

Atividade 4

ECM245-Arquitetura e Organização de Computadores

Apresentação: 07/11/2019

Professor Doutor João Carlos Lopes Fernandes



Integrantes:

Paulo Belo Kaari Fernandes	16.00962-2
Caio Petrelli Cominato	17.00100-5
Enricco D L Amaral	17.00165-0
Xiaoying He	17.00670-8
Karina L. D. Kuroda	17.00709-7
Fernanda Veneroso de Almeida	17.00122-9

Objetivo:

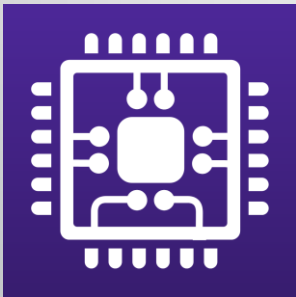
- Apresentação de um modelo de melhoria de performance, com informações adquiridas a partir de um Benchmarking

Benchmark

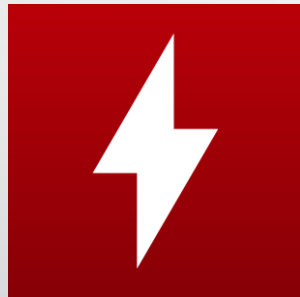
- Trata- se de um conjunto de teste ;
- Leva em conta a capacidade de trabalho do hardware ou de um software;
- Quando avaliando o Hardware, avalia-se de forma única cada peça do computador, por exemplo, placa de vídeo, processador etc.

Benchmarks- Exemplos

- CPU-Z



- HWMonitor



- SiSoftware
Sandra



- Fraps




Benchmarks- CPU-Z

CPU-Z

CPU | Caches | Mainboard | Memory | SPD | Graphics | About

Processor

Name	Intel Core i5 2500		
Code Name	Sandy Bridge	Max TDP	95 W
Package	Socket 1155 LGA		
Technology	32 nm	Core Voltage	1.048 V



Specification

Intel(R) Core(TM) i5-2500 CPU @ 3.30GHz			
Family	6	Model	A
Ext. Family	6	Ext. Model	2A
Stepping	7	Revision	D2

Instructions MMX, SSE (1, 2, 3, 3S, 4.1, 4.2), EM64T, VT-x, AES, AVX

Clocks (Core #0)

Core Speed	1596.3 MHz
Multiplier	x 16.0
Bus Speed	99.8 MHz
Rated FSB	

Cache

L1 Data	4 x 32 KBytes	8-way
L1 Inst.	4 x 32 KBytes	8-way
Level 2	4 x 256 KBytes	8-way
Level 3	6 MBytes	12-way

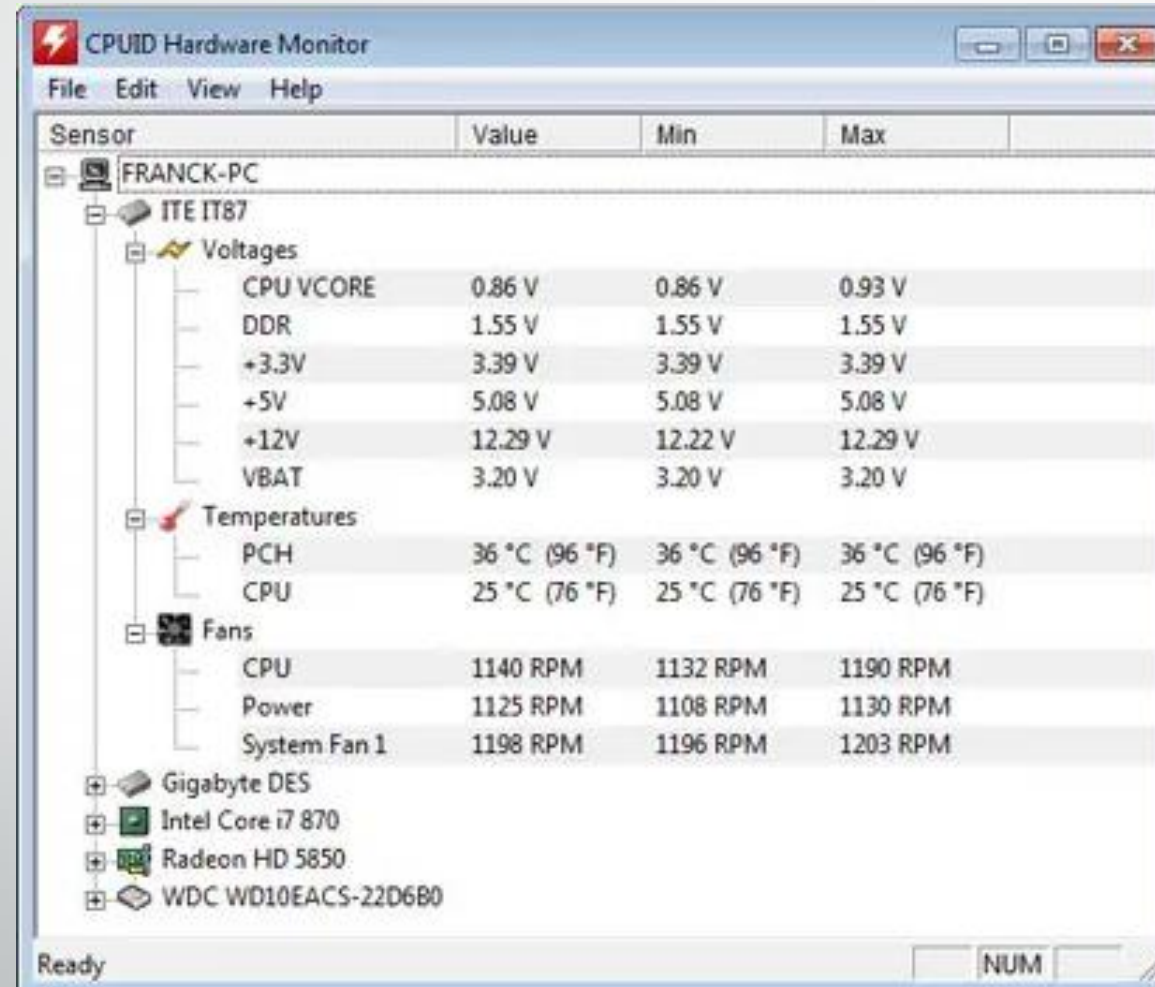
Selection Processor #1

Cores 4 Threads 4

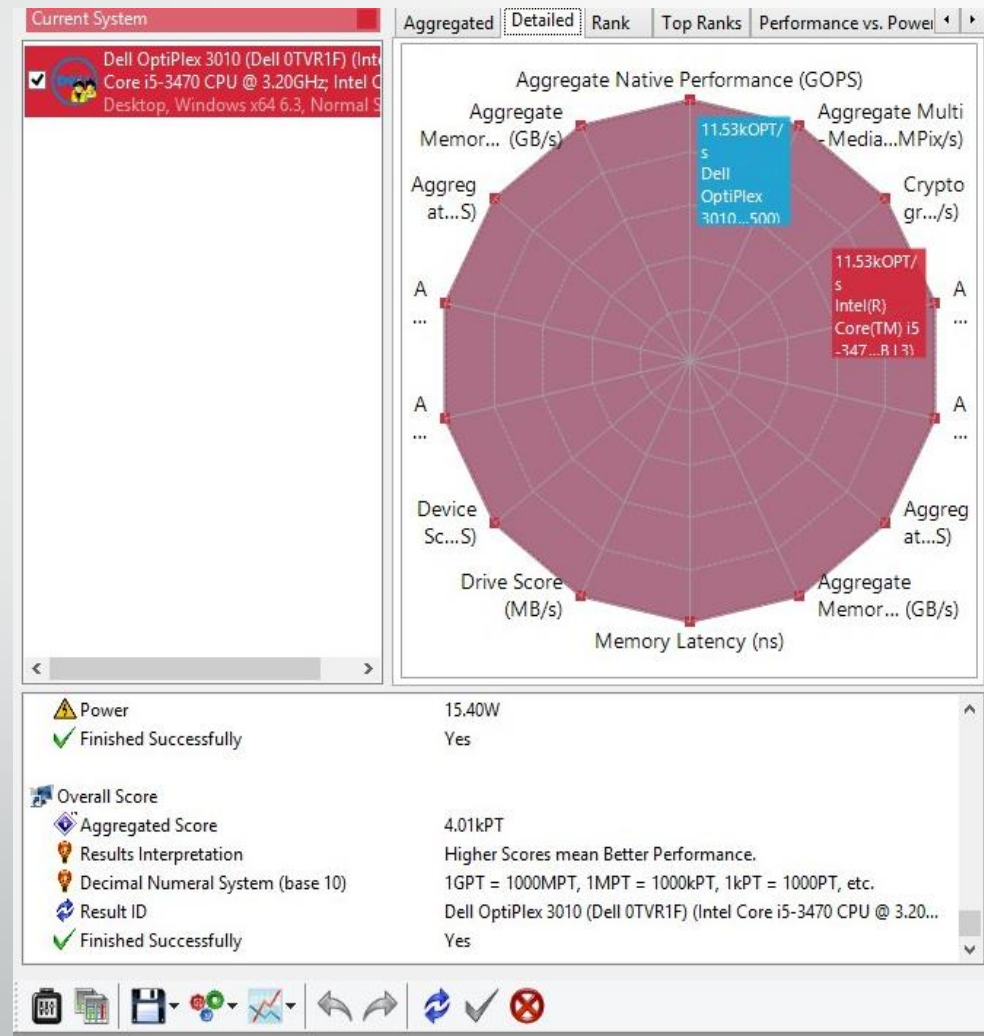
CPU-Z Version 1.59

Validate OK

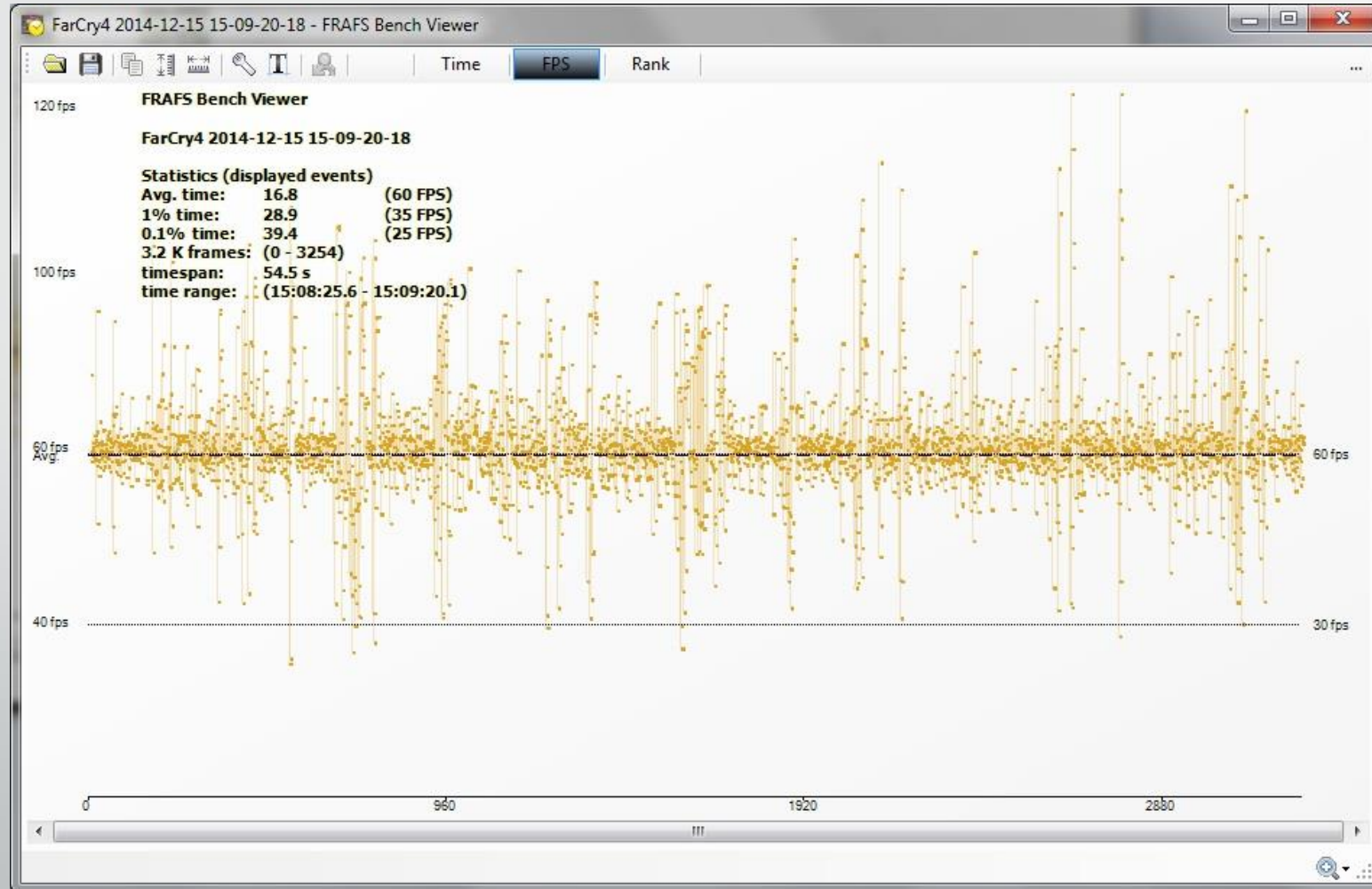
Benchmarks-HWMonitor



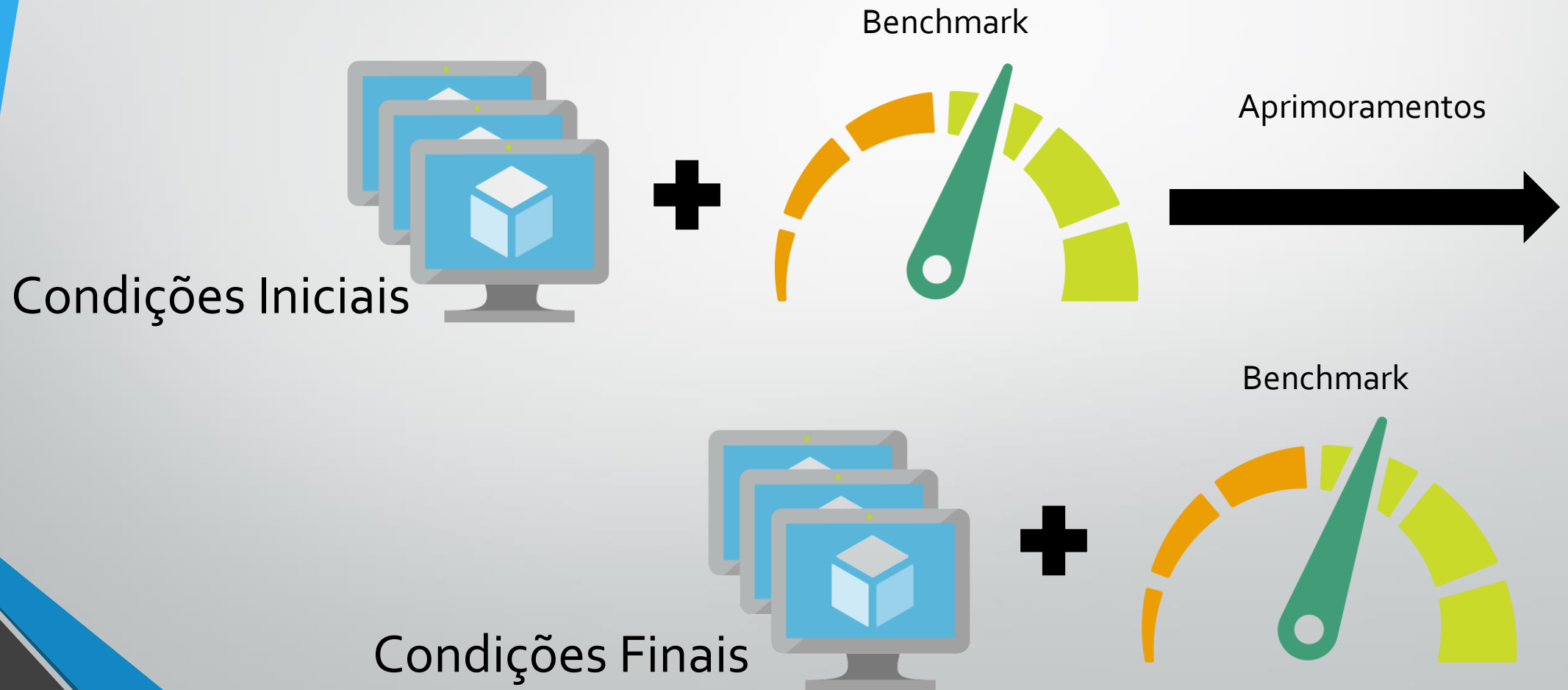
Benchmarks-SiSoftware Sandra



Benchmarks-Fraps



Estratégia de Resolução



Ferramentas utilizadas



- 2 cores CPU
- 6GB de RAM
- 10 GB de Armazenamento

- open source
- Versão oficial para Ubuntu
- Instalação de teste automatizada

Ferramentas utilizadas



- 2 processadores
- 6GB de RAM
- 10 GB de Armazenamento

Geral

Nome: Máquina1
Sistema Operacional: Ubuntu (64-bit)
Localização do Arquivo de Configurações: C:\Users\enric\VirtualBox VMs\Máquina1

Sistema

Memória Principal: 4096 MB
Processadores: 2
Ordem de Boot: Disquete, Óptico, Disco Rígido
Aceleração: VT-x/AMD-V, Paginação Aninhada, Paravirtualização KVM

Tela

Memória de Vídeo: 16 MB
Controladora Gráfica: VMSVGA
Servidor de Desktop Remoto: Desabilitado
Gravação: Desabilitado

Armazenamento

Controladora: IDE
IDE Secundário Master: [Disco Óptico] Vazio
Controladora: SATA
Porta SATA 1: NewVirtualDisk1.vdi (Normal, 10,00 GB)

Áudio

Driver do Hospedeiro: Windows DirectSound
Controladora: ICH AC97

Pré-Visualização

A screenshot of a terminal window with a dark background and light-colored text. It shows the output of a command, likely a system boot or configuration check, with various status messages and timestamps.

Teste



John The Ripper :

- É uma ferramenta popular de quebra de senha que combina vários programas diferentes;
- Pode ser executada por força bruta;
- Frequentemente usado em empresas para detectar senhas fracas que podem colocar em risco a segurança da rede, além de outros fins administrativos;
- O estresse colocado na CPU faz com que seja um programa ideal para testes.

Teste: Blowfish

- Algoritmo de criptografia simétrico;
- Cifra de bloco: bloco de 64 bits;
- Comprimento variável da chave: 32 bits a 448 bits;
- Sem patente e sem royalties.

Teste: Blowfish



Teste

- Executamos Jonh the Ripper, no modo força bruta, em uma senha gerada pelo blowfish.

```
Test: Blowfish:
```

```
2599
```

```
2584
```

```
2598
```

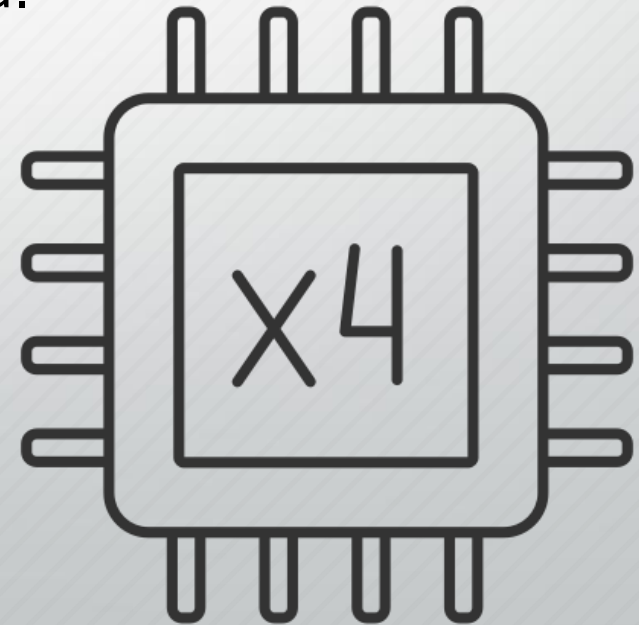
```
Average: 2594 Real C/S
```

```
Deviation: 0.32%
```

C/S: Comparações por Segundo

Aprimoramentos

- A carga de teste é paralelizável, portanto aumentando o número de núcleos, teoricamente, a performance melhora.



Aprimoramentos



- 4 processadores
- 6GB de RAM
- 10 GB de Armazenamento

Geral

Nome: Máquina2
Sistema Operacional: Ubuntu (64-bit)
Localização do Arquivo de Configurações: C:\Users\enric\VirtualBox VMs\Máquina2

Sistema

Memória Principal: 5976 MB
Processadores: 4
Ordem de Boot: Disquete, Óptico, Disco Rígido
Aceleração: VT-x/AMD-V, Paginação Aninhada, Paravirtualização KVM

Tela

Memória de Vídeo: 16 MB
Controladora Gráfica: VMSVGA
Servidor de Desktop Remoto: Desabilitado
Gravação: Desabilitado

Armazenamento

Controladora: IDE
IDE Secundário Master: [Disco Óptico] Vazio
Controladora: SATA
Porta SATA 0: Máquina2.vdi (Normal, 10,00 GB)

Áudio

Driver do Hospedeiro: Windows DirectSound
Controladora: ICH AC97

Pré-Visualização

A screenshot of a terminal window showing the boot process of a virtual machine. The text includes "disabled AIO TUNING", "Would you like to save these boot results (Y/N)?", and a prompt "root@ubuntu:~#". The background is dark with light-colored text.

Teste pós Aprimoramentos

- Executamos Jonh the Ripper, no modo força bruta, em uma senha gerada pelo blowfish.

```
Test: Blowfish:
```

```
4489
```

```
4467
```

```
4479
```

```
Average: 4478 Real C/S
```

```
Deviation: 0.25%
```

C/S: Comparações por Segundo



Vídeo

Comparação dos resultados dos testes

```
John The Ripper 1.9.0-jumbo-1:
pts/john-the-ripper-1.7.0 [Test: Blowfish]
Test 1 of 1
Estimated Trial Run Count:      3
Estimated Time To Completion: 2 Minutes [02:59 UTC]
  Started Run 1 @ 02:57:51
  Started Run 2 @ 02:58:26
  Started Run 3 @ 02:59:00

Test: Blowfish:
  2599
  2584
  2598

Average: 2594 Real C/S
Deviation: 0.32%
```

```
John The Ripper 1.9.0-jumbo-1:
pts/john-the-ripper-1.7.0 [Test: Blowfish]
Test 1 of 1
Estimated Trial Run Count:      3
Estimated Time To Completion: 2 Minutes [22:05 EST]
  Started Run 1 @ 22:03:58
  Started Run 2 @ 22:04:33
  Started Run 3 @ 22:05:07

Test: Blowfish:
  4489
  4467
  4479

Average: 4478 Real C/S
Deviation: 0.25%
```

Resumo do Teste

 **ubuntu** +
2 processadores


Phoronix Test Suite

+


2594 c/s

APRIMORAMENTOS

 **ubuntu** +
4 processadores

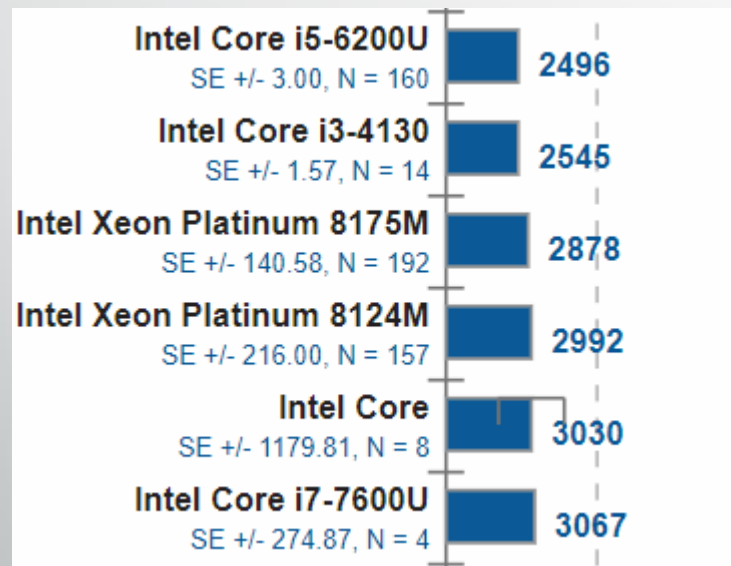

Phoronix Test Suite

+

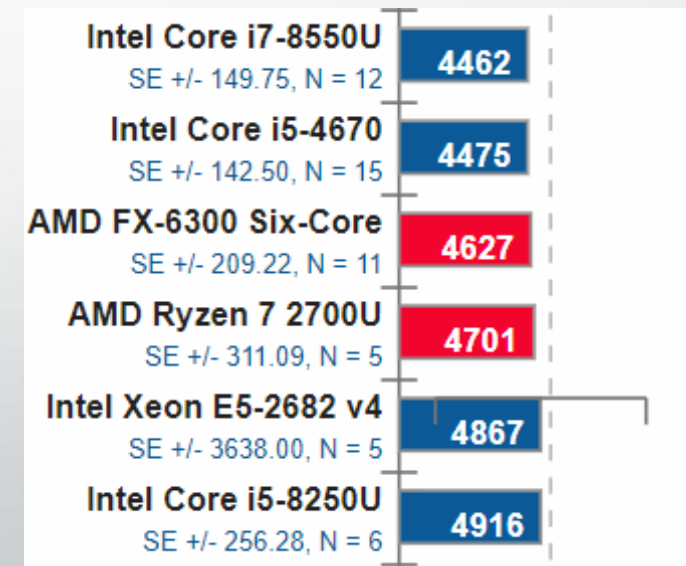

4478 c/s

Comparando o Desempenho com outros Processadores

Condições Iniciais:

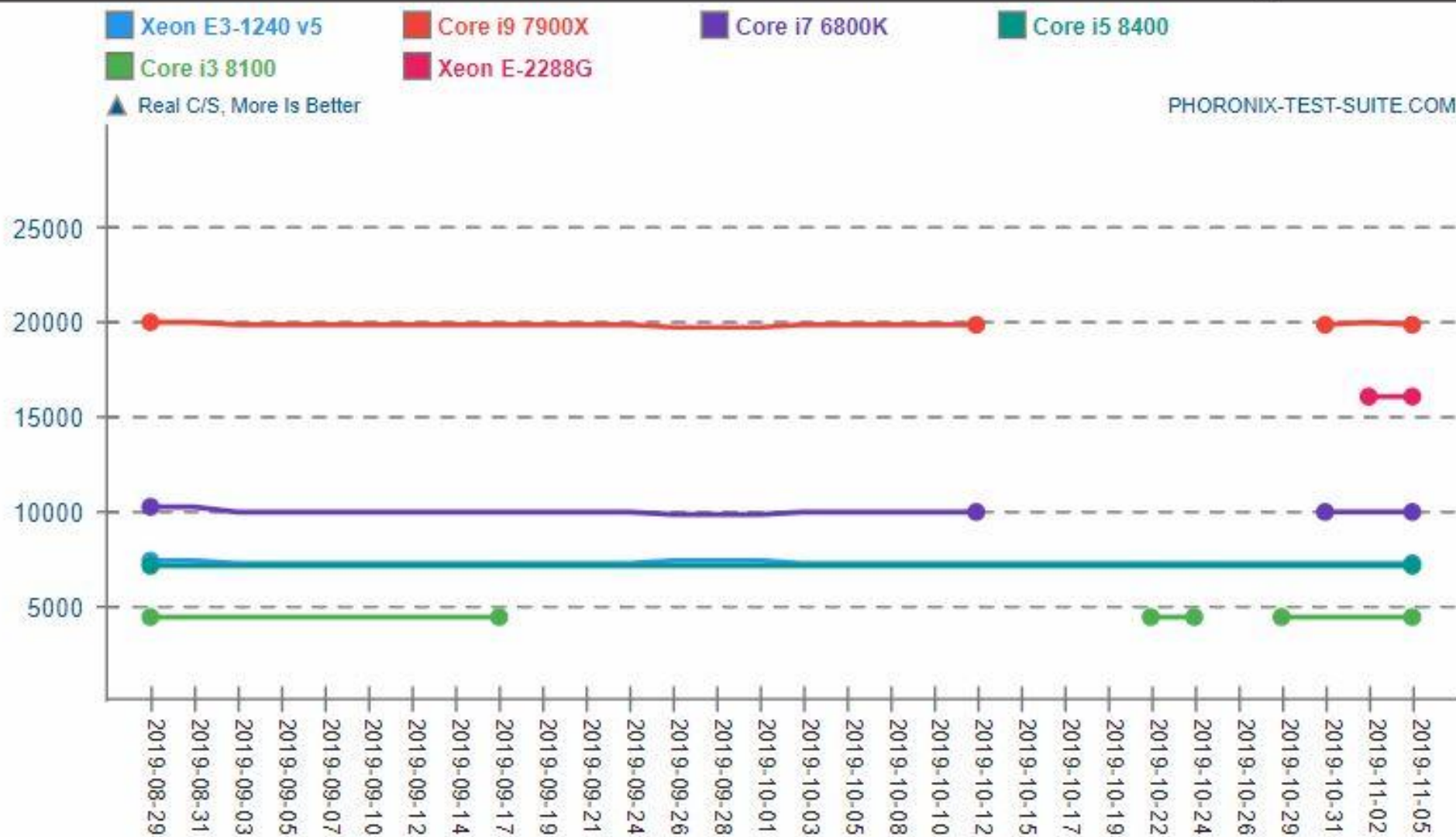


Condições Finais:



John The Ripper v1.8.0

Test: Blowfish



Bibliografia

- <https://whatis.techtarget.com/definition/John-the-Ripper>
- <https://www.openwall.com/john/>
- <https://www.linuxbenchmarking.com/?daily-gcc-benchmarks>
- <https://openbenchmarking.org/test/pts/john-the-ripper>
- <https://linuxconfig.org/how-to-benchmark-your-linux-system#h10-2-john-the-ripper>
- <https://infosecaddicts.com/john-ripper/>
- <https://openbenchmarking.org/innhold/co8d3e85031b201b155e4409d53acfb45cc13f4e>
- <http://www.passwordtool.hu/>
- <https://www.phoronix-test-suite.com/>
- <https://www.schneier.com/academic/blowfish/>