

SIN414

Auditoria e Segurança de Sistemas de Informação

Computação Forense

Ivan Leoni Vilas Boas - 2018009073

Leonardo Rodrigo de Sousa - 2018015965

Lucas Tiense Blazzi - 2018003310

Thiago Marcelo Passos - 2018002850



Computação
Forense



Sumário



Introdução



Crime Cibernéticos



Processo da computação forense (ciclo de vida)



Exames aplicados na perícia forense digital



Integridade e judicialização



Importância e problemas da computação forense



O futuro da computação forense

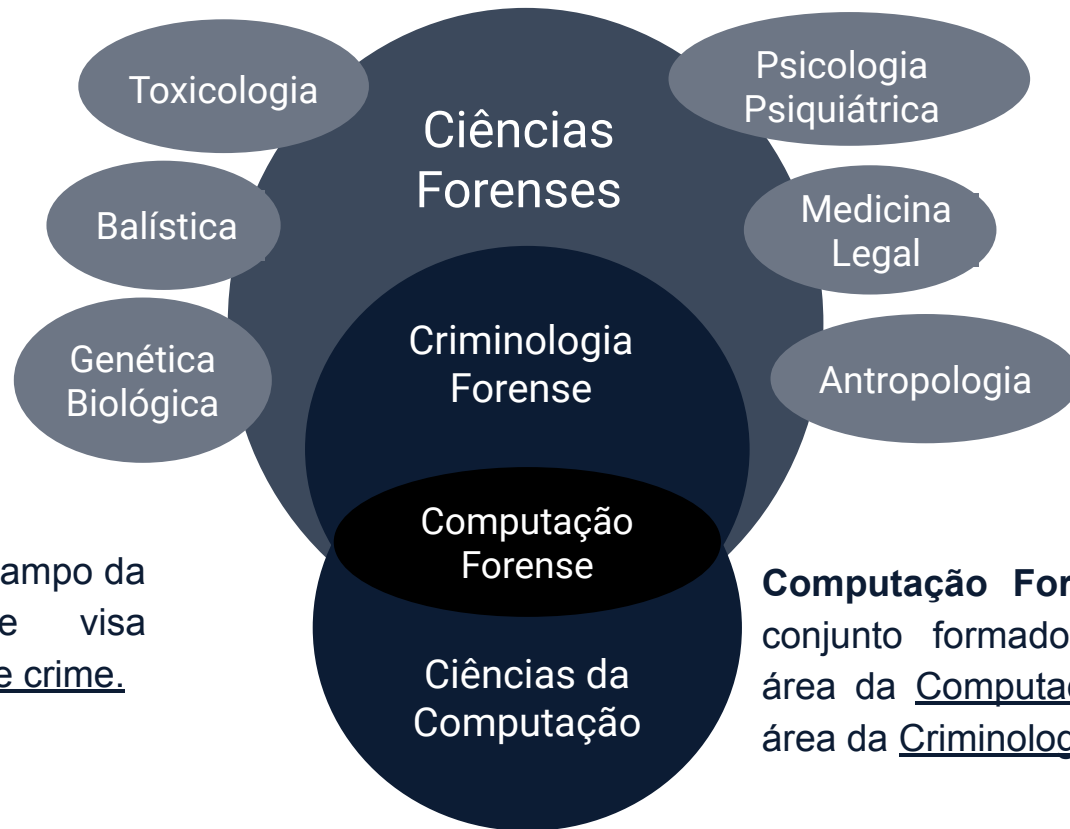


Introdução

Ciências Forenses:

Conjunto de métodos e técnicas científicas que contempla várias áreas do saber.




Criminologia Forense: Campo da Ciências forense que visa solucionar qualquer tipo de crime.



Computação Forense: conjunto formado pela área da Computação e área da Criminologia.



Crimes Cibernéticos

- Crime cibernético é qualquer delito que seja cometido utilizando dispositivos e meios tecnológicos e que gera prejuízos e danos a uma pessoa ou a uma organização.
- Ponto negativo do avanço tecnológico:  Aumento de crimes cibernéticos
 - ◆ Novas tecnologias  novas técnicas de cometer crimes
 - ◆ Transferência de delitos: **Real**  **Virtual**
- Conforme os estudiosos da área, o crime cibernético pode ser classificado de acordo com a forma de **utilização dos dispositivos para o cometimento do crime**.

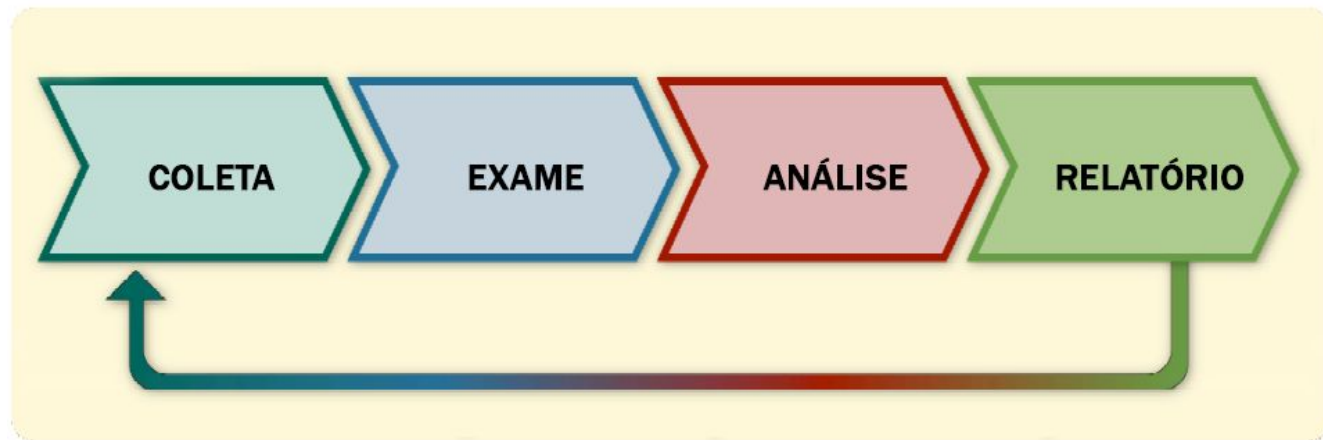


Crimes Cibernéticos: Classificação

Classificação dos Crimes Cibernéticos		
Características	FERRAMENTA DE APOIO - Impuros	CONDIÇÃO NECESSÁRIA - Puros
Equipamento tecnológico	É apenas um instrumento facilitador. Os crimes existiriam mesmo sem o instrumento.	É fundamental para o cometimento. Sem o instrumento não haveria crime.
Alvo	Normalmente direcionados às pessoas ou grupos de pessoas	Normalmente são direcionados a outros dispositivos, redes, sistemas e dados.
Regularização	Já existem leis Brasileiras	Ainda não existem leis e garantias.
Exemplos	Pedofilia, ameaça, racismo, corrupção, pornografia infantil, etc.	Invasões, ataque com ransomwares, contaminação por vírus, roubo de senhas e informações pessoais, etc.



Processo da computação forense (ciclo de vida)



Coleta: plano de aquisição, coleta dos dados, verificação de integridade.

Exame: exame sobre os dados coletados para separar dados relevantes.

Análise: analisar as informações e tirar conclusões em cima dos dados.

Relatórios: preparação e na apresentação formal dos resultados da análise.



Exames aplicados na perícia forense digital





Exames aplicados na perícia forense digital





Exames em mídias de armazenamento

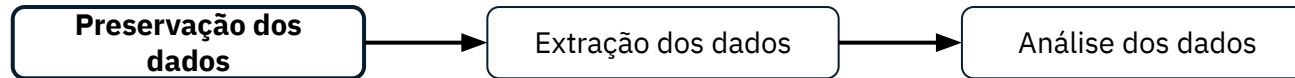


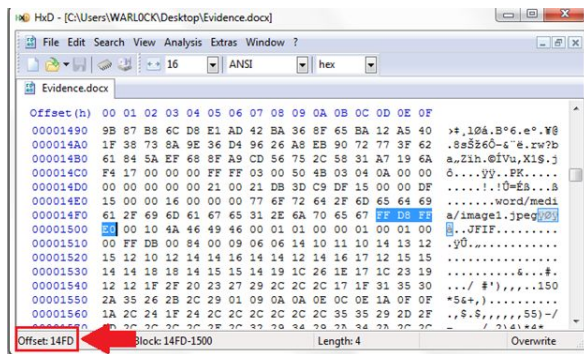
Tableau TD2U Forensic Duplicator

```
* Source: /dev/sdb
* Destination: /dev/sda1
* Image filename: image.img
* Options: bs=1M gzip=0 checksum=y checksum_method=md5
*****
Menu Options:
1. Select Source
2. Select Destination drive
3. Change image filename
4. Change Options
5. Image
6. Return to Previous Menu
> 5
The following 'dd' command will be executed (Note: /dev/sda1 will be mounted on /mnt/temp):
dd if=/dev/sdb of=/mnt/temp/image.img bs=1M conv=noerror,noerruc
Continue (y/n) ? > y
15:45:24 STATUS: Mounting /dev/sda1 of type HPFS-NTFS to /mnt/temp
15:45:26 STATUS: dd if=/dev/sdb of=/mnt/temp/image.img bs=1M conv=noerror,noerruc
0+15127 records in
0+15127 records out
1886+0 records in
1886+0 records out
15:48:43 STATUS: Imaging Finished.
15:48:43 STATUS: Computing md5 checksum of /mnt/temp/image.img...
15:51:13 STATUS: md5 checksum of /dev/sdb - 927d19b57f5ab71143f1d6f42b5023b
15:51:13 STATUS: md5 checksum of /mnt/temp/image.img - 927d19b57f5ab71143f1d6f42b5023b
15:51:13 STATUS: md5 checksum MATCH
15:51:13 STATUS: Unmounting /mnt/temp
TIME:
Start time: Oct 26, 2010 15:45:24
dd time: Oct 26, 2010 15:48:43
checksum time: Oct 26, 2010 15:51:13
Done ... Press <Enter> to continue.
```



OSFClone - Open Source OSForensics Software

Exames em mídias de armazenamento



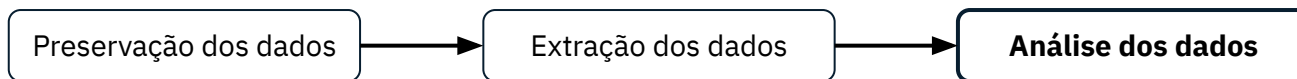
Magic Number - Assinatura de formato de arquivo

Description	Extension	Magic Number
Adobe Illustrator	.ai	25 50 44 46 [%PDF]
Bitmap graphic	.bmp	42 4D [BM]
Class File	.class	CA FE BA BE
JPEG graphic file	.jpg	FFD8
JPEG 2000 graphic file	.jp2	000000006A50202000A [...JP...]
GIF graphic file	.gif	47 49 46 38 [GIF89]
TIF graphic file	.tif	49 49 [II]
PNG graphic file	.png	89 50 4E 47 .PNG
WAV audio file	.png	52 49 46 46 RIFF
ELF Linux EXE	.png	7F 45 4C 46 .ELF
Photoshop Graphics	.psd	38 42 50 53 [8BPS]
Windows Meta File	.wmf	D7 CD C6 9A
MIDI file	.mid	4D 54 68 64 [MThd]
Icon file	.ico	00 00 01 00
MP3 file with ID3 identity tag	.mp3	49 44 33 [ID3]
AVI video file	.avi	52 49 46 46 [RIFF]
Flash Shockwave	.swf	46 57 53 [FWS]
Flash Video	.flv	46 4C 56 [FLV]
Mpeg 4 video file	.mp4	00 00 00 18 66 74 79 70 6D 70 34 32 [...ftypmp42]
MOV video file	.mov	6D 6F 6F 76 [...movv]
Windows Video File	.wmv	30 26 82 75 8E 66 CF
Windows Audio File	.wma	30 26 82 75 8E 66 CF
PKZip	.zip	50 4B 03 04 [PK]
GZip	.gz	1F 8B 08
Tar file	.tar	75 73 74 61 72
Microsoft Installer	.msi	D0 CF 11 E0 1B 1A E1
Object Code File	.obj	4C 01
Dynamic Library	.dll	4D 5A [MZ]
CAB Installer file	.cab	4D 53 43 46 [MSCF]
Executable file	.exe	4D 5A [MZ]
RAR file	.rar	52 61 72 21 1A 07 00 [Rar!...]
SYS file	.sys	4D 5A [MZ]
Help file	.hlp	3F 5F 03 00 [7...]
VHware Disk file	.vmdk	4B 44 4D 56 [KDMV]
Outlook Post Office file	.pst	21 42 44 4E 42 [BDN8]
PDF Document	.pdf	25 50 44 46 [%PDF]

Tabela de magic numbers



Exames em mídias de armazenamento



NIST Search NIST

Information Technology Laboratory / Software and Systems Division

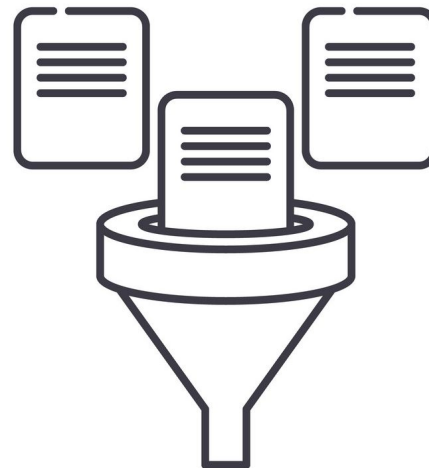
SOFTWARE QUALITY GROUP

National Software Reference Library (NSRL)

Welcome to the National Software Reference Library (NSRL) Project Web Site.

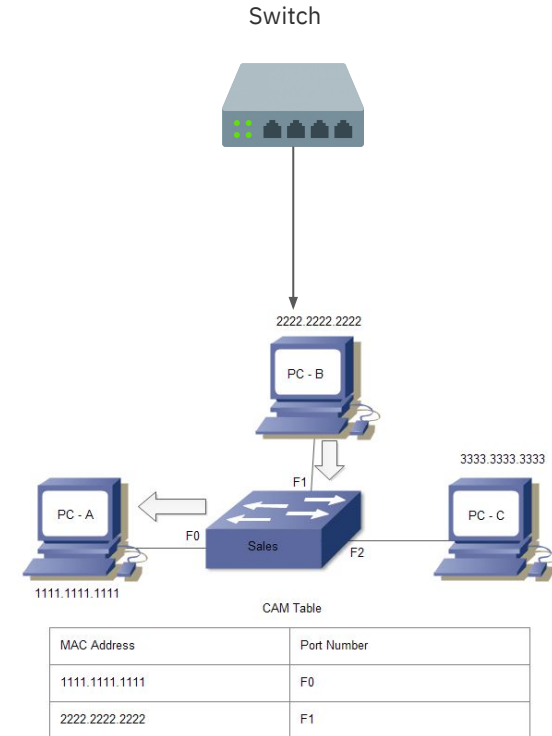
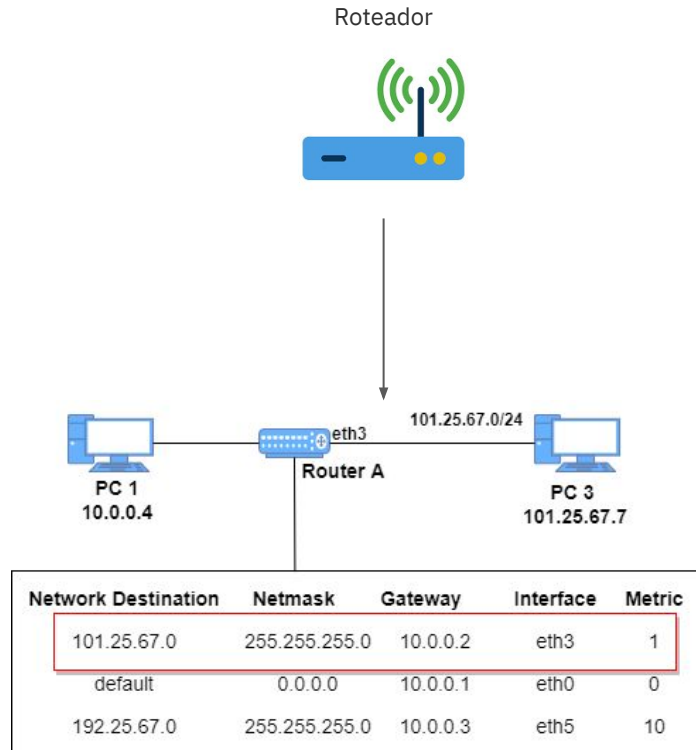
RDS 2.77 June 2022 Hash Counts

Modern:	222,113,224
Modern (minimal):	46,688,292
Modern (unique):	25,018,441
Legacy:	135,200,245
Android:	76,155,515
iOS:	26,051,461





Exames em redes de computadores





```

.../services/SOSU/region.php?region=999999.9 %2f**%2fuNiOn%2f**%2faLl
%2f**%2fsElEcT(%2f**%2fsElEcT
%2f**%2foCnCaT(%2f017e21,count(t,%2f**%2ftAbLe_nAMe),0x217e21)
%2f**%2fRoM information_schema.%2f**%2fscHEmAAt%2f join
information_schema.%2f**%2ftAbLeS at t on t.%2f**%2ftAbLe_sCHEmA =
d.%2f**%2fscHEmA NaMe join information_schema.%2f**%2fcolUmNs as c on
c.%2f**%2ftAbLe_sCHEmA = d.%2f**%2fscHEmA NaMe and
c.%2f**%2ftAbLe_nAMe = t.%2f**%2ftAbLe_nAMe %2f**%2fwHeRe not
c.%2f**%2ftAbLe_sCHEmA
in (0x696ae66f726d174696f6e5f736368656d61,0xd67973716c) and
c.%2f**%2fcolUmN NaMe like
0x256d61696c25),2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18"

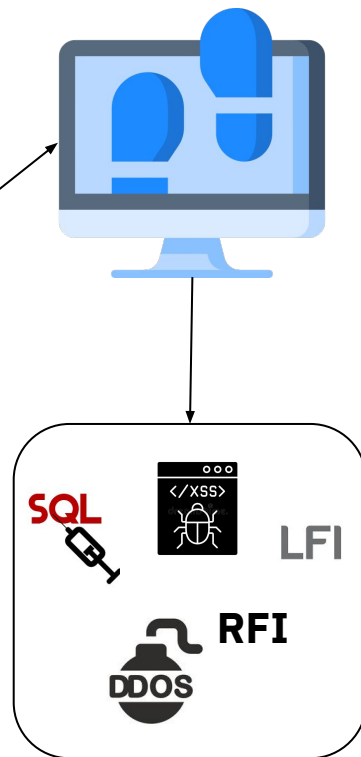
```

```
2013-03-20 19:03:11 60.166.3.22 5081 192.168.100.11 80 HTTP/1.1 GET
/images"OTA2NjAw40 400 - URL -

2013-03-20 19:03:36 60.166.3.22 5083 192.168.100.11 80 HTTP/1.1 GET
/Login/../../../../../../../../etc/passwd 403 -
Forbidden -

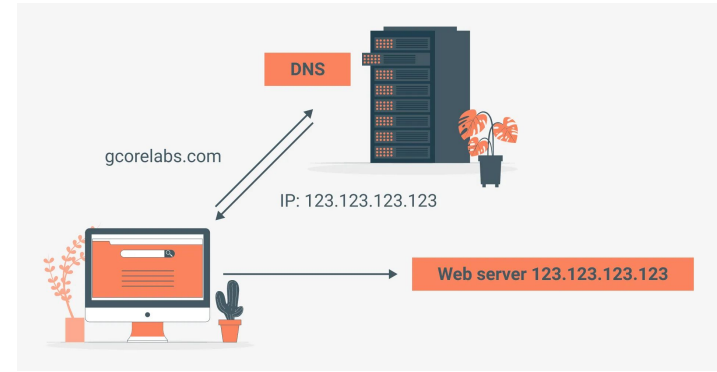
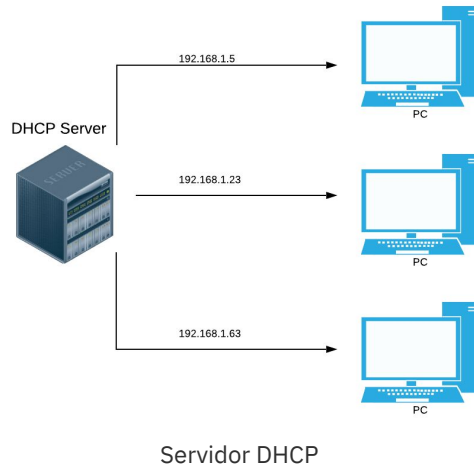
2013-03-20 19:03:36 60.166.3.22 5109 192.168.100.11 80 HTTP/1.1 GET
/Login/../../../../../../../../etc/windows/win.ini 403 -
Forbidden -

2013-03-20 19:03:37 60.166.3.22 5093 192.168.100.11 80 HTTP/1.1 GET
/Login/../../../../../../../../etc/passwd 403 - Forbidden -
```





Exames em redes de computadores



Servidor de Autenticação



Exames em dados criptografados

Recuperação direta

Direct Vulnerabilities

Known vulnerabilities in the cryptography package. This does not include vulnerabilities belonging to this package's dependencies.

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

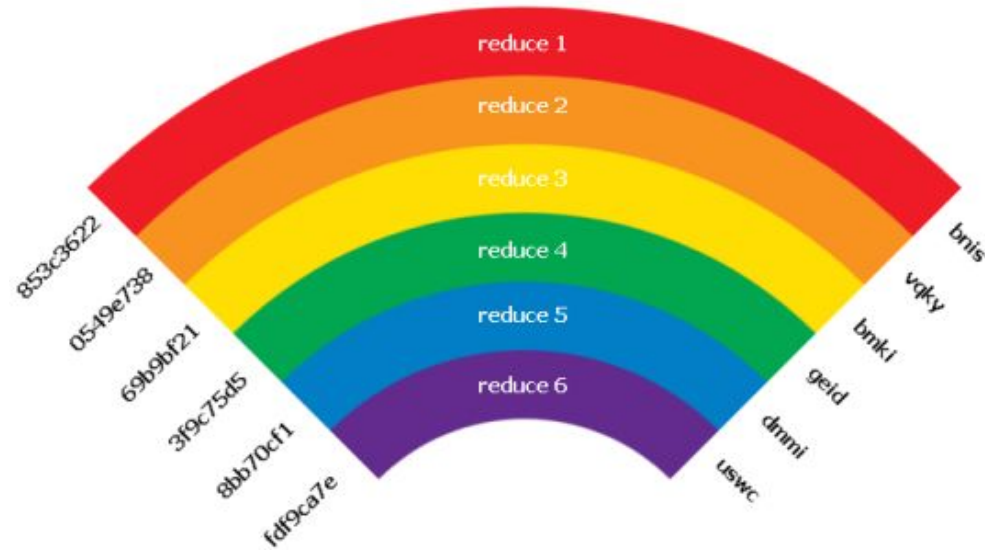
Fix for free

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
M Cryptographic Issues	[3.1 , 3.3.2)	Not available	08 Feb, 2021
H Timing Attack	[, 3.2)	Not available	27 Oct, 2020
H Authentication Bypass	[1.9.0, 2.3)	Not available	19 Jul, 2018
M Denial of Service (DoS)	[, 1.0.2)	Not available	04 Dec, 2017
H Denial of Service (DoS)	[, 0.9.1)	Not available	04 Dec, 2017
H Use of a Risky Cryptographic Algorithm	[, 1.5.2)	Not available	01 Nov, 2016
M TLS Truncation Attack	[, 1.1)	Not available	10 Sep, 2015



Exames em dados criptografados

Recuperação pré-computada

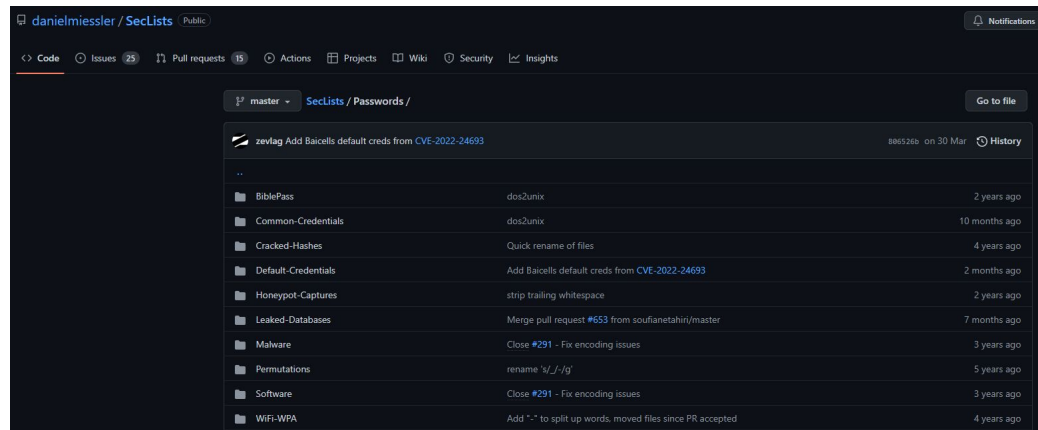




Exames em dados criptografados

Recuperação por tentativa

- Tentativa por força bruta
- Tentativa guiada por dicionários





Integridade e judicialização - legislação brasileira

Direitos:

- Uso de todos meios legais, moralmente legítimos como prova de fato;
- Impugnação da exatidão destes meios.

Valor legal:

- Autenticidade
- Integridade
- Cadeia de custódia

OBS: Dados de terceiros precisam de ordem judicial para a coleta.



Importância e problemas no cenário

Importância da computação forense:

- A computação forense tornou-se hoje a maior ferramenta na investigação de crimes cibernéticos.
- Acesso às informações de qualquer dispositivo.

Problemas da computação forense:

- Falta de profissionais especializados.
- Aumento dos pontos de acesso a internet (IOT).
- Garantir a validade das provas.





O futuro da computação forense

- Aumento dos ataques cibernéticos na pandemia.
- Acesso de dados confidenciais em ambiente não controlado
- Aumento da importância da computação forense no cenário empresarial
- Aumento da demanda por profissionais.



Conclusão

A **computação forense** é uma forte e importante aliada na investigação de atos ilegais:

- **Ajuda na solução, no combate e na prevenção crimes;**
- **Contribui na evolução e melhorias de sistemas** perante as falhas que podem ser encontradas na fase de exame.



Computação Forense