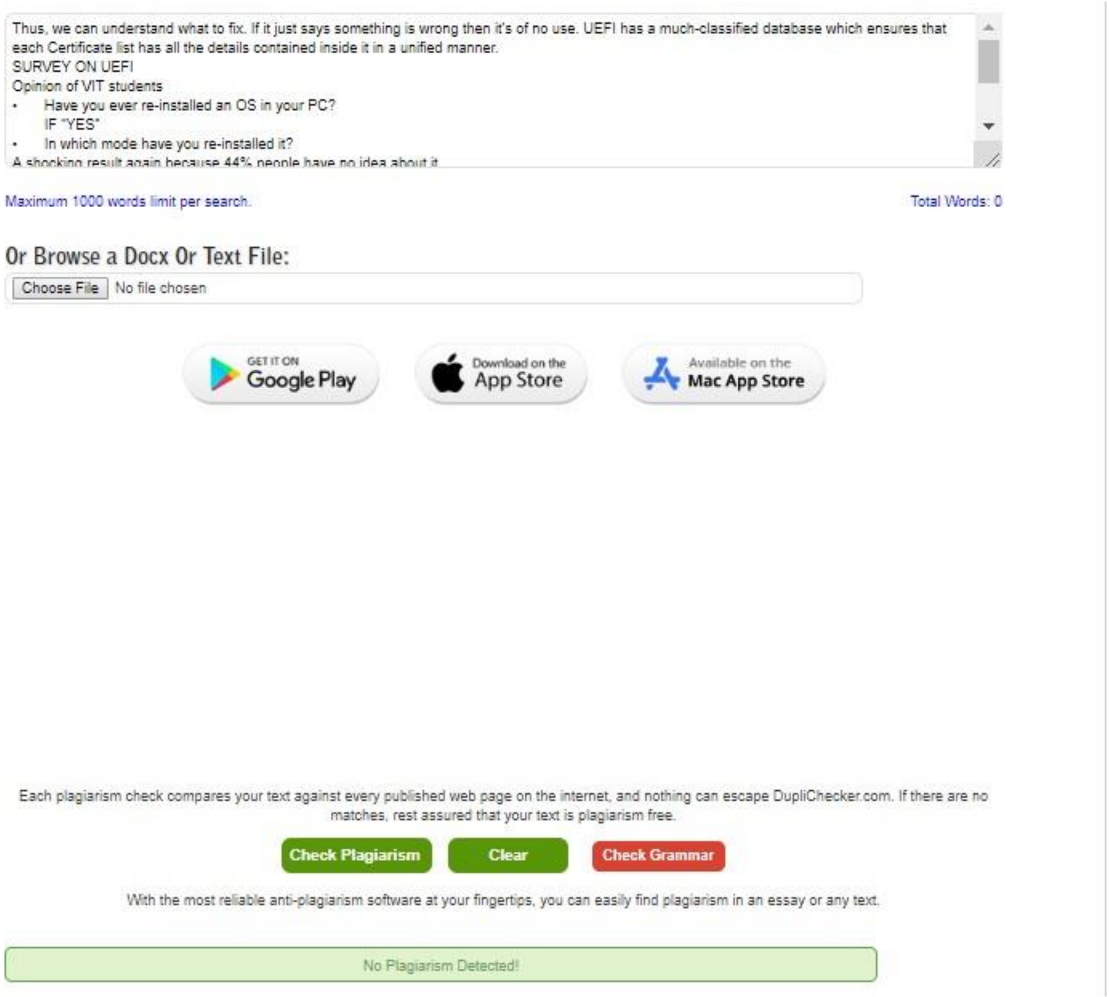
Choose File No file chosen

Each plagiarism check compares your text against every published web page on the internet, and nothing can escape DupliChecker.com. If there are no matches, rest assured that your text is plagiarism free.

With the most reliable anti-plagiarism software at your fingertips, you can easily find plagiarism in an essay or any text.

No Plagiarism Detected!

PAGE 19-21:



Thus, we can understand what to fix. If it just says something is wrong then it's of no use. UEFI has a much-classified database which ensures that each Certificate list has all the details contained inside it in a unified manner.

SURVEY ON UEFI

Opinion of VIT students

- Have you ever re-installed an OS in your PC?

  IF "YES"

- In which mode have you re-installed it?

A shocking result again because 44% people have no idea about it

Maximum 1000 words limit per search.

Total Words: 0

Or Browse a Docx Or Text File:

Each plagiarism check compares your text against every published web page on the internet, and nothing can escape DupliChecker.com. If there are no matches, rest assured that your text is plagiarism free.

With the most reliable anti-plagiarism software at your fingertips, you can easily find plagiarism in an essay or any text.

No Plagiarism Detected!