Hacking Ultrasound Machines for Fun and Profit

Victor Pasknel

MORPHUS
SEGURANÇA DA INFORMAÇÃO

meterpreter> sysinfo

Victor Pasknel

- Doutorando @ Unifor
- Pentester @ Morphus
- Pesquisador @ Morphus Labs
- Professor Universitário
- Medium: @pasknel
- Blogspot: HackingComTapioca
- Baterista ☺

Agradecimentos

Tadeu Leandro

- Especialista em redes de computadores
- Mais de 15 anos em segurança da informação
- 10 anos como CSO em planos de saúde e hospitalar

Lenine Matos

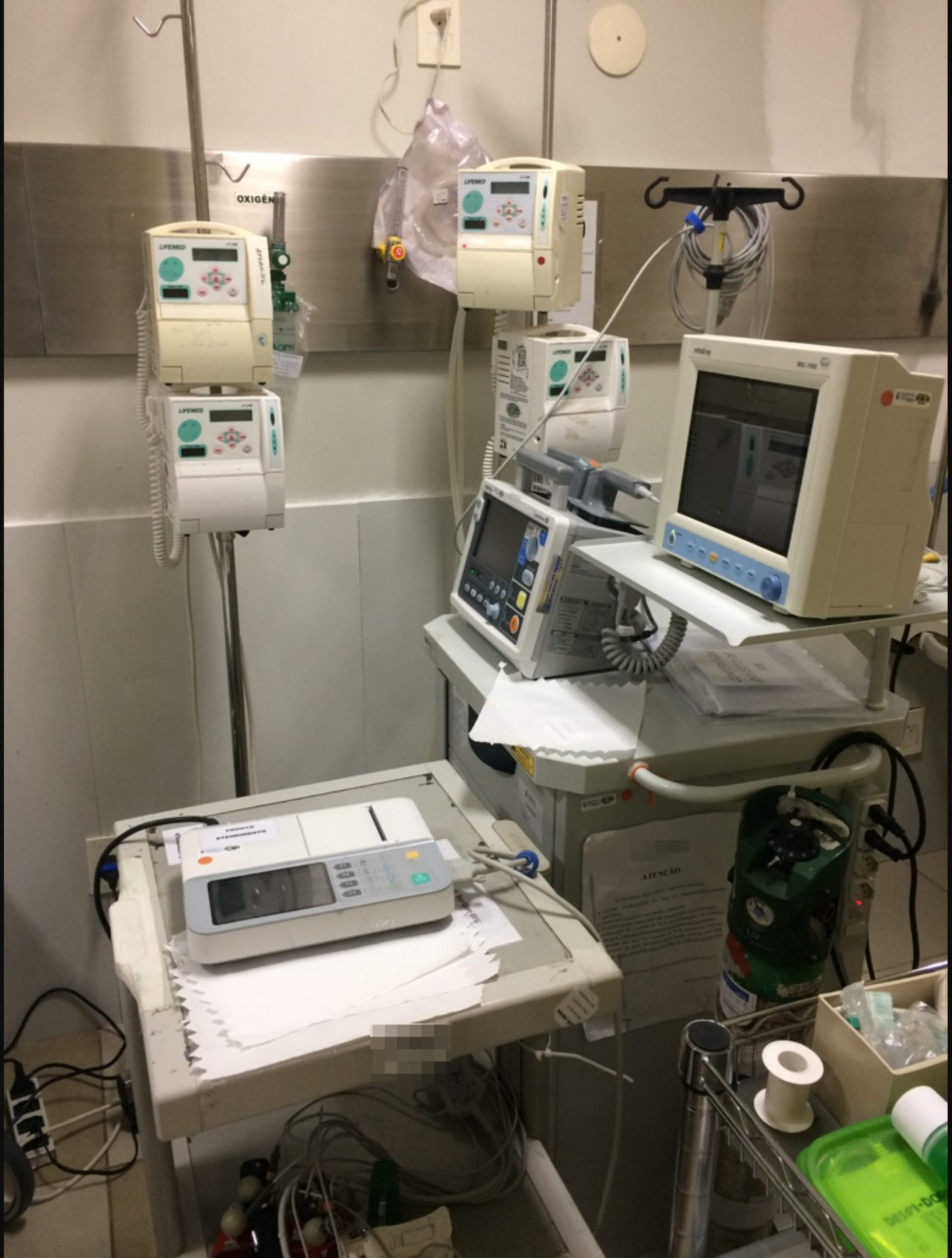
- Técnico em radiologia
- Trabalha no Instituto de Saúde e Gestão Hospitalar
- Professor universitário desde 2011

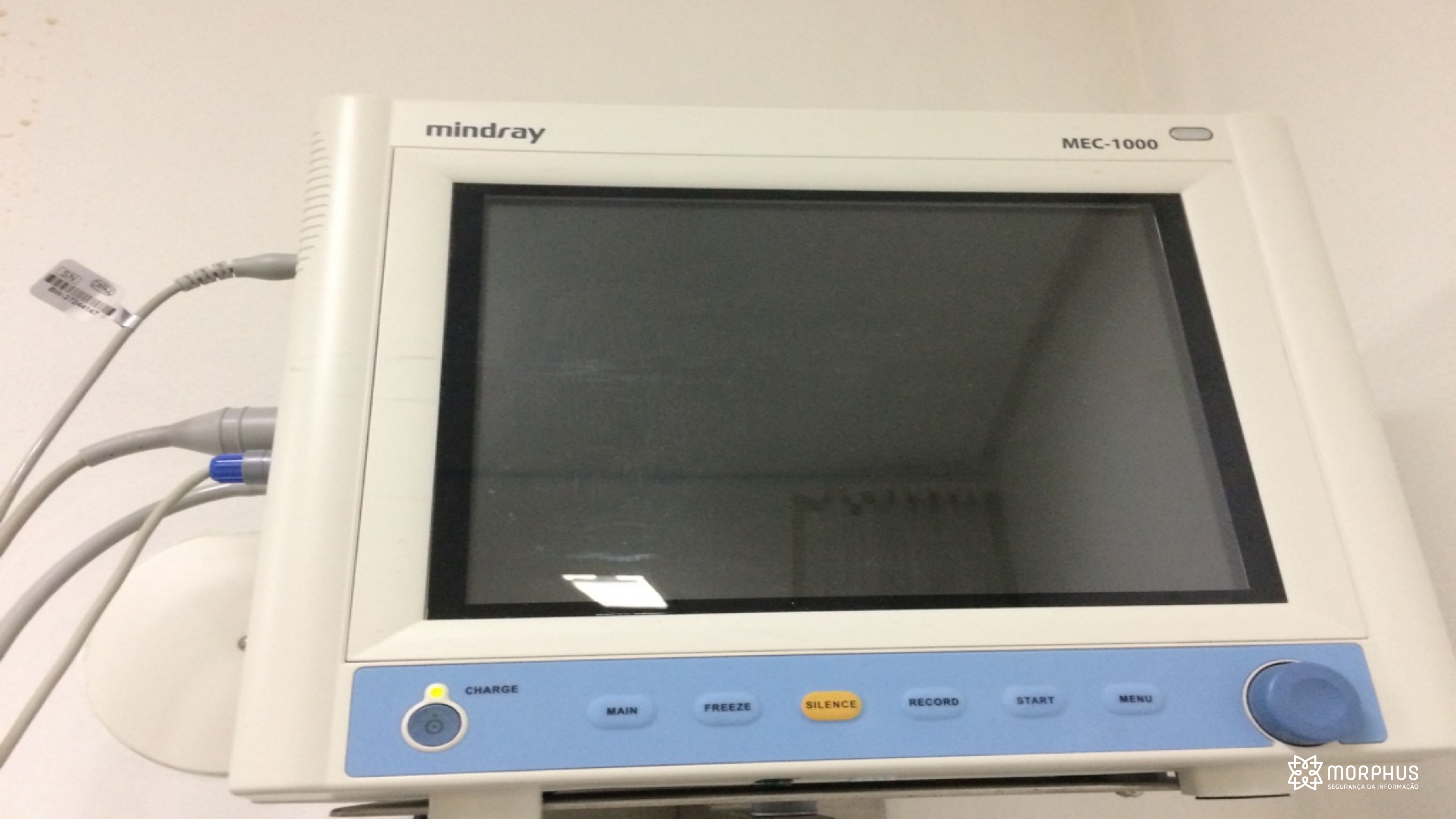
”Radiology is all about images, and about confidential images”

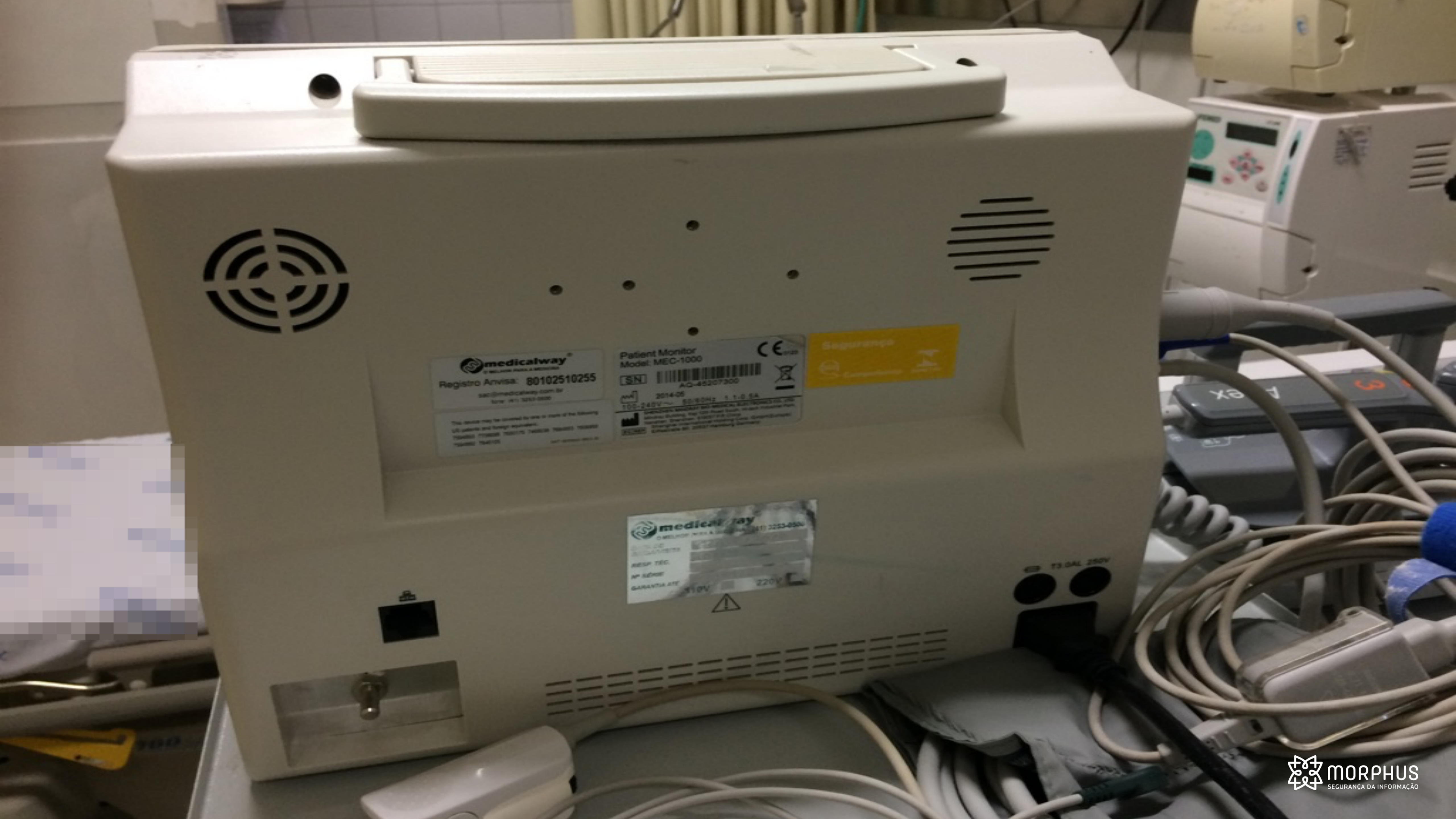
Oleg S. Pianykh

#MomentoStoryTelling

MORPHUS
SEGURANÇA DA INFORMAÇÃO

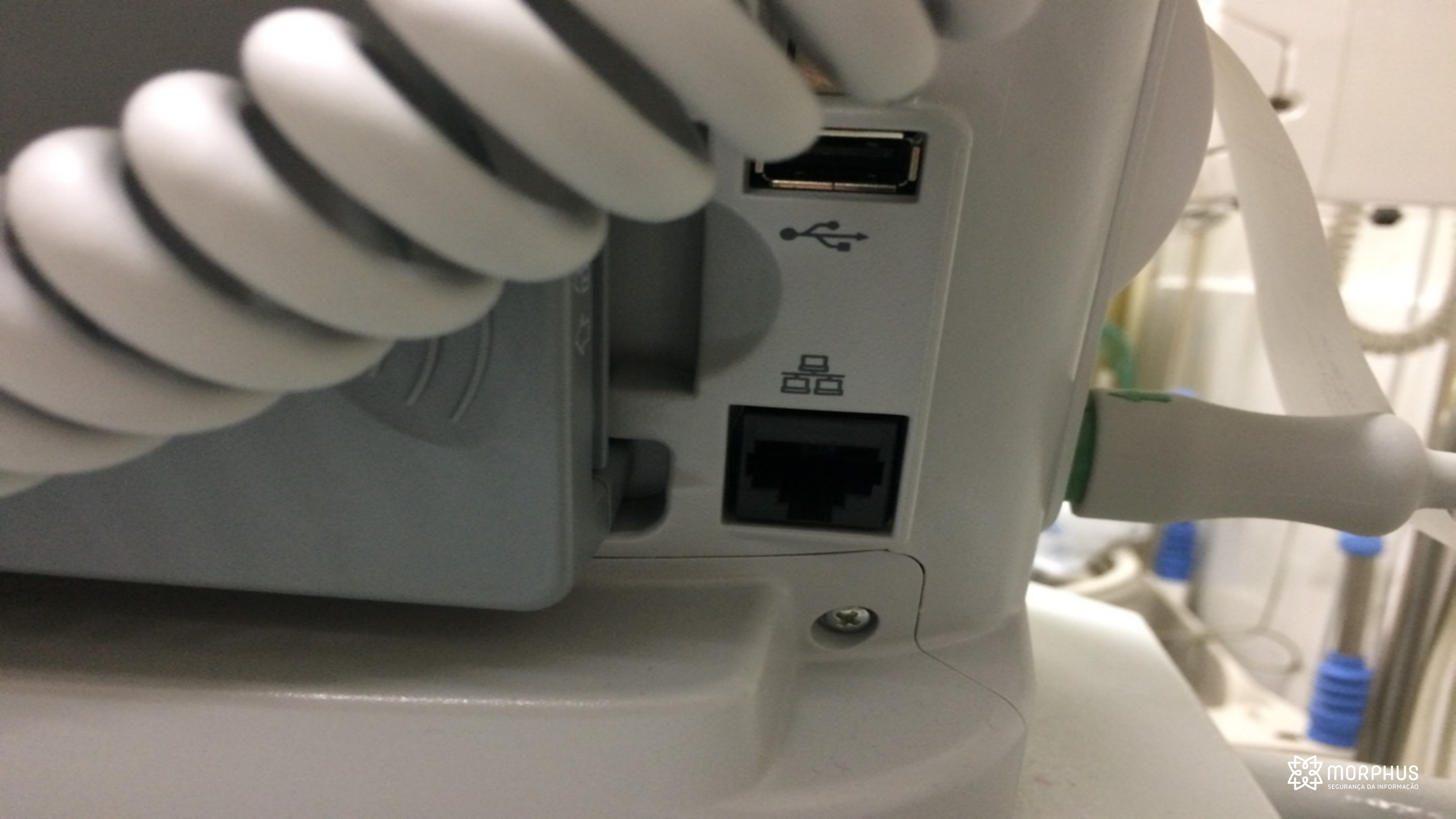

OXIGÊN
LIFEMED
LIFEMED
LIFEMED
LIFEMED
mindray
ATENÇÃO

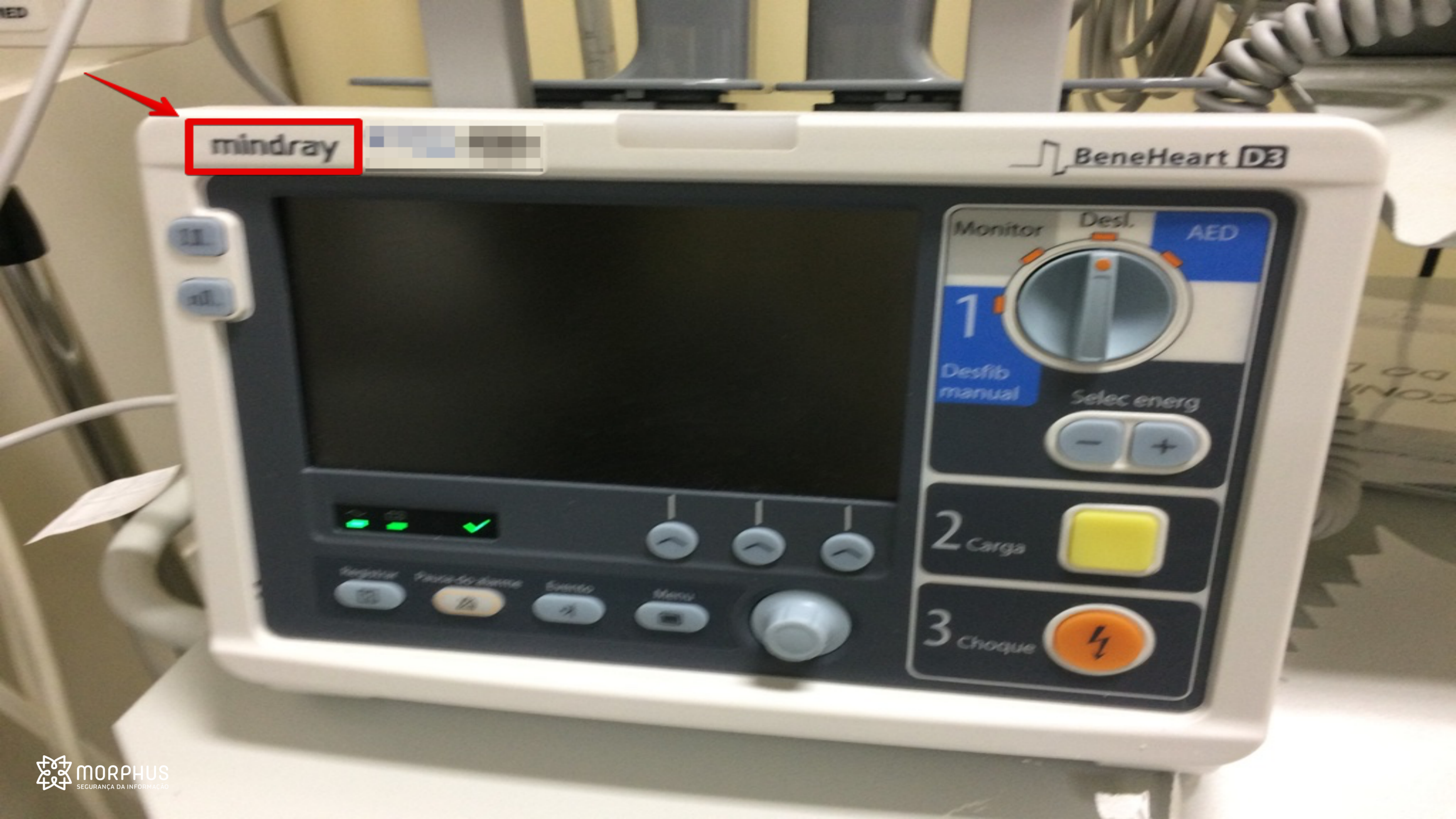

mindray
MEC-1000
CHARGE
MAIN
FREEZE
SILENCE
RECORD
START
MENU


medicalway
O MELHOR PARA A MEDICINA
Registro Anvisa: 80102510255
sac@medicalway.com.br
Patient Monitor
Model: MEC-1000
SN
AQ-45207300
2014-05
100-240V~ 50/60Hz 1.1-0.5A
Segurança
medicalway
RESP. TÉC.
Nº SÉRIE
GARANTIA ATÉ
110V
220V
T3.0AL 250V

mindray
BeneHeart D3
Monitor
Desf.
AED
1 Desfib manual
Selec energ
2 Carga
3 Choque
CHARGE
MAIN
FREEZE
SILENCE
RECORD
CONFERÊNCIA DO LEITO DE PCR

Apex
Esterno

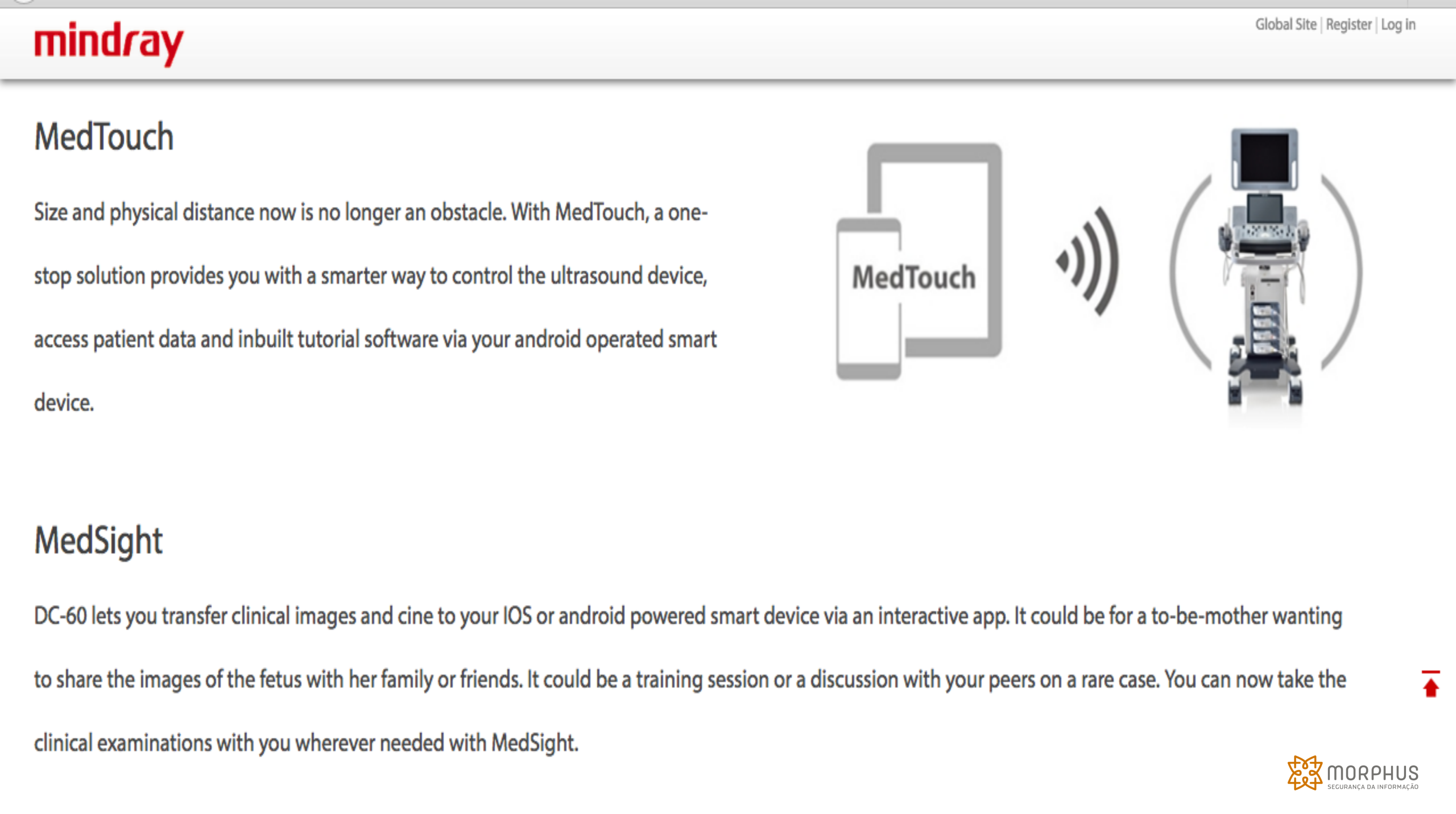



mindray
[redacted]
BeneHeart D3
Monitor
Desl.
AED
1
Desfib manual
Selec energ
−
+
2 Carga
3 Choque
Registrar
Pausa do alarme
Evento
Menu

DC-60

Ultrasound System

Quality Exams at Your Fingertips

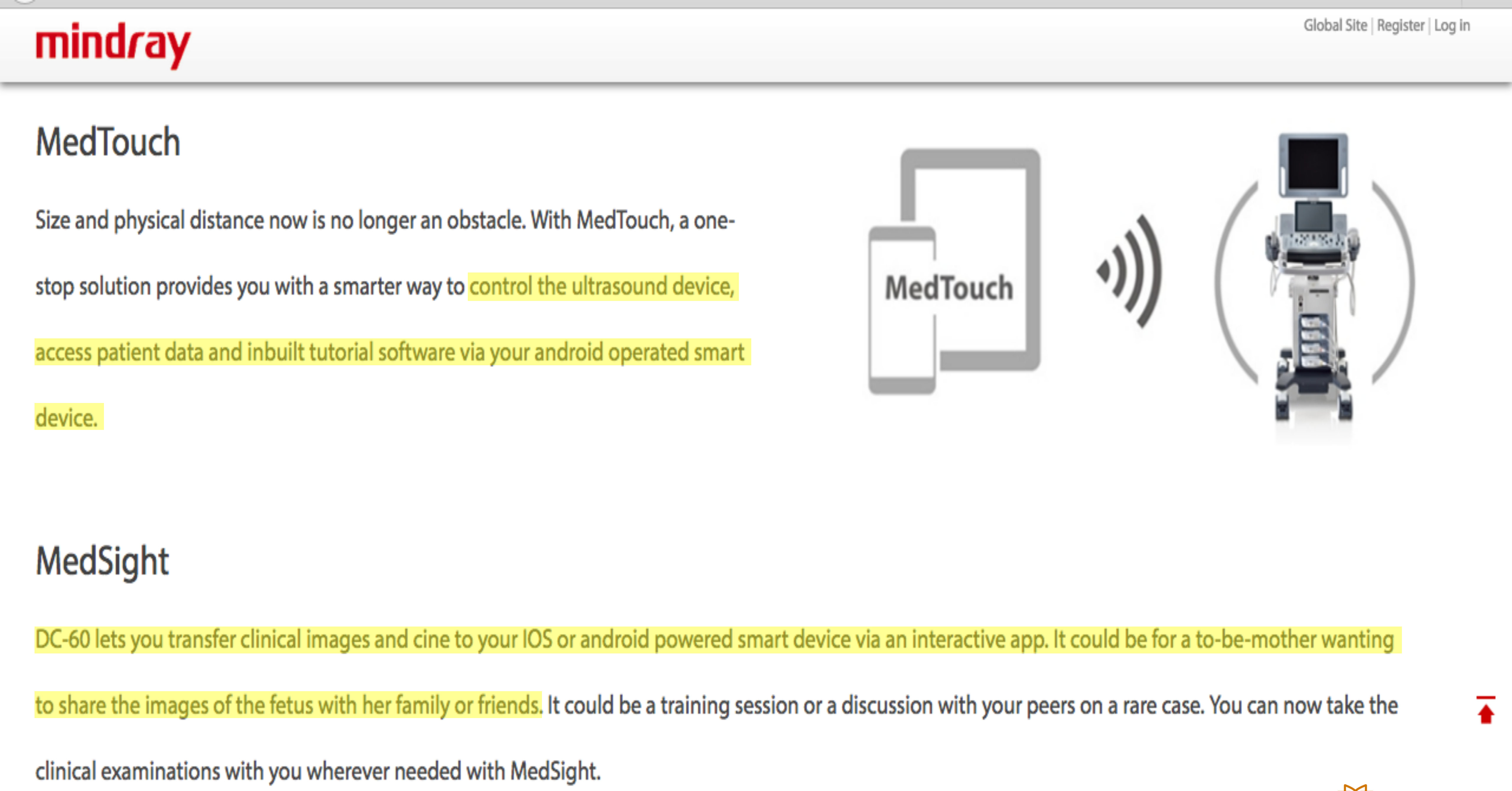


MedTouch

Size and physical distance now is no longer an obstacle. With MedTouch, a one-stop solution provides you with a smarter way to control the ultrasound device, access patient data and inbuilt tutorial software via your android operated smart device.

MedSight

DC-60 lets you transfer clinical images and cine to your IOS or android powered smart device via an interactive app. It could be for a to-be-mother wanting to share the images of the fetus with her family or friends. It could be a training session or a discussion with your peers on a rare case. You can now take the clinical examinations with you wherever needed with MedSight.

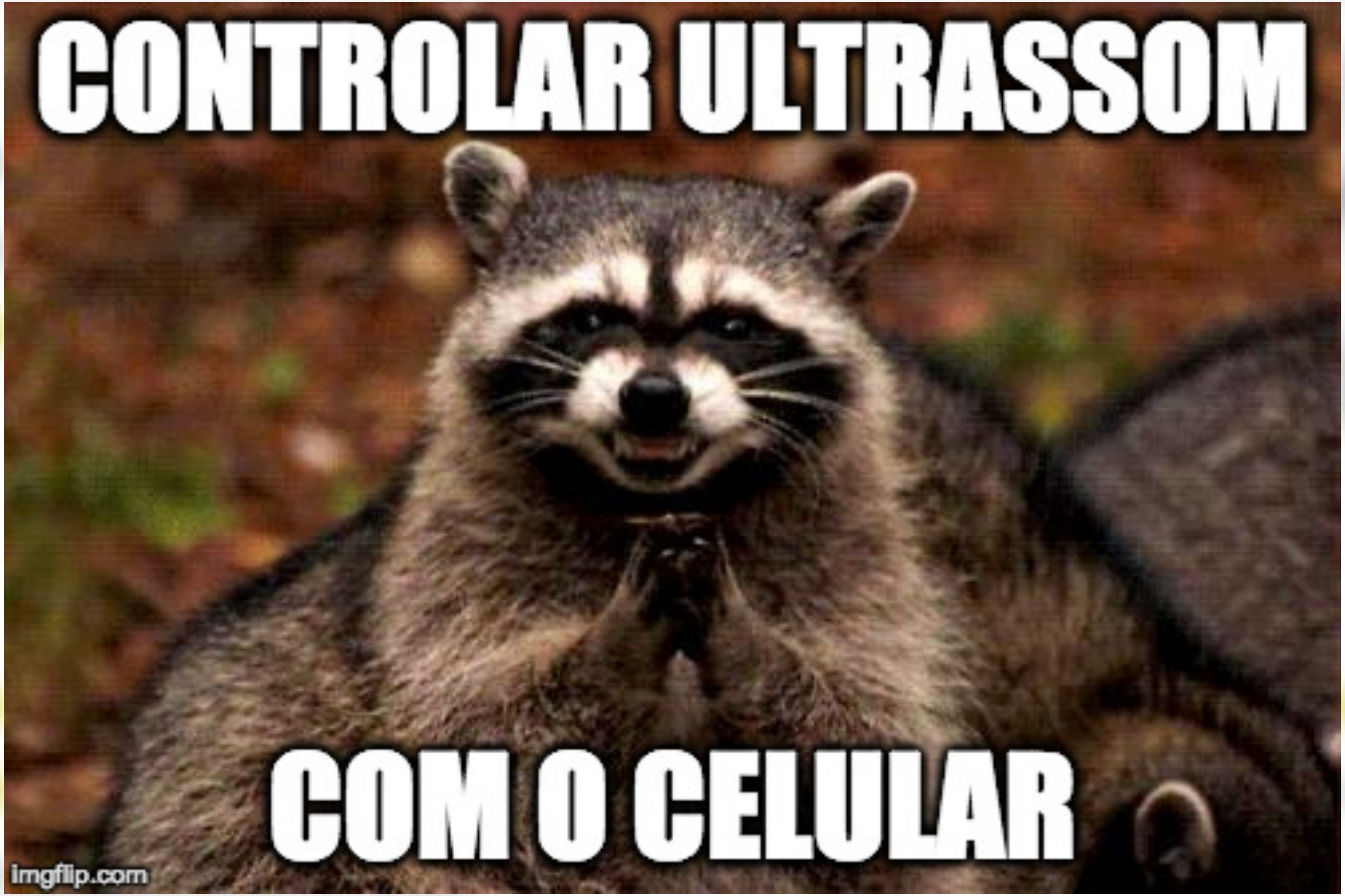


MedTouch

Size and physical distance now is no longer an obstacle. With MedTouch, a one-stop solution provides you with a smarter way to control the ultrasound device, access patient data and inbuilt tutorial software via your android operated smart device.

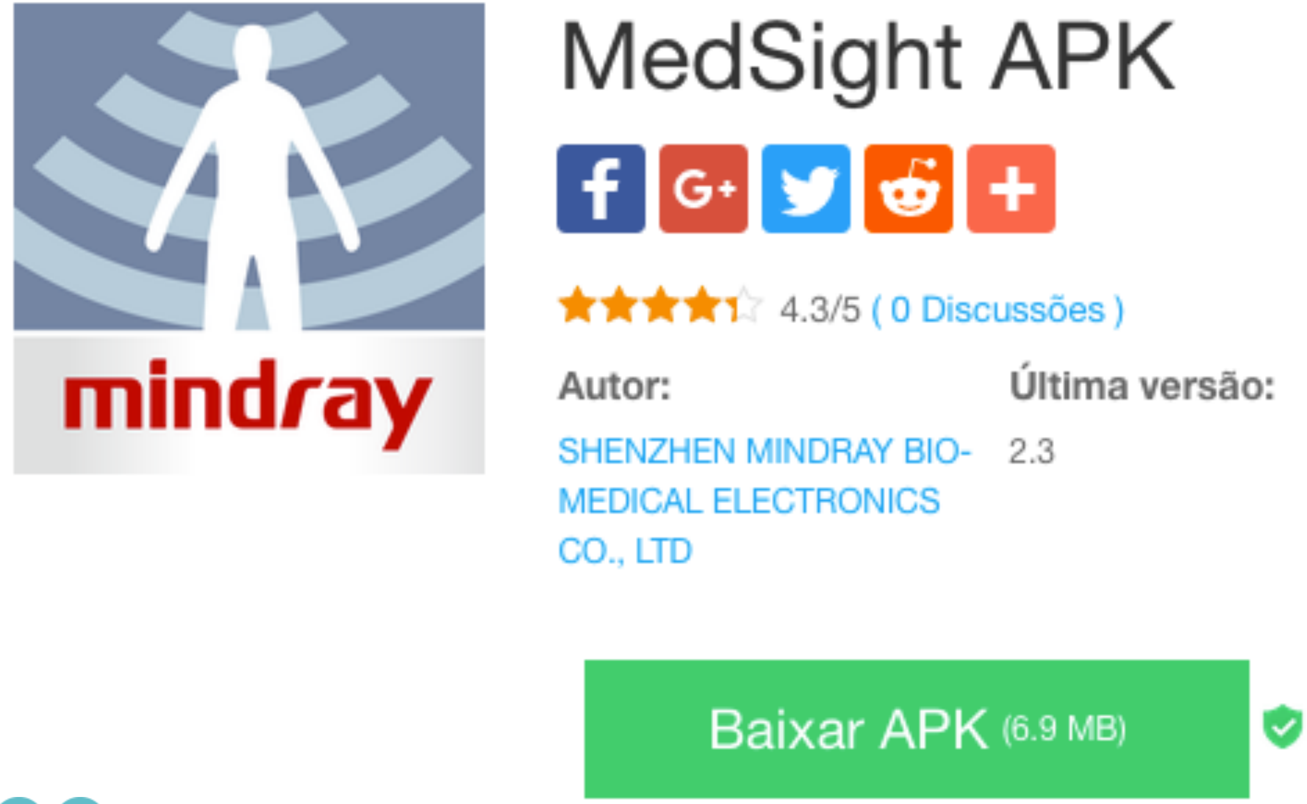
MedSight

DC-60 lets you transfer clinical images and cine to your IOS or android powered smart device via an interactive app. It could be for a to-be-mother wanting to share the images of the fetus with her family or friends. It could be a training session or a discussion with your peers on a rare case. You can now take the clinical examinations with you wherever needed with MedSight.


CONTROLAR ULTRASSOM
COM O CELULAR
imgflip.com

Mindray: MedSight

Decompile do app



MedSight APK

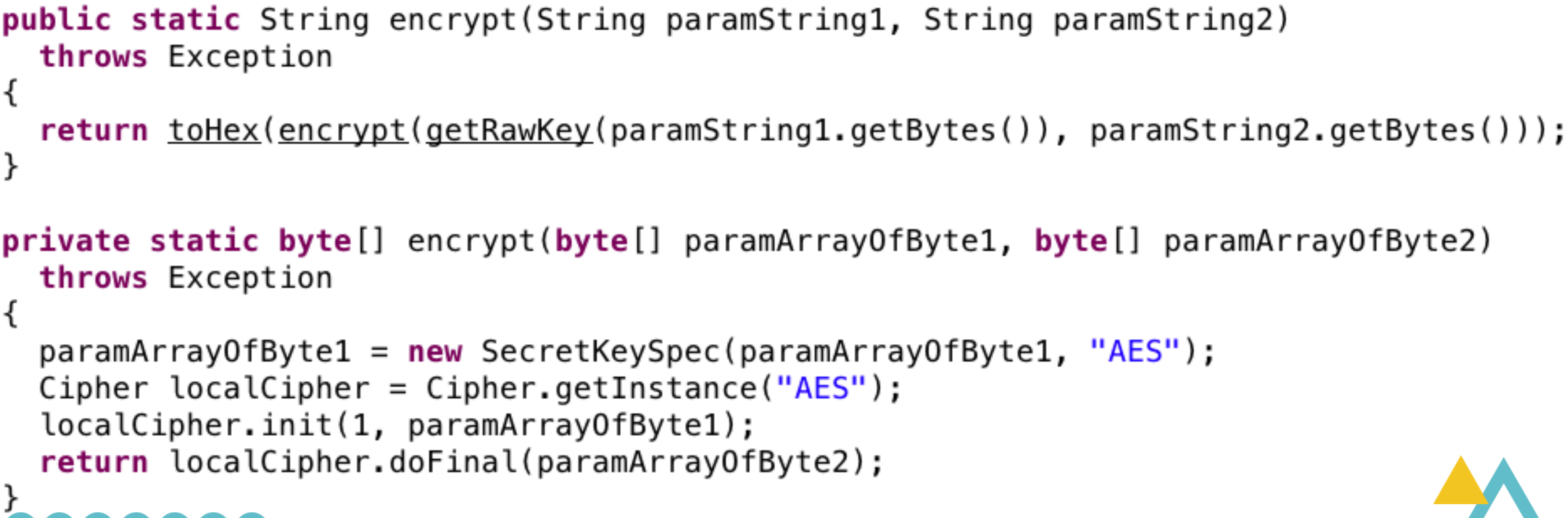
★★★★☆ 4.3/5 (0 Discussões)

Autor:	Última versão:	Data de publicação:
SHENZHEN MINDRAY BIO-MEDICAL ELECTRONICS CO., LTD	2.3	2017-08-22

Baixar APK (6.9 MB)

Mindray: MedSight

Decompile do app (2)

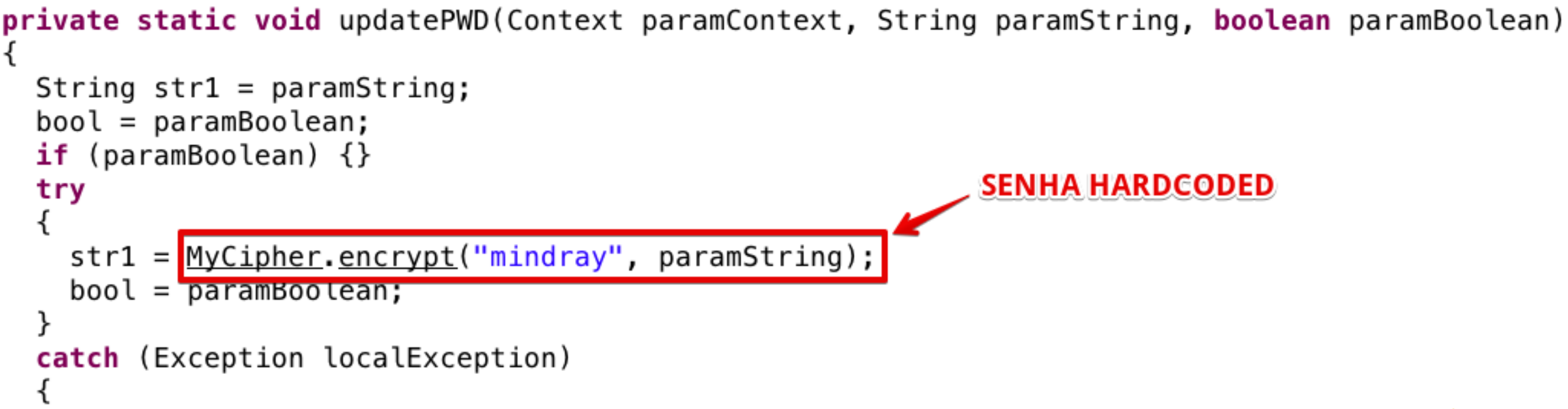


```
public static String encrypt(String paramString1, String paramString2)
  throws Exception
{
  return toHex(encrypt(getRawKey(paramString1.getBytes()), paramString2.getBytes()));
}

private static byte[] encrypt(byte[] paramArrayOfByte1, byte[] paramArrayOfByte2)
  throws Exception
{
  paramArrayOfByte1 = new SecretKeySpec(paramArrayOfByte1, "AES");
  Cipher localCipher = Cipher.getInstance("AES");
  localCipher.init(1, paramArrayOfByte1);
  return localCipher.doFinal(paramArrayOfByte2);
}
```

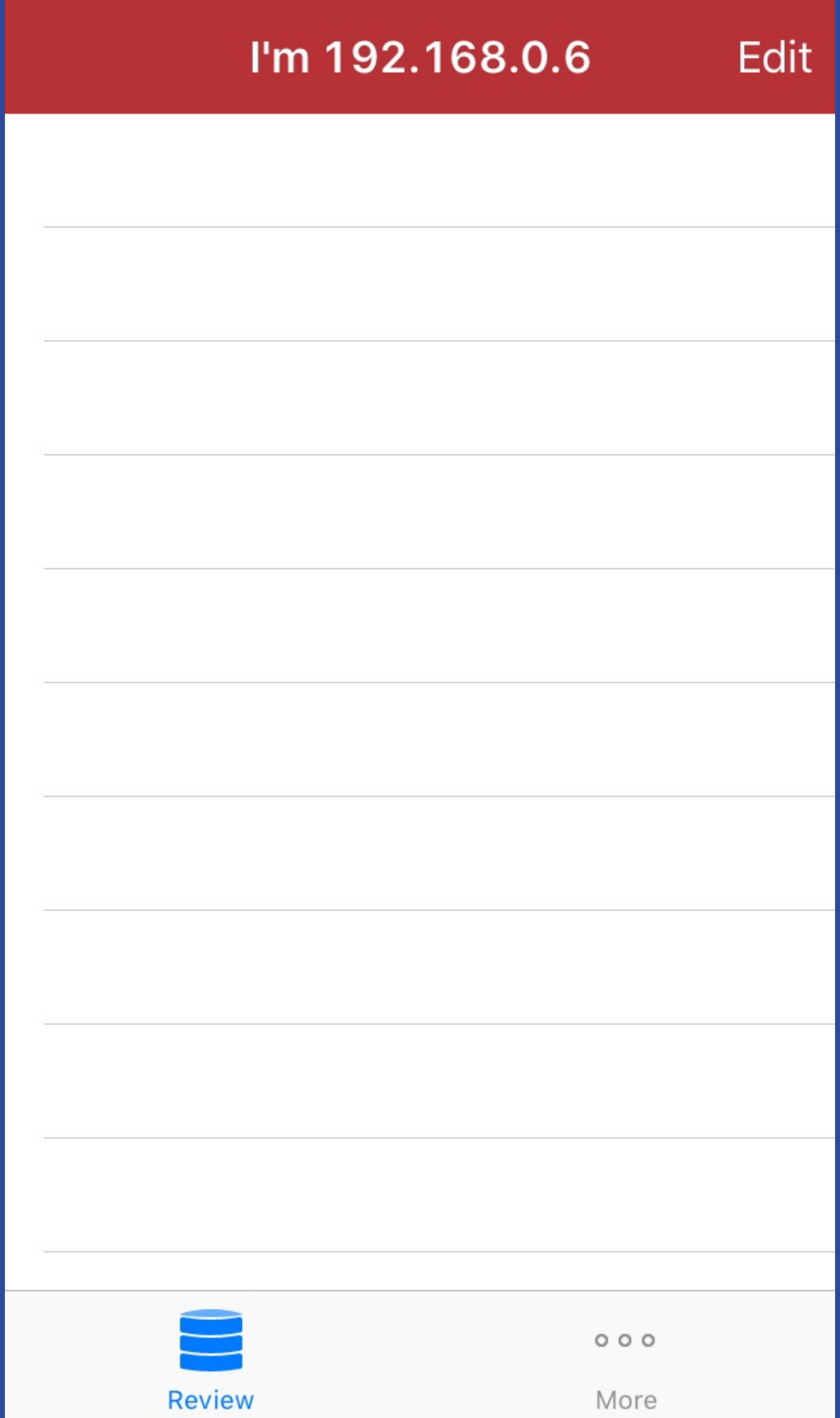
Mindray: MedSight

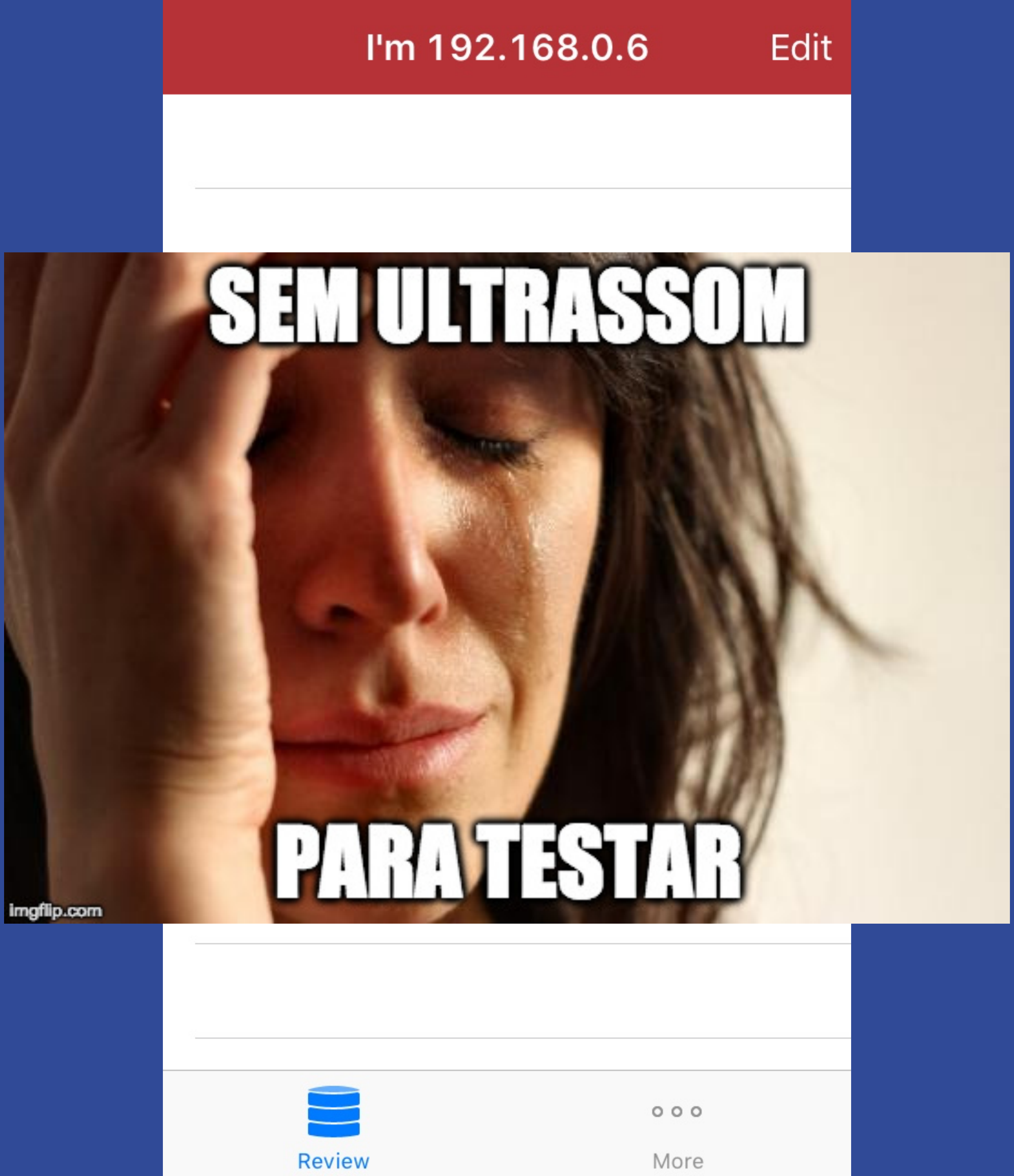
Decompile do app (3)

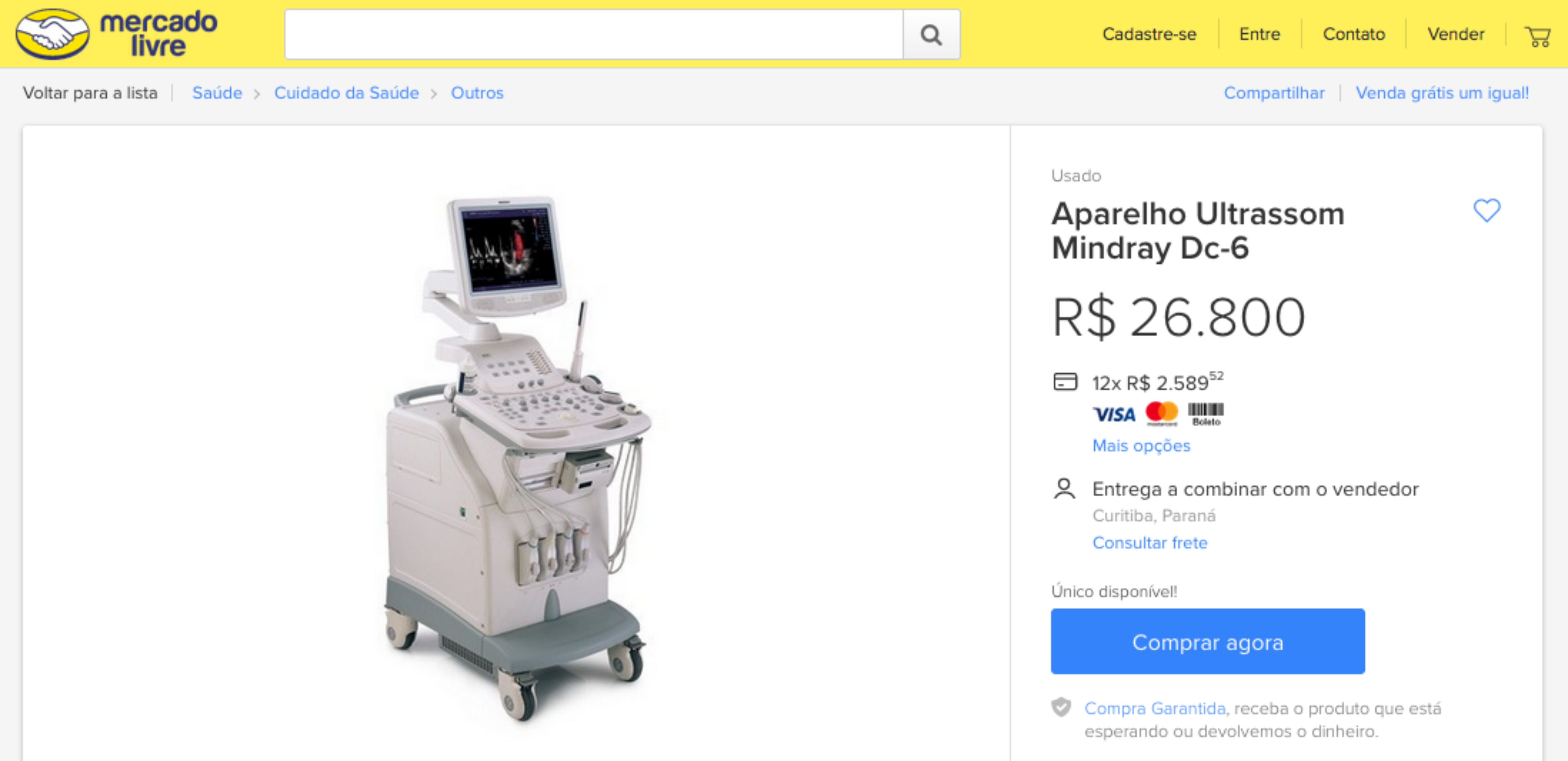


```java
private static void updatePWD(Context paramContext, String paramString, boolean paramBoolean)
{
  String str1 = paramString;
  bool = paramBoolean;
  if (paramBoolean) {}
  try
  {
    str1 = MyCipher.encrypt("mindray", paramString);
    bool = paramBoolean;
  }
  catch (Exception localException)
  {
```

SENHA HARDCODED


I'm 192.168.0.6
Edit
Review
More


I'm 192.168.0.6
Edit
SEM ULTRASSOM
PARA TESTAR
imgflip.com
Review
More



Usado

Aparelho Ultrassom Mindray Dc-6

R$ 26.800

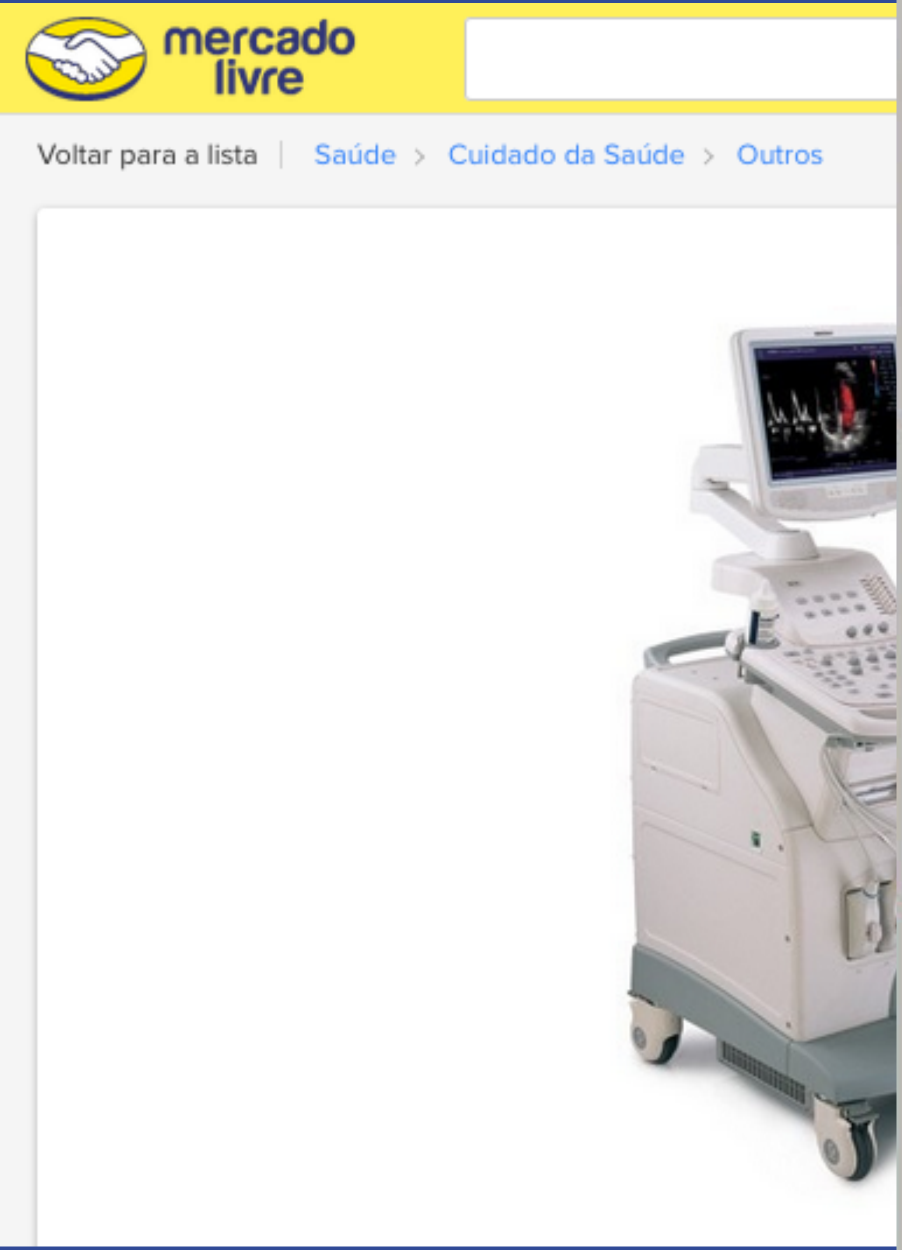
12x R$ 2.589⁵²

Entrega a combinar com o vendedor

Curitiba, Paraná

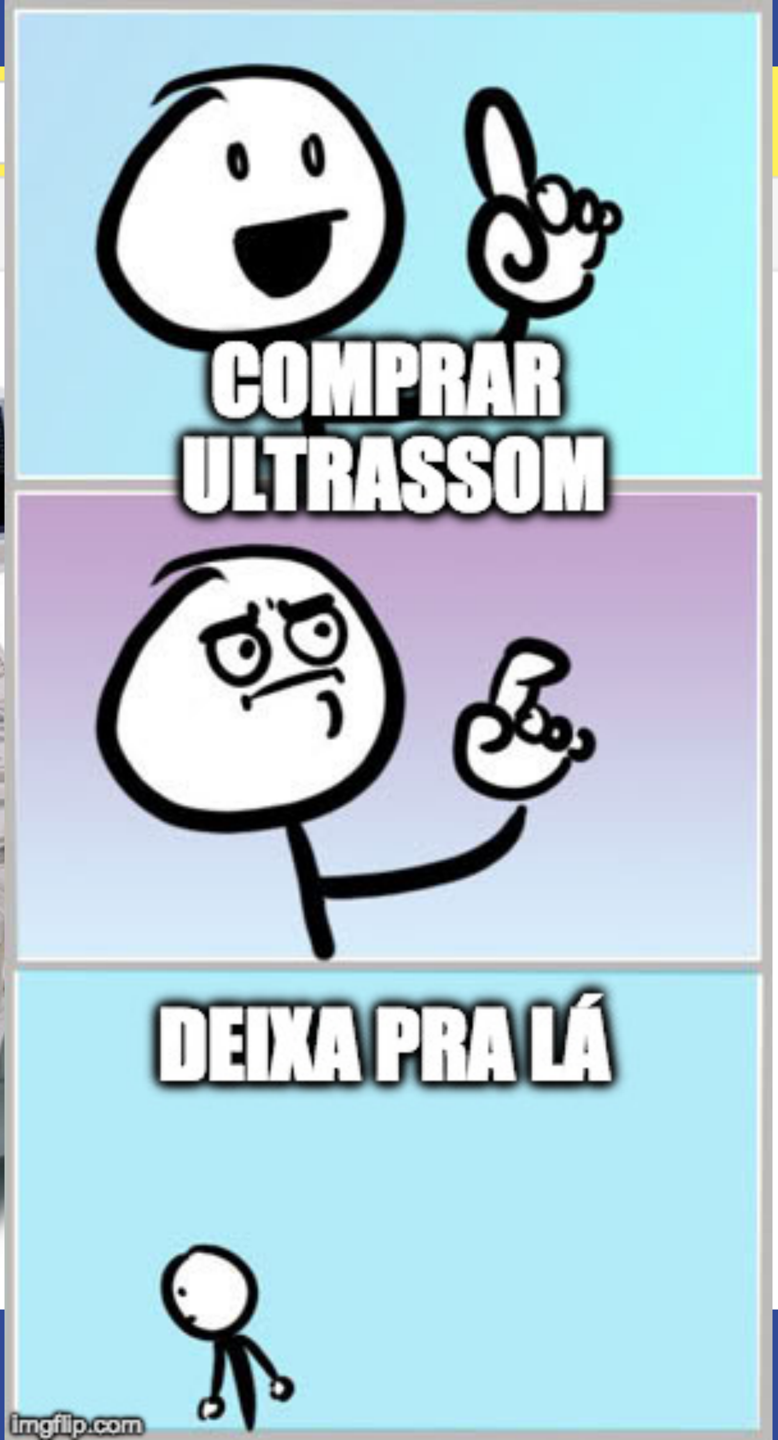
Único disponível!

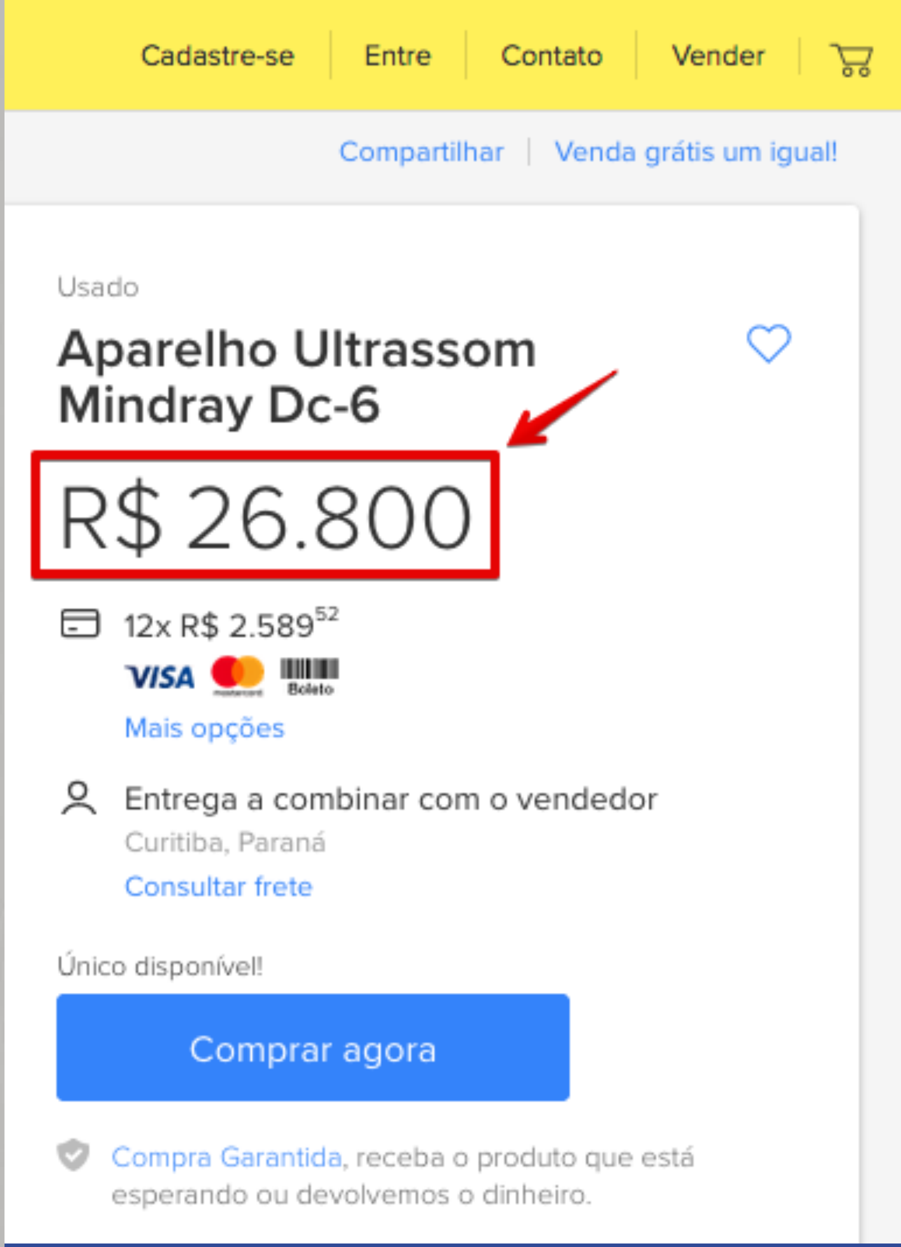
Compra Garantida, receba o produto que está esperando ou devolvemos o dinheiro.



mercado livre

Voltar para a lista | Saúde > Cuidado da Saúde > Outros





Cadastre-se | Entre | Contato | Vender

Compartilhar | Venda grátis um igual!

Usado

Aparelho Ultrassom Mindray Dc-6

R$ 26.800

12x R$ 2.589 52

VISA Boleto

Mais opções

Entrega a combinar com o vendedor

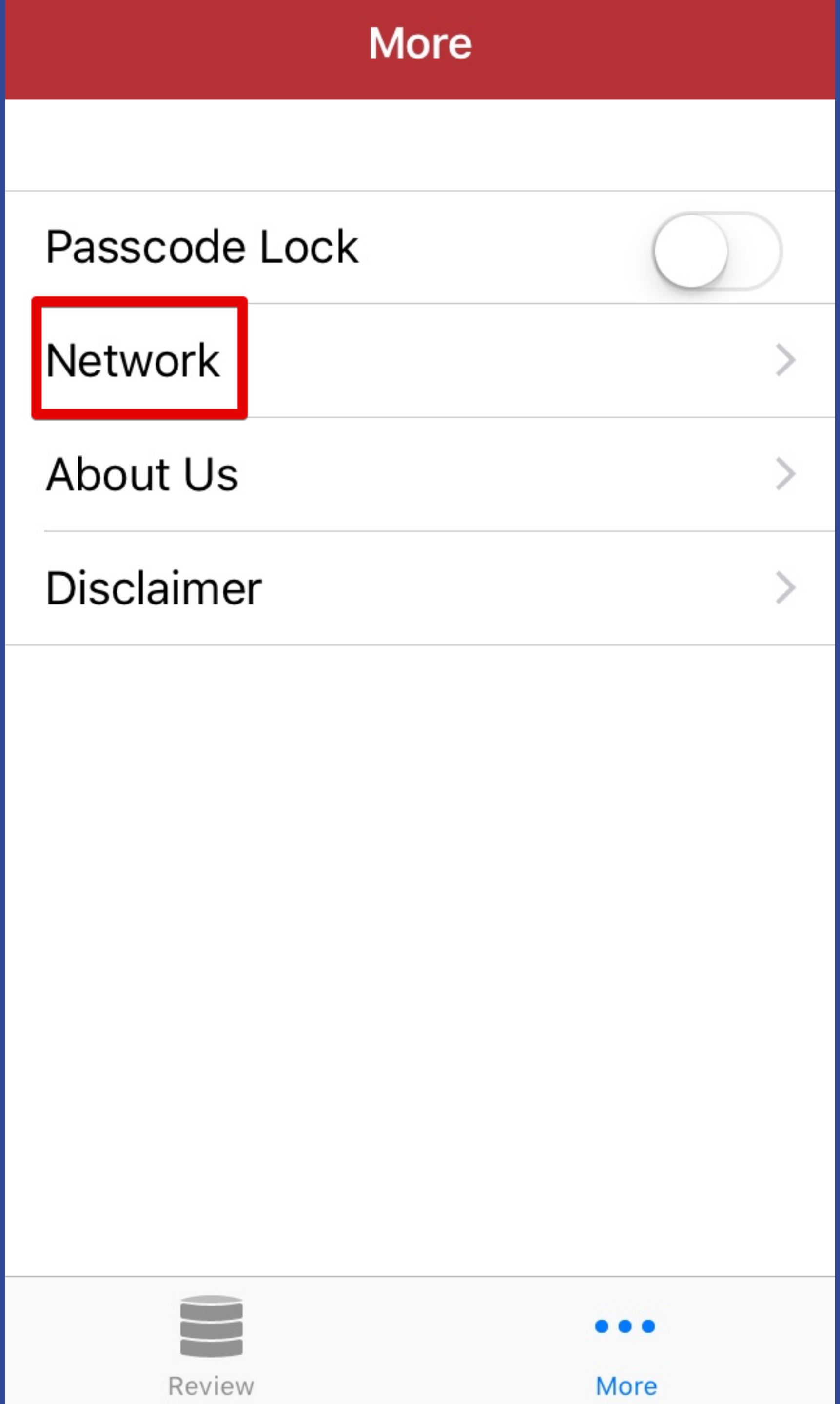
Curitiba, Paraná

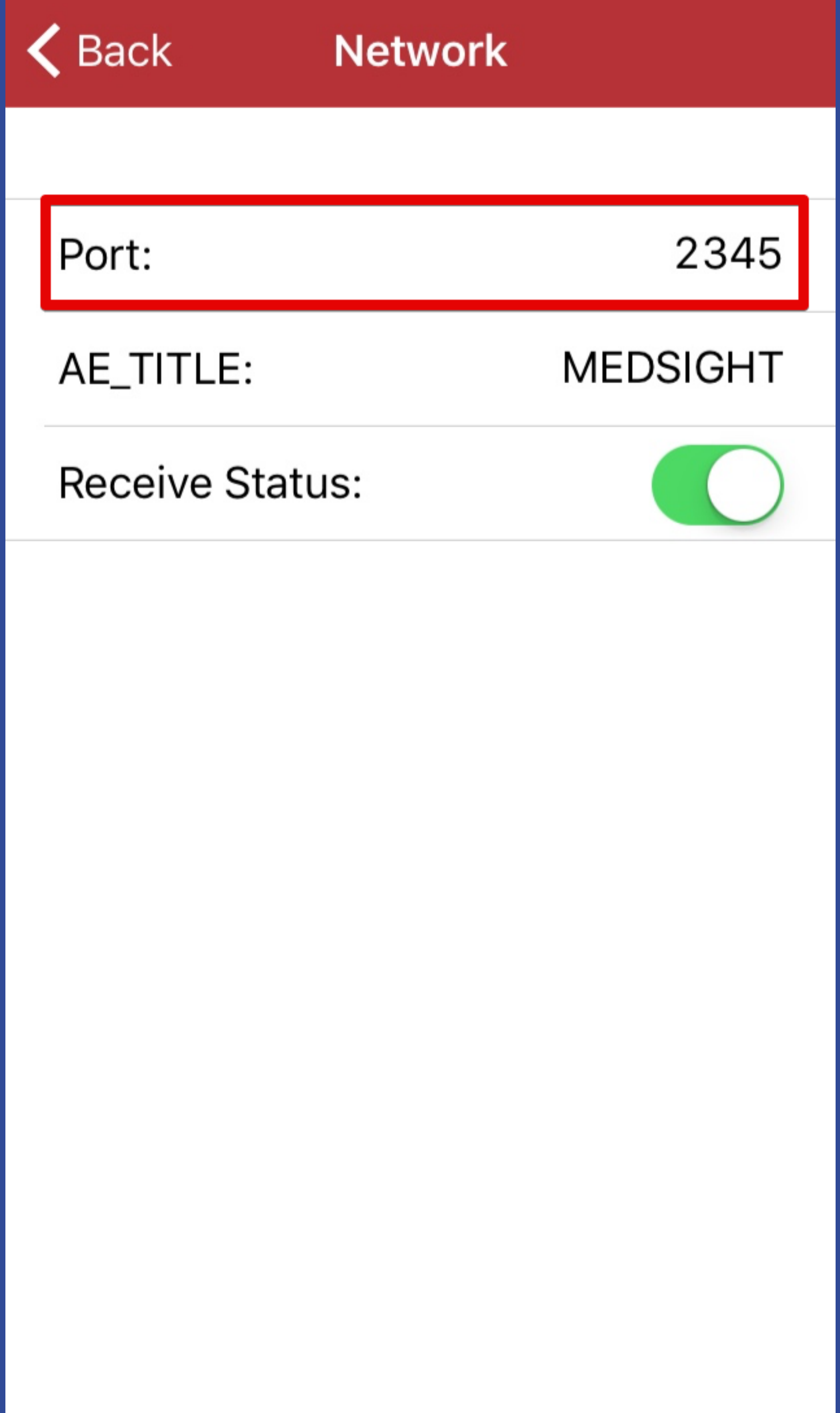
Consultar frete

Único disponível!

Comprar agora

Compra Garantida, receba o produto que está esperando ou devolvemos o dinheiro.

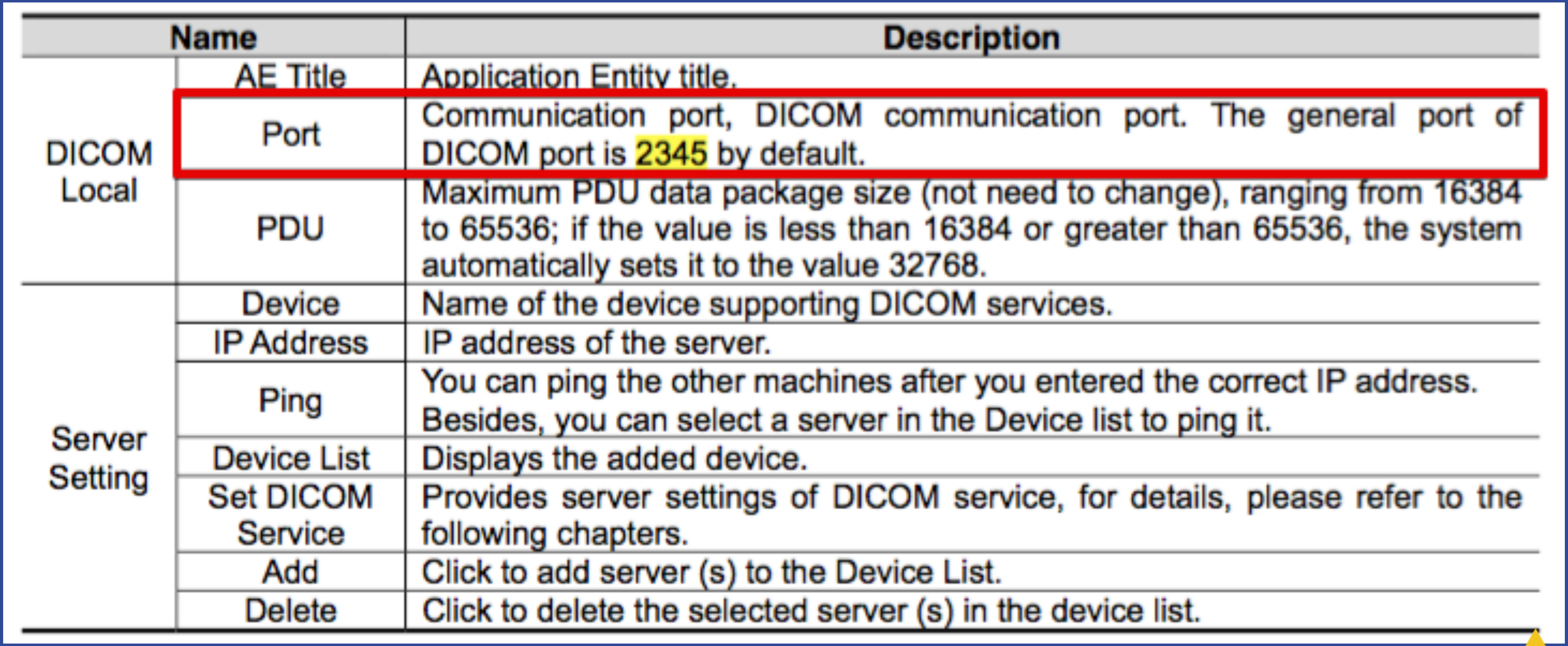




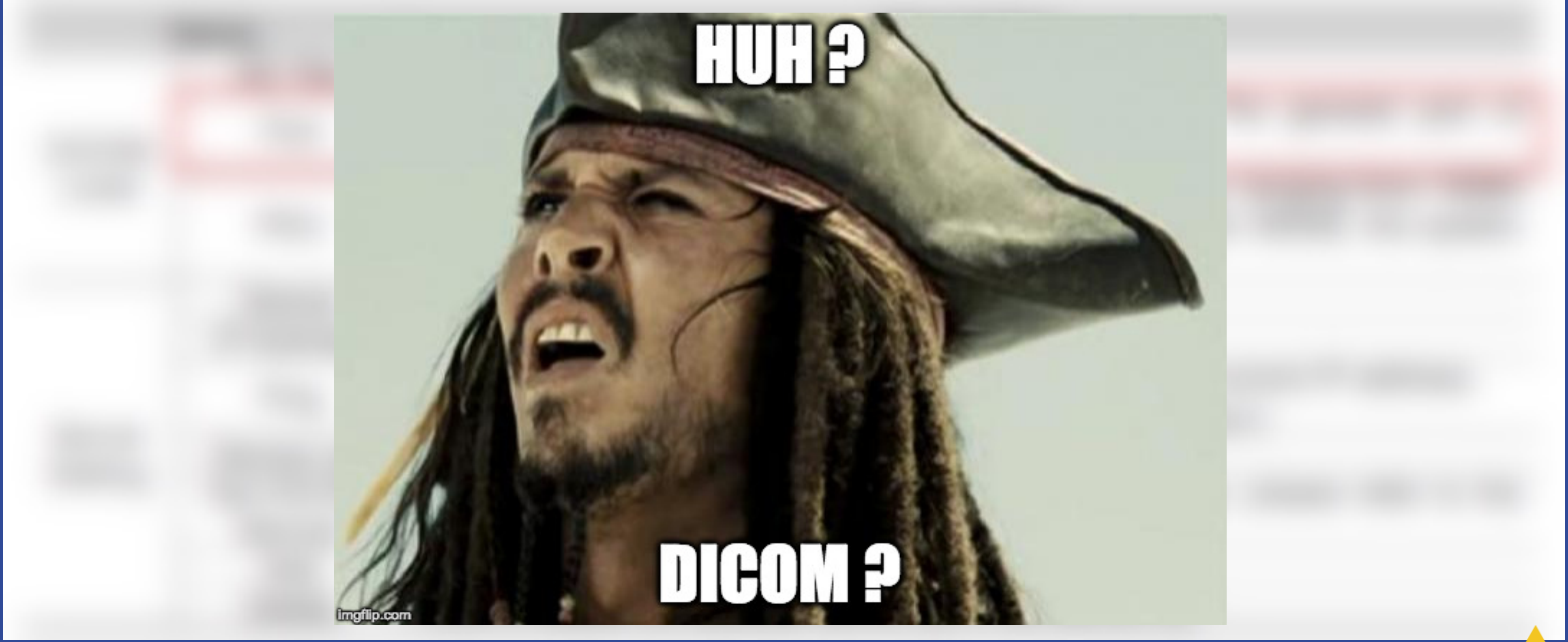
Port: 2345

AE_TITLE: MEDSIGHT

Receive Status: ●



Name		Description
DICOM Local	AE Title	Application Entity title.
	Port	Communication port, DICOM communication port. The general port of DICOM port is 2345 by default.
	PDU	Maximum PDU data package size (not need to change), ranging from 16384 to 65536; if the value is less than 16384 or greater than 65536, the system automatically sets it to the value 32768.
Server Setting	Device	Name of the device supporting DICOM services.
	IP Address	IP address of the server.
	Ping	You can ping the other machines after you entered the correct IP address. Besides, you can select a server in the Device list to ping it.
	Device List	Displays the added device.
	Set DICOM Service	Provides server settings of DICOM service, for details, please refer to the following chapters.
	Add	Click to add server (s) to the Device List.
	Delete	Click to delete the selected server (s) in the device list.

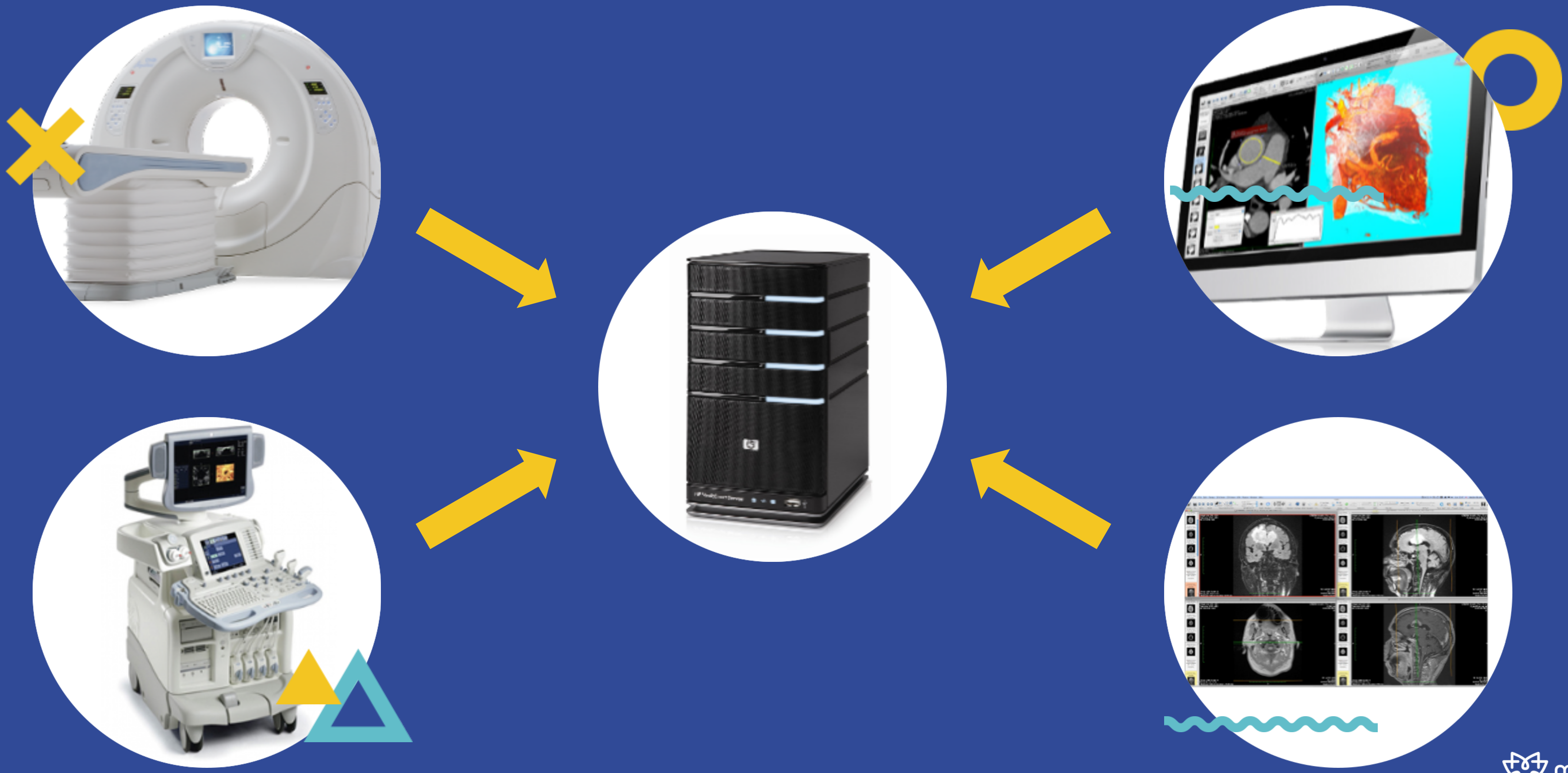

HUH ?
DICOM ?
imgflip.com

Digital Imaging and Communications in Medicine (DICOM)

MORPHUS
SEGURANÇA DA INFORMAÇÃO

Formato de Arquivo & Protocolo de Rede

Cenário Básico (PACS)



DICOM

Padrão desenvolvido por:

- American College of Radiology (ACR)
- National Electrical Manufacturers Association (NEMA)

Histórico

- Primeira versão foi lançada em 1985 !
- Recebeu o nome "DICOM" na terceira versão (1993)
- Documentação oficial atual é dividida em 20 volumes !

Recomendação de leitura

- PIANYKH, Oleg S. **Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide**. Springer Science & Business Media, 2009.

ACR-NEMA STANDARDS PUBLICATION/ NO. 300-1985

nema

Digital Imaging
and
Communications

NEMA

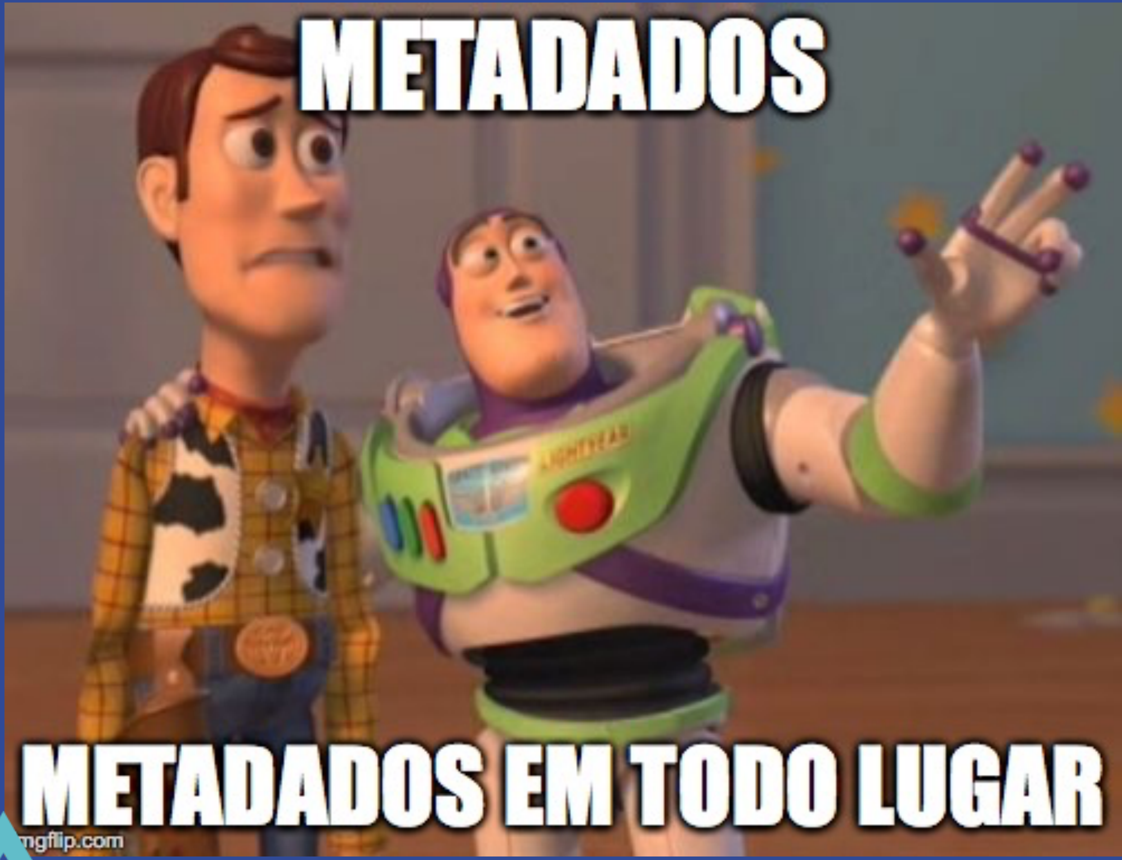
NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION ■ 2101 L STREET, N.W., WASHINGTON, D.C. 20037

MORPHUS
SEGURANÇA DA INFORMAÇÃO

DICOM

Information Object Definitions (IOD)

- Coleção de atributos que representam um objeto do mundo real
- DICOM mantém uma lista de atributos (mais de 2000!)
- Exemplo: Patient IOD
  - ID
  - Nome
  - Idade
  - Peso
  - Entre outros...



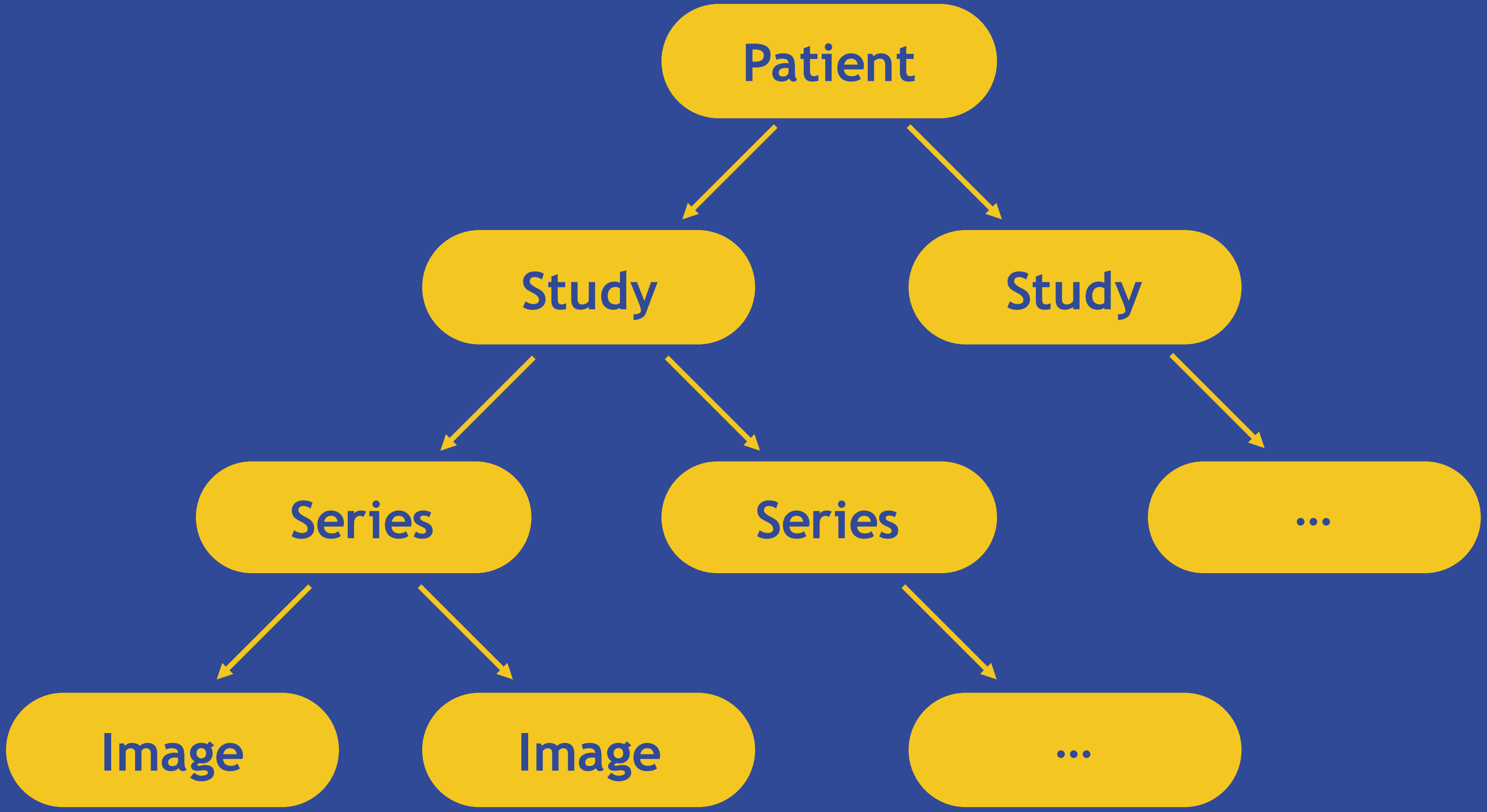
DICOM

Hierarquia de Dados

- DICOM utiliza uma estrutura de informações
- Tipos de dados
  - Patient
  - Study
  - Series
  - Images

DICOM

Hierarquia de Dados



DICOM

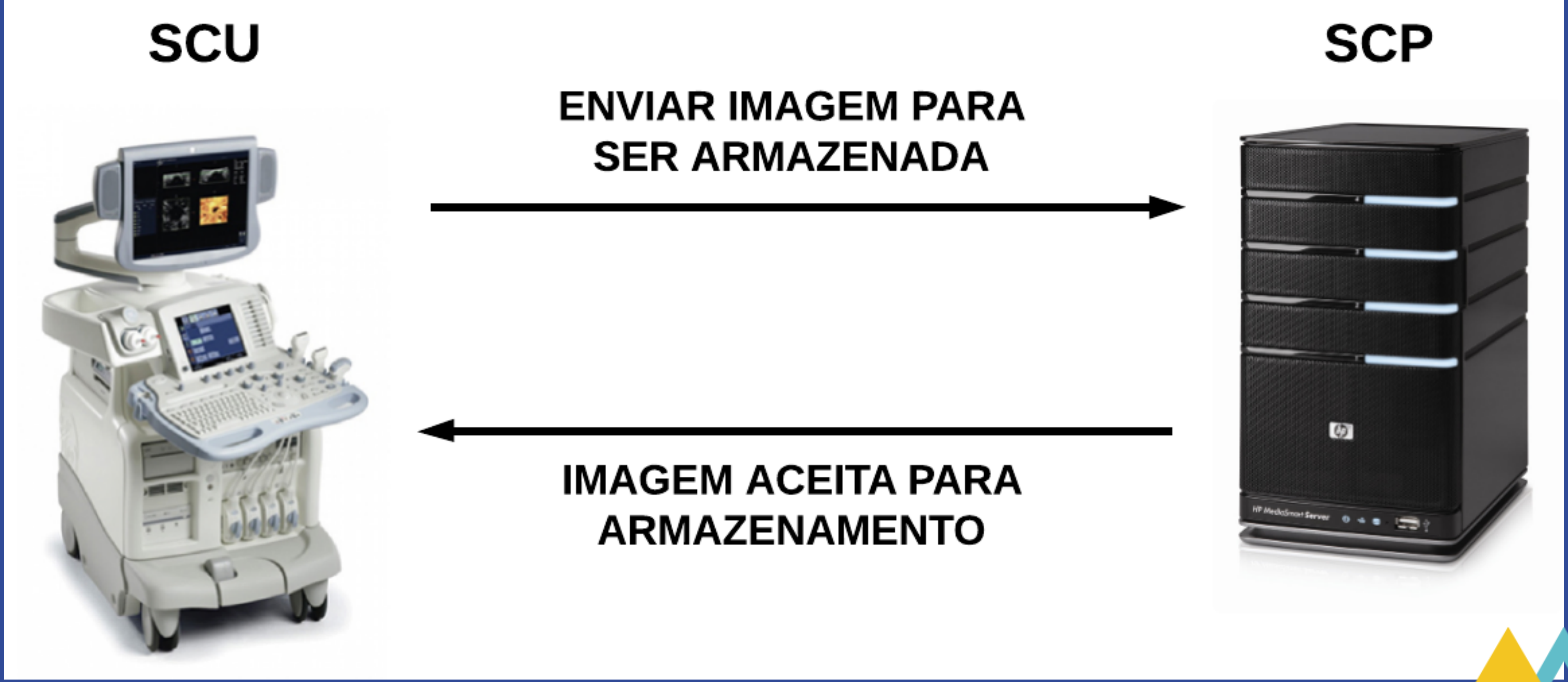
Application Entities (AE)

- Dispositivos e/ou softwares que executam DICOM
- AEs podem oferecer serviços para outros AEs
  - Exemplo: Transmissão de imagens
  - AE Cliente: Service Class User (SCU)
  - AE Servidor: Service Class Provider (SCP)

Service Object Pairs (SOP)

- Associa tipos de serviços com atributos específicos

DICOM



SCU

SCP

ENVIAR IMAGEM PARA SER ARMAZENADA

IMAGEM ACEITA PARA ARMAZENAMENTO

DICOM

DICOM Message Service Elements (DIMSE)

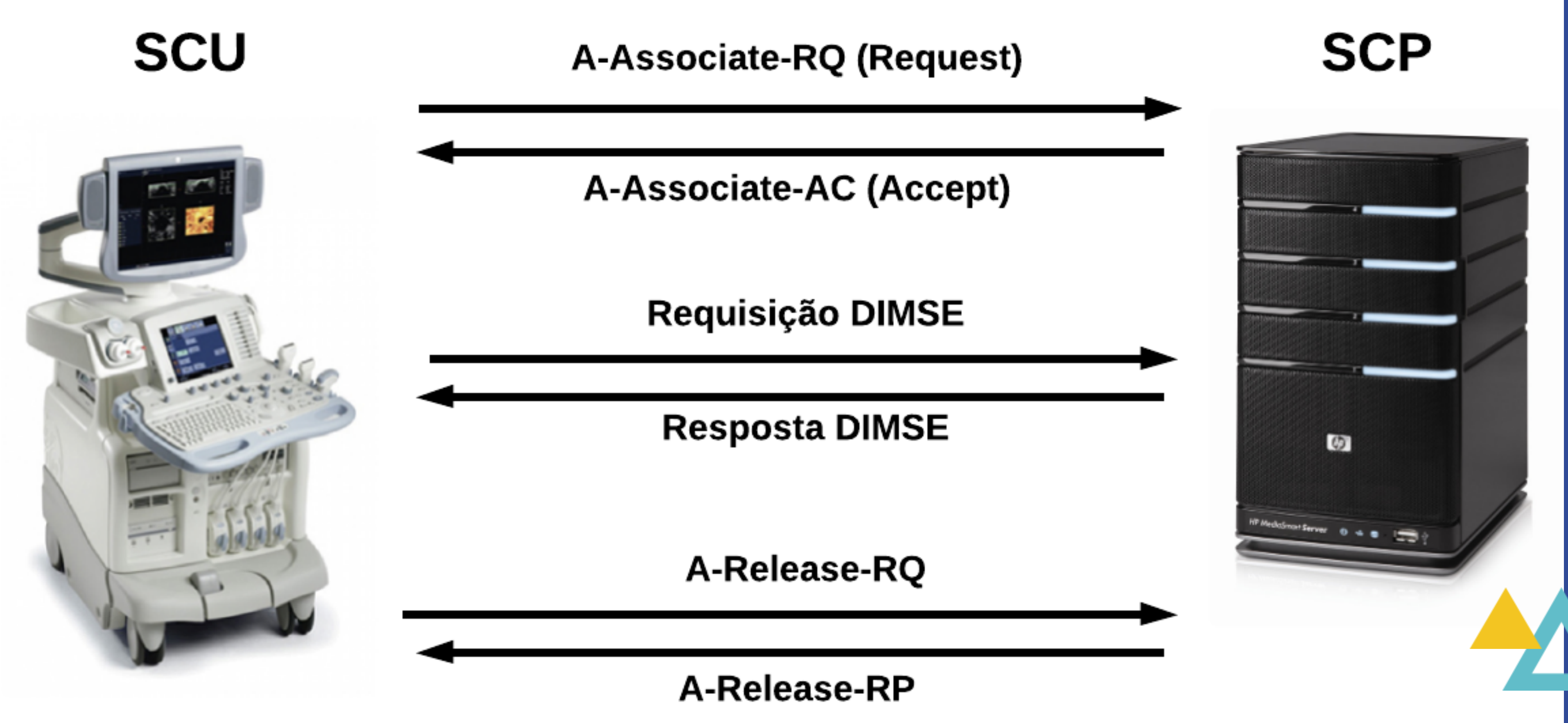
- Mensagens contendo comandos de serviços
- Possui formatos para requisições e respostas
- Exemplo de DIMSE:
  - C-Store-Req / C-Store-Rsp

Dados básicos para conexão

- Endereço IP
- Número de porta: 104/TCP (Porta padrão)
- Nome do AE (AE Title)

DICOM

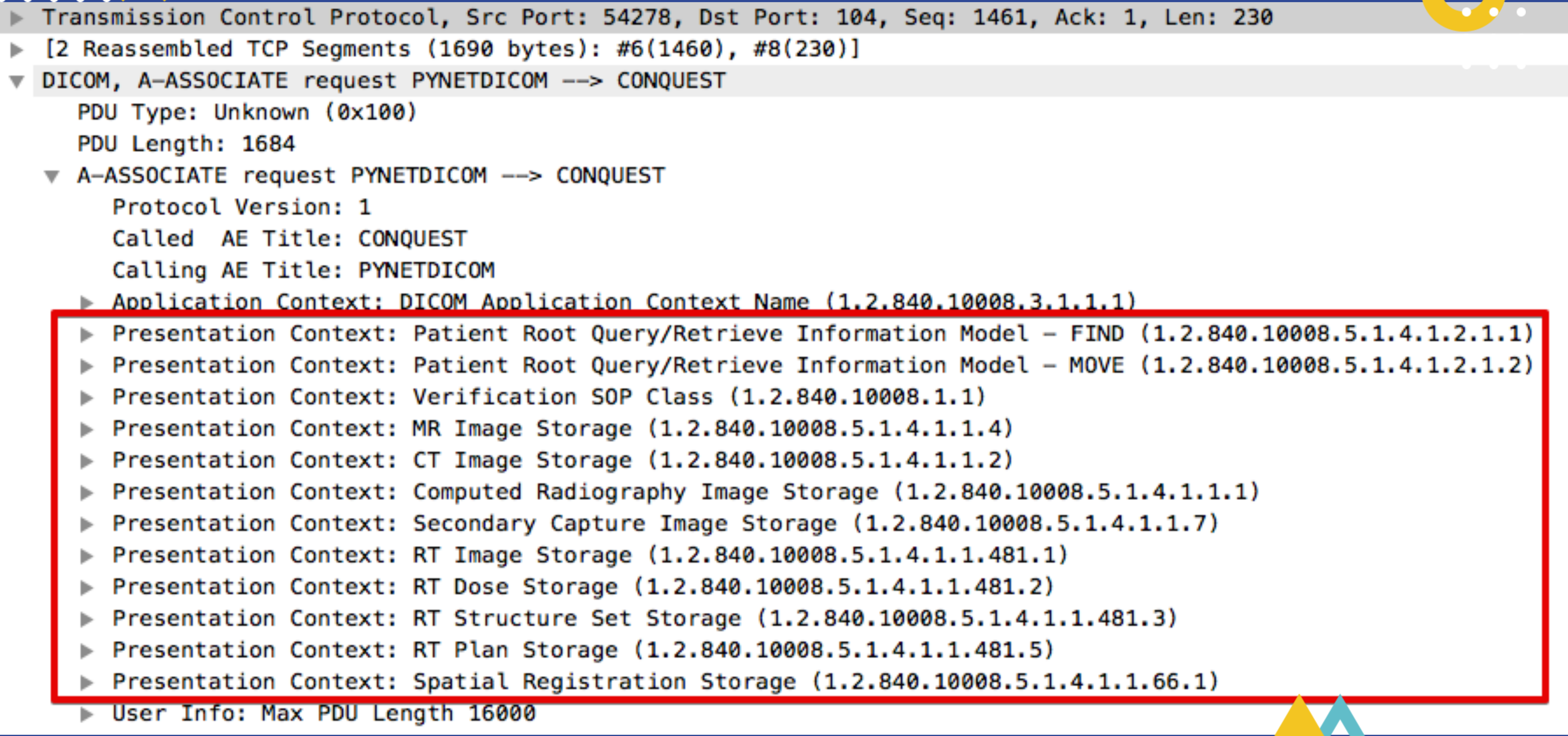
Conexão básica entre SCU e SCP



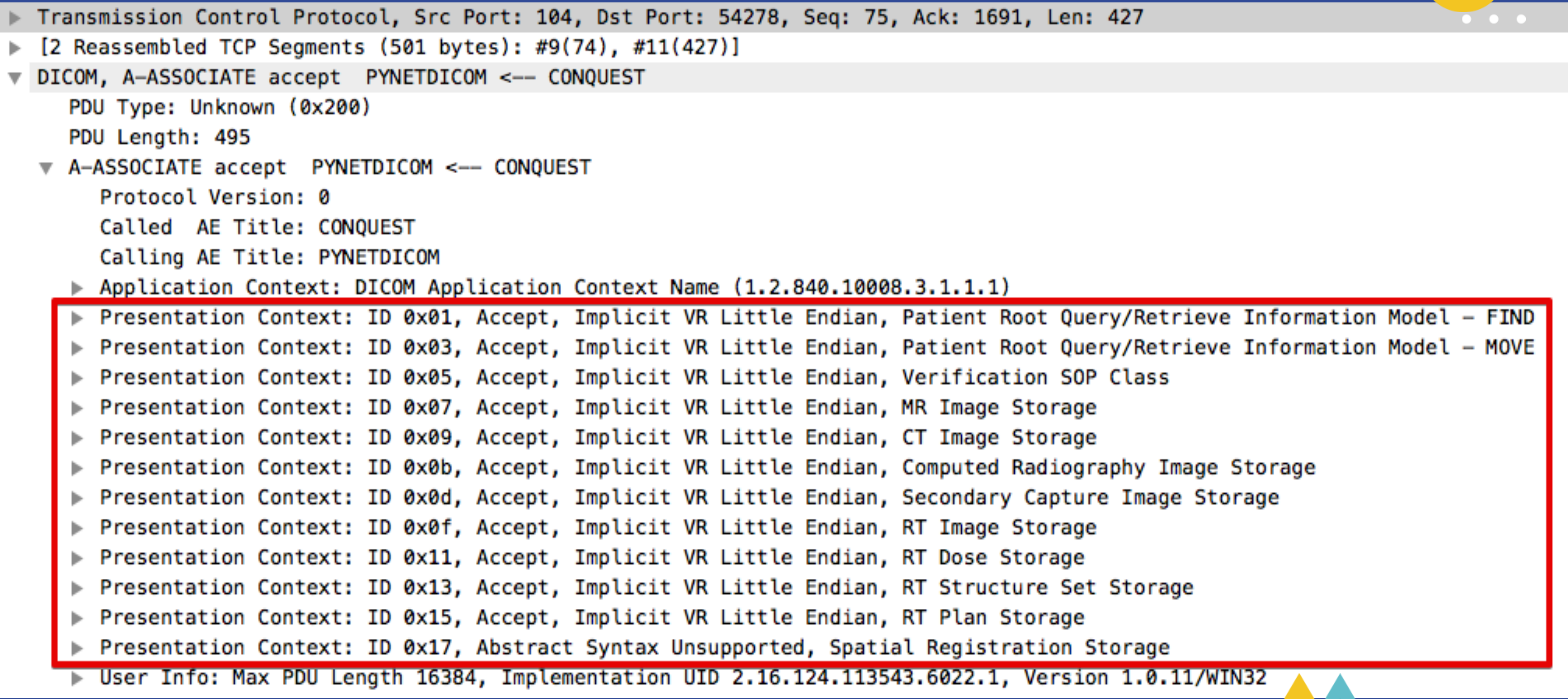
DICOM

Associação

- Handshake realizado entre SCU e SCP
- Troca de informações
  - Identificação de dispositivos
  - Lista de serviços disponíveis
- Tipos de mensagens:
  - A-Associate-RQ
  - A-Associate-AC
  - A-Associate-RJ



```
▶ Transmission Control Protocol, Src Port: 54278, Dst Port: 104, Seq: 1461, Ack: 1, Len: 230
▶ [2 Reassembled TCP Segments (1690 bytes): #6(1460), #8(230)]
▼ DICOM, A-ASSOCIATE request PYNETDICOM --> CONQUEST
    PDU Type: Unknown (0x100)
    PDU Length: 1684
  ▼ A-ASSOCIATE request PYNETDICOM --> CONQUEST
      Protocol Version: 1
      Called  AE Title: CONQUEST
      Calling AE Title: PYNETDICOM
    ▶ Application Context: DICOM Application Context Name (1.2.840.10008.3.1.1.1)
    ▶ Presentation Context: Patient Root Query/Retrieve Information Model - FIND (1.2.840.10008.5.1.4.1.2.1.1)
    ▶ Presentation Context: Patient Root Query/Retrieve Information Model - MOVE (1.2.840.10008.5.1.4.1.2.1.2)
    ▶ Presentation Context: Verification SOP Class (1.2.840.10008.1.1)
    ▶ Presentation Context: MR Image Storage (1.2.840.10008.5.1.4.1.1.4)
    ▶ Presentation Context: CT Image Storage (1.2.840.10008.5.1.4.1.1.2)
    ▶ Presentation Context: Computed Radiography Image Storage (1.2.840.10008.5.1.4.1.1.1)
    ▶ Presentation Context: Secondary Capture Image Storage (1.2.840.10008.5.1.4.1.1.7)
    ▶ Presentation Context: RT Image Storage (1.2.840.10008.5.1.4.1.1.481.1)
    ▶ Presentation Context: RT Dose Storage (1.2.840.10008.5.1.4.1.1.481.2)
    ▶ Presentation Context: RT Structure Set Storage (1.2.840.10008.5.1.4.1.1.481.3)
    ▶ Presentation Context: RT Plan Storage (1.2.840.10008.5.1.4.1.1.481.5)
    ▶ Presentation Context: Spatial Registration Storage (1.2.840.10008.5.1.4.1.1.66.1)
    ▶ User Info: Max PDU Length 16000
```



```
▶ Transmission Control Protocol, Src Port: 104, Dst Port: 54278, Seq: 75, Ack: 1691, Len: 427
▶ [2 Reassembled TCP Segments (501 bytes): #9(74), #11(427)]
▼ DICOM, A-ASSOCIATE accept  PYNETDICOM <-- CONQUEST
    PDU Type: Unknown (0x200)
    PDU Length: 495
  ▼ A-ASSOCIATE accept  PYNETDICOM <-- CONQUEST
      Protocol Version: 0
      Called  AE Title: CONQUEST
      Calling AE Title: PYNETDICOM
    ▶ Application Context: DICOM Application Context Name (1.2.840.10008.3.1.1.1)
    ▶ Presentation Context: ID 0x01, Accept, Implicit VR Little Endian, Patient Root Query/Retrieve Information Model - FIND
    ▶ Presentation Context: ID 0x03, Accept, Implicit VR Little Endian, Patient Root Query/Retrieve Information Model - MOVE
    ▶ Presentation Context: ID 0x05, Accept, Implicit VR Little Endian, Verification SOP Class
    ▶ Presentation Context: ID 0x07, Accept, Implicit VR Little Endian, MR Image Storage
    ▶ Presentation Context: ID 0x09, Accept, Implicit VR Little Endian, CT Image Storage
    ▶ Presentation Context: ID 0x0b, Accept, Implicit VR Little Endian, Computed Radiography Image Storage
    ▶ Presentation Context: ID 0x0d, Accept, Implicit VR Little Endian, Secondary Capture Image Storage
    ▶ Presentation Context: ID 0x0f, Accept, Implicit VR Little Endian, RT Image Storage
    ▶ Presentation Context: ID 0x11, Accept, Implicit VR Little Endian, RT Dose Storage
    ▶ Presentation Context: ID 0x13, Accept, Implicit VR Little Endian, RT Structure Set Storage
    ▶ Presentation Context: ID 0x15, Accept, Implicit VR Little Endian, RT Plan Storage
    ▶ Presentation Context: ID 0x17, Abstract Syntax Unsupported, Spatial Registration Storage
    ▶ User Info: Max PDU Length 16384, Implementation UID 2.16.124.113543.6022.1, Version 1.0.11/WIN32
```

DICOM

Obtendo imagens

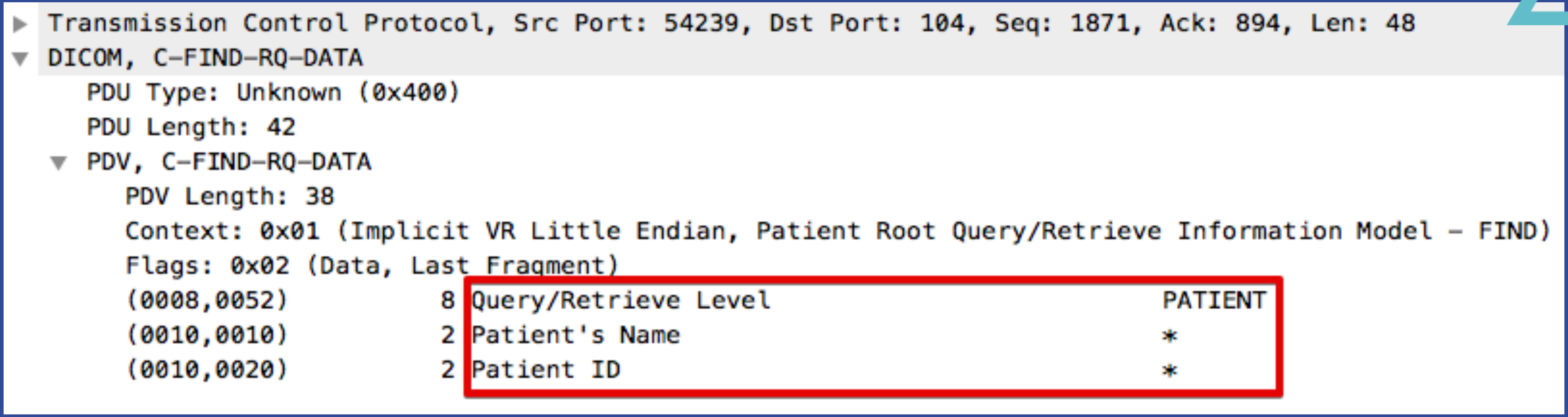
- C-Find
- C-Get
- C-Move

MORPHUS
SEGURANÇA DA INFORMAÇÃO

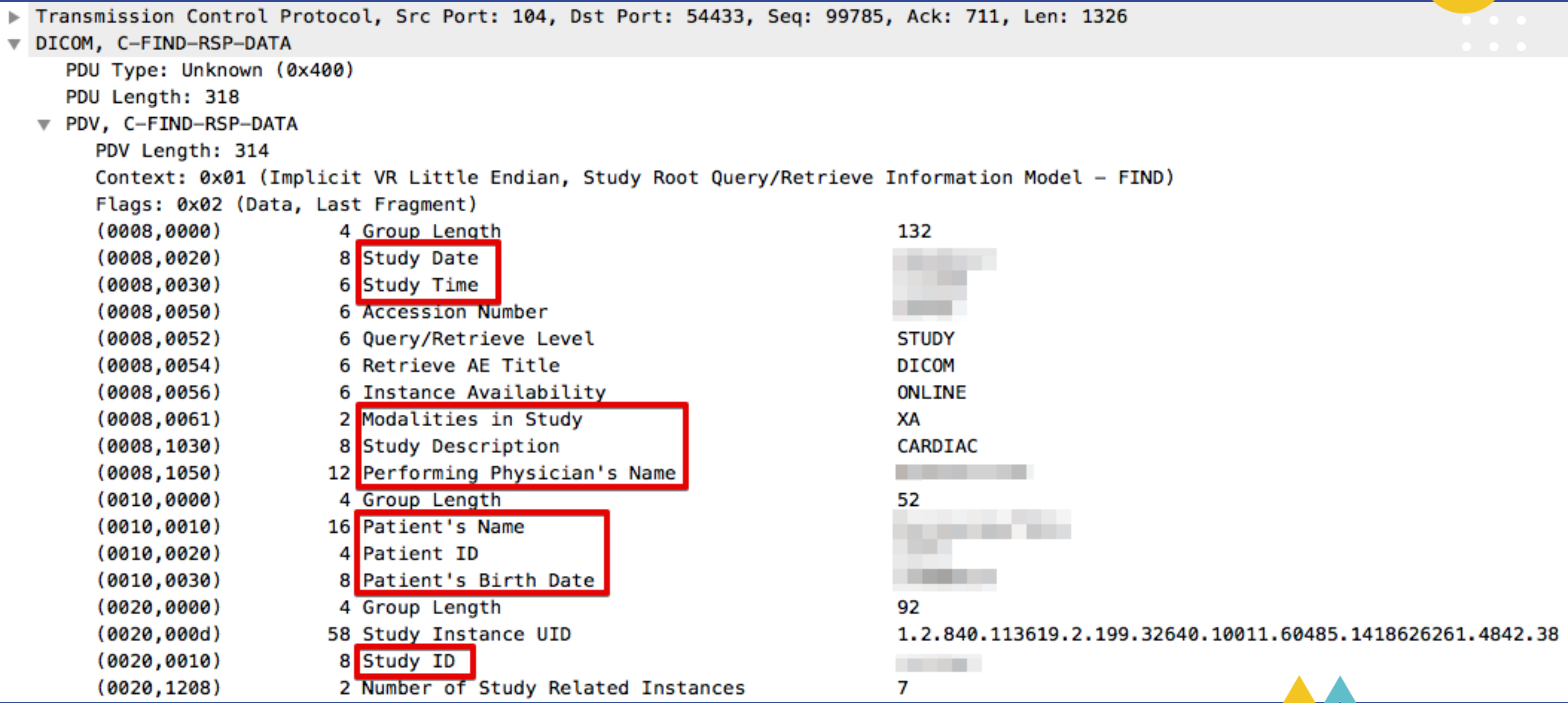
DICOM

C-Find

- Realiza pesquisas baseado em filtros



```
▶ Transmission Control Protocol, Src Port: 54239, Dst Port: 104, Seq: 1871, Ack: 894, Len: 48
▼ DICOM, C-FIND-RQ-DATA
    PDU Type: Unknown (0x400)
    PDU Length: 42
  ▼ PDV, C-FIND-RQ-DATA
      PDV Length: 38
      Context: 0x01 (Implicit VR Little Endian, Patient Root Query/Retrieve Information Model - FIND)
      Flags: 0x02 (Data, Last Fragment)
      (0008,0052)         8 Query/Retrieve Level                          PATIENT
      (0010,0010)         2 Patient's Name                                *
      (0010,0020)         2 Patient ID                                    *
```

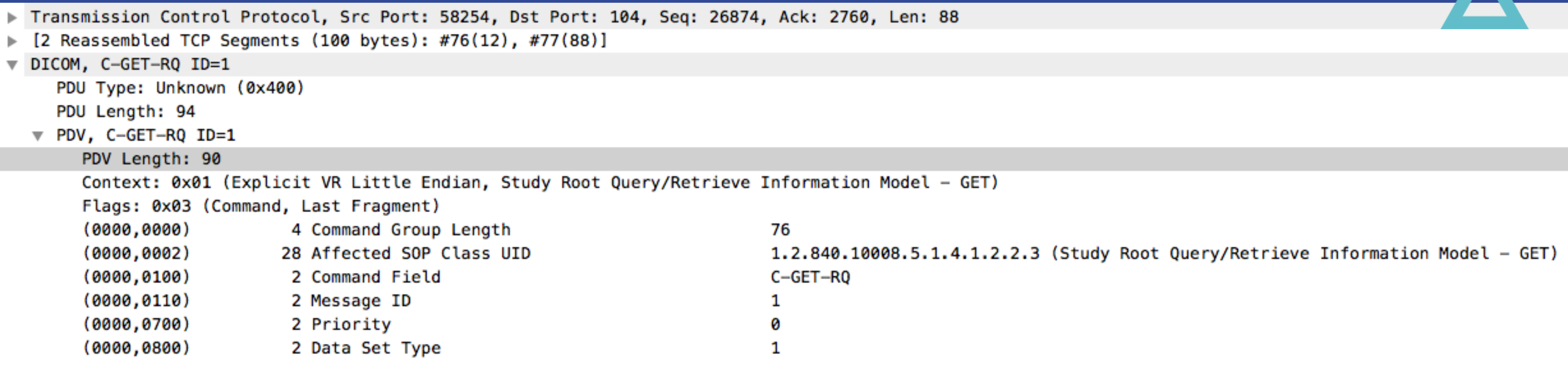


```
▶ Transmission Control Protocol, Src Port: 104, Dst Port: 54433, Seq: 99785, Ack: 711, Len: 1326
▼ DICOM, C-FIND-RSP-DATA
    PDU Type: Unknown (0x400)
    PDU Length: 318
  ▼ PDV, C-FIND-RSP-DATA
      PDV Length: 314
      Context: 0x01 (Implicit VR Little Endian, Study Root Query/Retrieve Information Model - FIND)
      Flags: 0x02 (Data, Last Fragment)
      (0008,0000)          4 Group Length                      132
      (0008,0020)          8 Study Date                        [redacted]
      (0008,0030)          6 Study Time                        [redacted]
      (0008,0050)          6 Accession Number                  [redacted]
      (0008,0052)          6 Query/Retrieve Level              STUDY
      (0008,0054)          6 Retrieve AE Title                 DICOM
      (0008,0056)          6 Instance Availability             ONLINE
      (0008,0061)          2 Modalities in Study               XA
      (0008,1030)          8 Study Description                 CARDIAC
      (0008,1050)         12 Performing Physician's Name       [redacted]
      (0010,0000)          4 Group Length                      52
      (0010,0010)         16 Patient's Name                    [redacted]
      (0010,0020)          4 Patient ID                        [redacted]
      (0010,0030)          8 Patient's Birth Date              [redacted]
      (0020,0000)          4 Group Length                      92
      (0020,000d)         58 Study Instance UID                1.2.840.113619.2.199.32640.10011.60485.1418626261.4842.38
      (0020,0010)          8 Study ID                          [redacted]
      (0020,1208)          2 Number of Study Related Instances 7
```

DICOM

C-Get

- Utilizado para recuperação de imagens

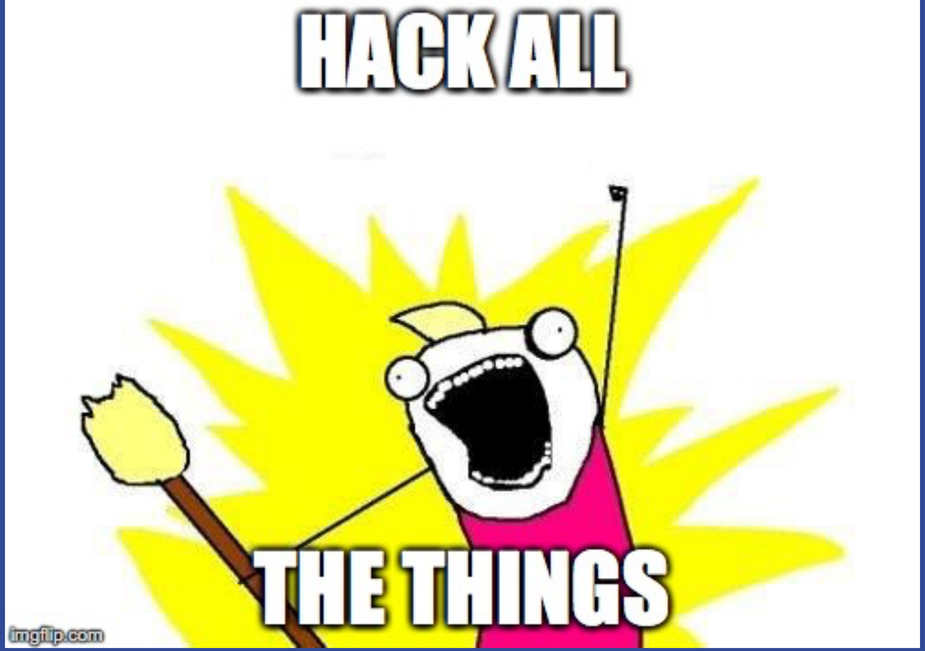


```
▶ Transmission Control Protocol, Src Port: 58254, Dst Port: 104, Seq: 26874, Ack: 2760, Len: 88
▶ [2 Reassembled TCP Segments (100 bytes): #76(12), #77(88)]
▼ DICOM, C-GET-RQ ID=1
    PDU Type: Unknown (0x400)
    PDU Length: 94
  ▼ PDV, C-GET-RQ ID=1
      PDV Length: 90
      Context: 0x01 (Explicit VR Little Endian, Study Root Query/Retrieve Information Model - GET)
      Flags: 0x03 (Command, Last Fragment)
      (0000,0000)          4 Command Group Length                   76
      (0000,0002)         28 Affected SOP Class UID                 1.2.840.10008.5.1.4.1.2.2.3 (Study Root Query/Retrieve Information Model - GET)
      (0000,0100)          2 Command Field                          C-GET-RQ
      (0000,0110)          2 Message ID                             1
      (0000,0700)          2 Priority                               0
      (0000,0800)          2 Data Set Type                          1
```

MORPHUS
SEGURANÇA DA INFORMAÇÃO

Pentesting DICOM Devices

- Ferramentas
- Devices in the wild
- Discovery interno
- Obtendo imagens
- Fuzzing



MORPHUS
SEGURANÇA DA INFORMAÇÃO

Pentesting DICOM Devices

Ferramentas

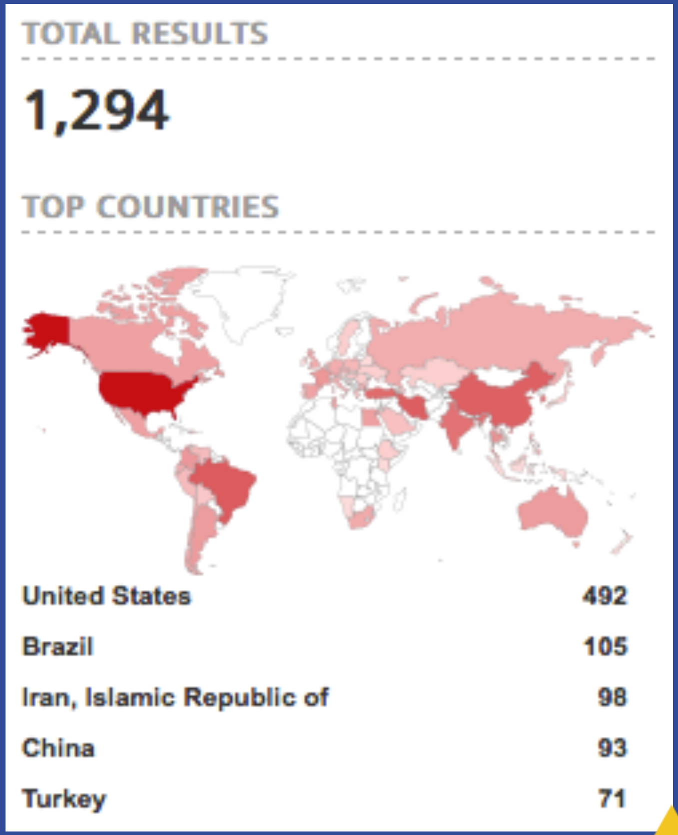
- Pydicom
  - https://github.com/pydicom/pydicom
- Pynetdicom
  - https://github.com/patmun/pynetdicom
- Horus
  - https://www.horosproject.org/
- Radamsa
  - https://github.com/aoh/radamsa

MORPHUS
SEGURANÇA DA INFORMAÇÃO

Pentesting DICOM Devices

Devices In The Wild

- Encontrando dispositivos com Shodan
- Pesquisas:
  - dicom port:104
  - findscu port:104
- Número de dispositivos
  - Global: 1294
  - Brasil: 105



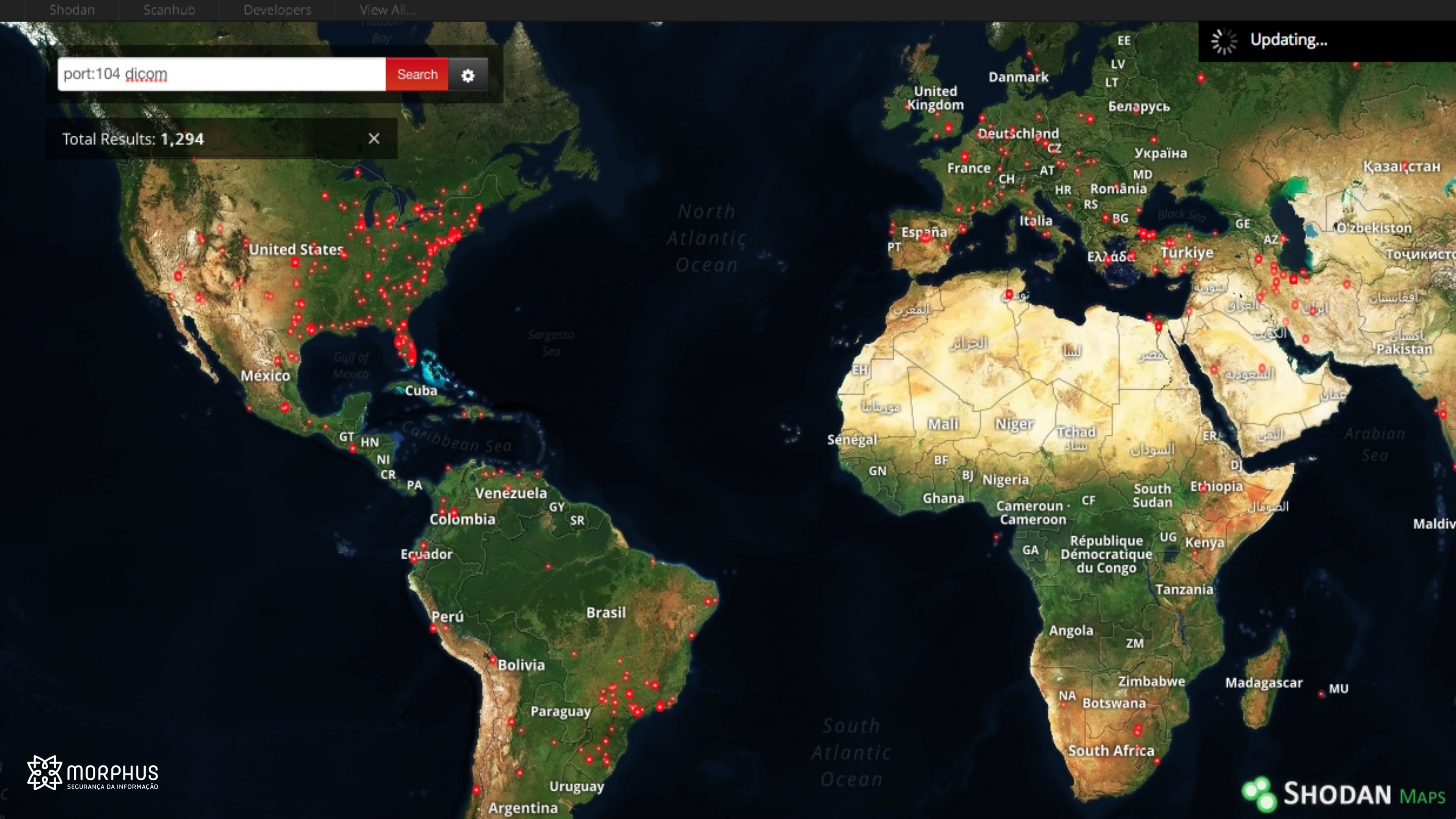
TOTAL RESULTS

1,294

TOP COUNTRIES

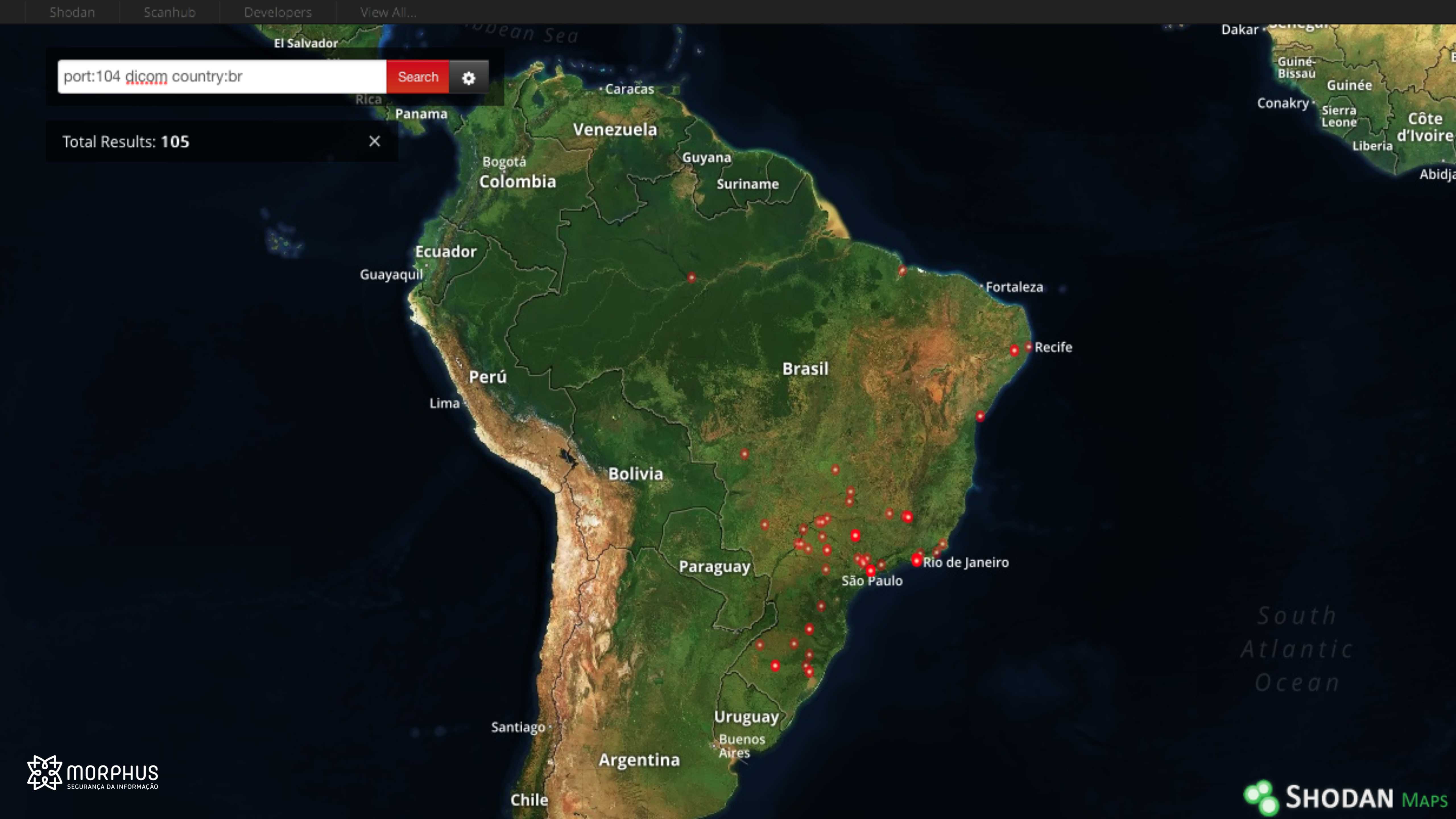
United States	492
Brazil	105
Iran, Islamic Republic of	98
China	93
Turkey	71

MORPHUS
SEGURANÇA DA INFORMAÇÃO



port:104 dicom

Total Results: 1,294



port:104 dicom country:br

Total Results: **105**

MORPHUS
SEGURANÇA DA INFORMAÇÃO

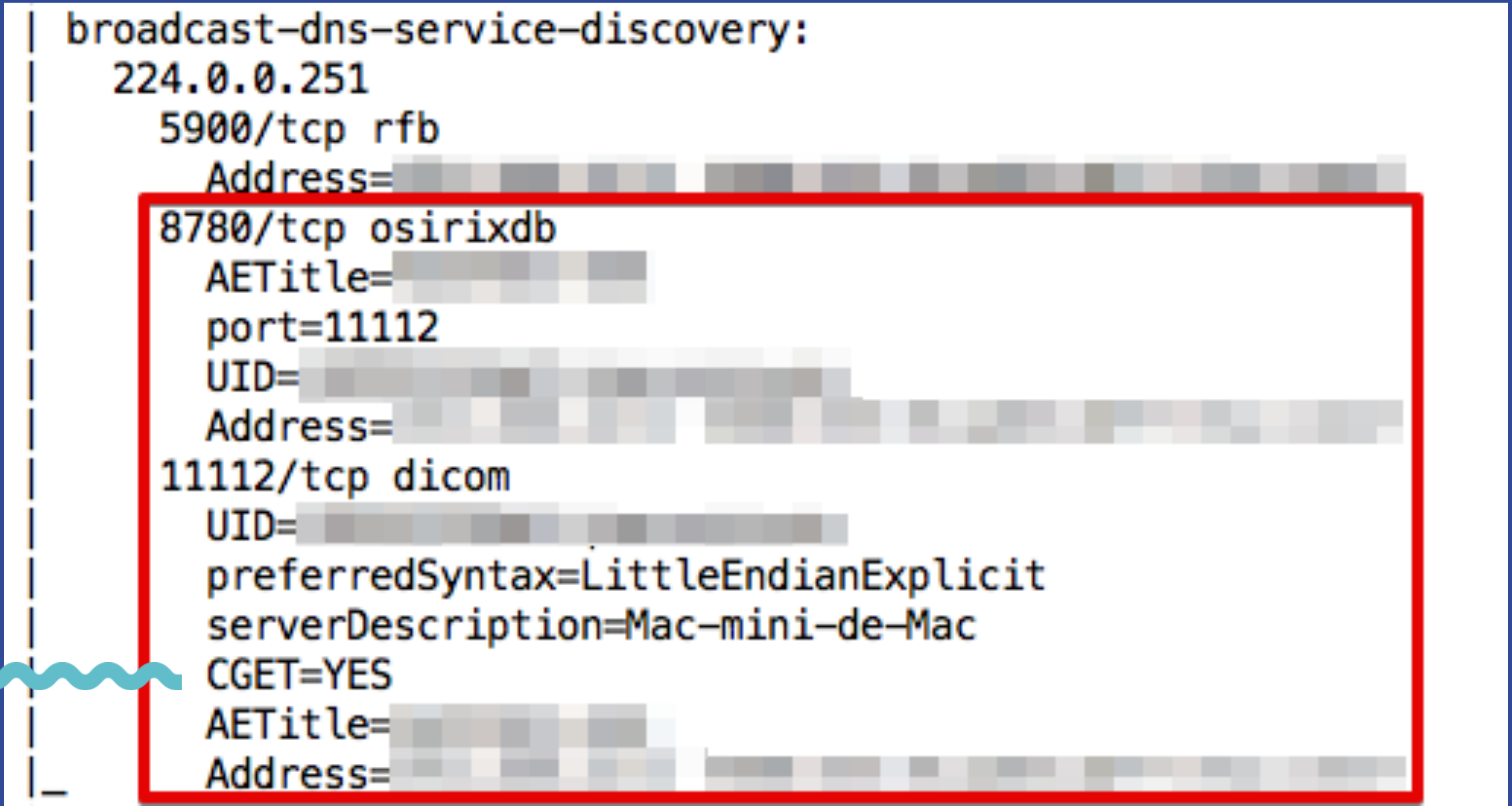
Pentesting DICOM Devices

Discovery Interno

- Scan por porta padrão: 104/TCP
- Enumerando serviços com broadcast:
  - *nmap -script broadcast*

Pentesting DICOM Devices

Discovery Interno

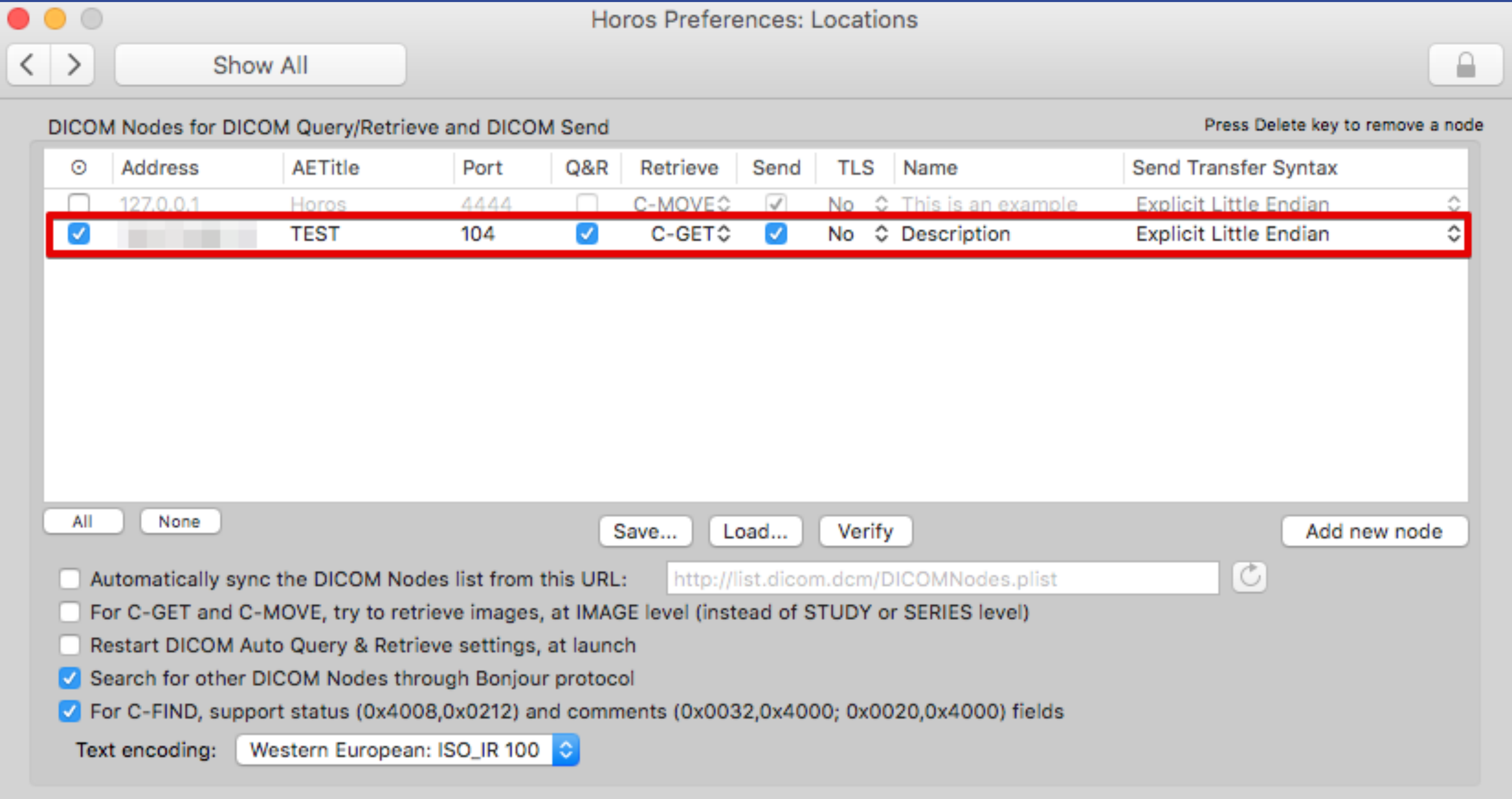


```
| broadcast-dns-service-discovery:
|   224.0.0.251
|     5900/tcp rfb
|       Address=[redacted]
|     8780/tcp osirixdb
|       AETitle=[redacted]
|       port=11112
|       UID=[redacted]
|       Address=[redacted]
|     11112/tcp dicom
|       UID=[redacted]
|       preferredSyntax=LittleEndianExplicit
|       serverDescription=Mac-mini-de-Mac
|       CGET=YES
|       AETitle=[redacted]
|_      Address=[redacted]
```

Pentesting DICOM Devices

Obtendo Imagens

- Horus é uma ferramenta Open Source
- Desenvolvida apenas para OSX
- Baseado no OsiriX
- Operações necessárias:
    - Informar endereço de dispositivo:
        - *Preferences -> Locations*
    - Realizar pesquisa e obter imagens:
        - *Network > Query / Retrieve*


Horos Preferences: Locations
Show All
Press Delete key to remove a node
All
None
Save...
Load...
Verify
Add new node

DICOM Nodes for DICOM Query/Retrieve and DICOM Send

⊙	Address	AETitle	Port	Q&R	Retrieve	Send	TLS	Name	Send Transfer Syntax
□	127.0.0.1	Horos	4444	□	C-MOVE	☑	No	This is an example	Explicit Little Endian
☑	[redacted]	TEST	104	☑	C-GET	☑	No	Description	Explicit Little Endian

□ Automatically sync the DICOM Nodes list from this URL: http://list.dicom.dcm/DICOMNodes.plist

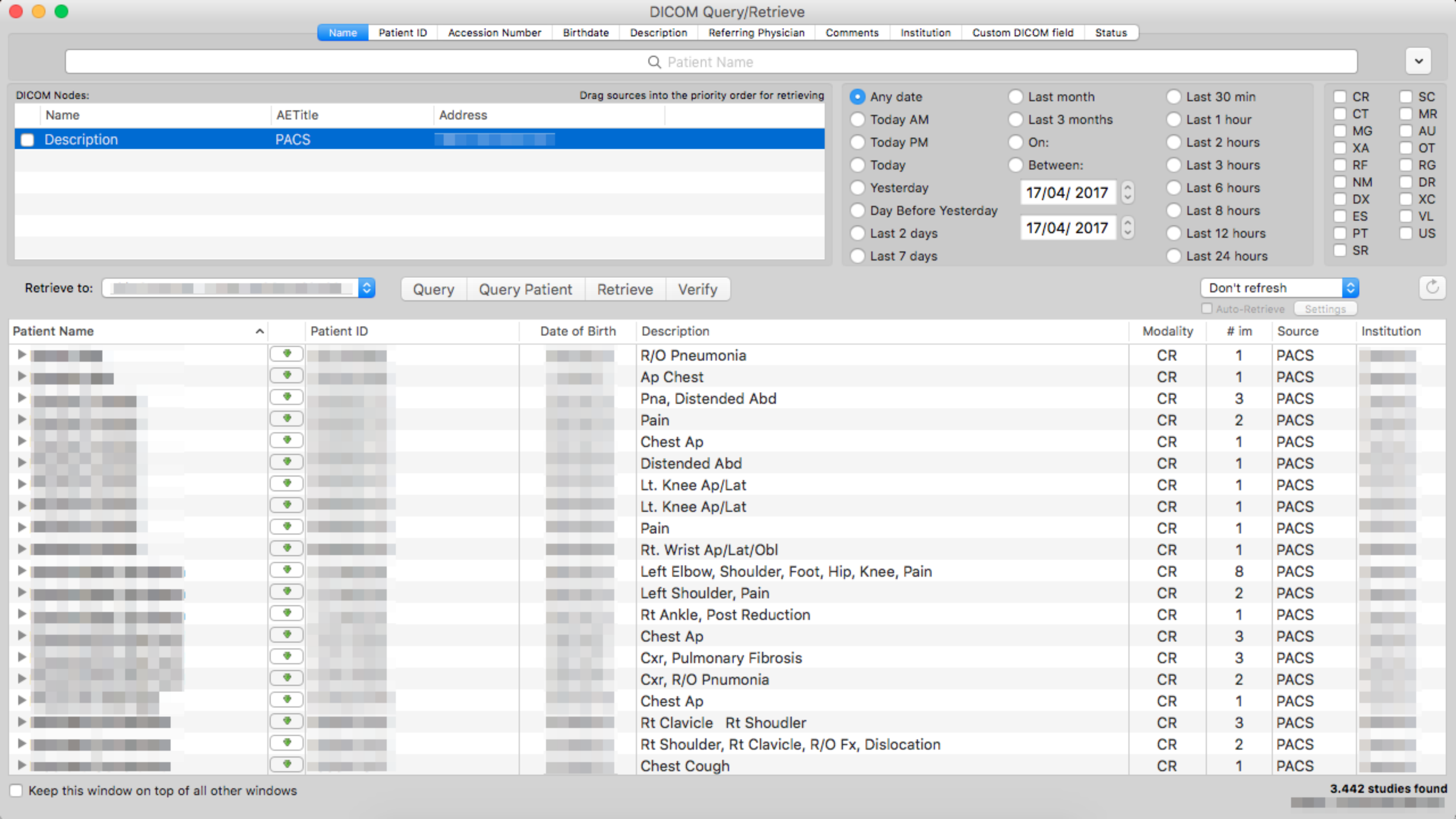
□ For C-GET and C-MOVE, try to retrieve images, at IMAGE level (instead of STUDY or SERIES level)

□ Restart DICOM Auto Query & Retrieve settings, at launch

☑ Search for other DICOM Nodes through Bonjour protocol

☑ For C-FIND, support status (0x4008,0x0212) and comments (0x0032,0x4000; 0x0020,0x4000) fields

Text encoding: Western European: ISO_IR 100



DICOM Query/Retrieve

DICOM Nodes:

Drag sources into the priority order for retrieving

	Name	AETitle	Address
□	Description	PACS	[redacted]

● Any date ○ Last month ○ Last 30 min

○ Today AM ○ Last 3 months ○ Last 1 hour

○ Today PM ○ On: ○ Last 2 hours

○ Today ○ Between: ○ Last 3 hours

○ Yesterday 17/04/ 2017 ○ Last 6 hours

○ Day Before Yesterday ○ Last 8 hours

○ Last 2 days 17/04/ 2017 ○ Last 12 hours

○ Last 7 days ○ Last 24 hours

□ CR □ SC
□ CT □ MR
□ MG □ AU
□ XA □ OT
□ RF □ RG
□ NM □ DR
□ DX □ XC
□ ES □ VL
□ PT □ US
□ SR

Retrieve to: [redacted]

Don't refresh

□ Auto-Retrieve

Patient Name		Patient ID	Date of Birth	Description	Modality	# im	Source	Institution
[redacted]		[redacted]	[redacted]	R/O Pneumonia	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Ap Chest	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Pna, Distended Abd	CR	3	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Pain	CR	2	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Chest Ap	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Distended Abd	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Lt. Knee Ap/Lat	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Lt. Knee Ap/Lat	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Pain	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Rt. Wrist Ap/Lat/Obl	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Left Elbow, Shoulder, Foot, Hip, Knee, Pain	CR	8	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Left Shoulder, Pain	CR	2	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Rt Ankle, Post Reduction	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Chest Ap	CR	3	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Cxr, Pulmonary Fibrosis	CR	3	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Cxr, R/O Pnumonia	CR	2	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Chest Ap	CR	1	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Rt Clavicle Rt Shoudler	CR	3	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Rt Shoulder, Rt Clavicle, R/O Fx, Dislocation	CR	2	PACS	[redacted]
[redacted]		[redacted]	[redacted]	Chest Cough	CR	1	PACS	[redacted]

□ Keep this window on top of all other windows

3.442 studies found

[redacted]

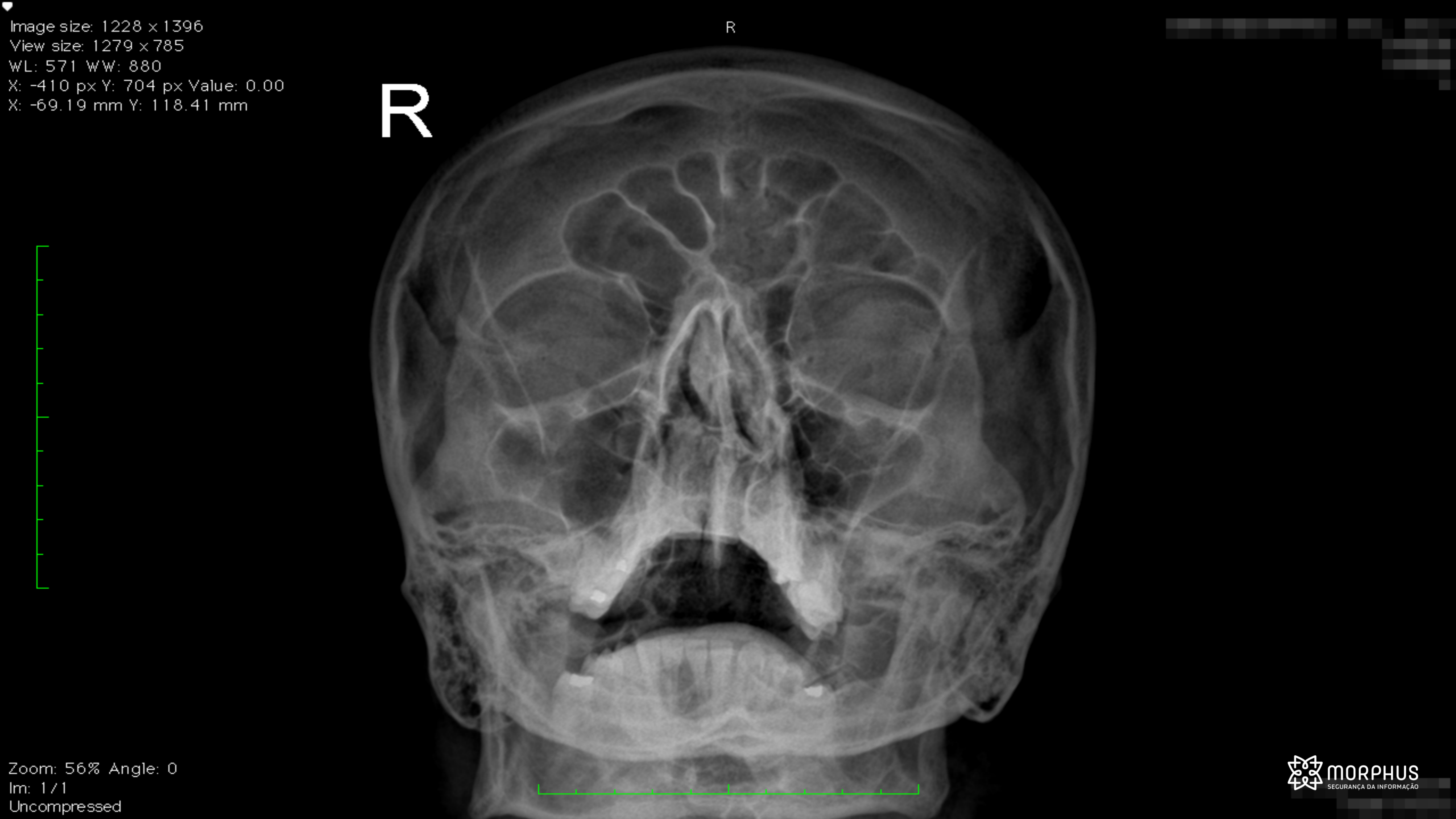


Image size: 1228 x 1396
View size: 1279 x 785
WL: 571 WW: 880
X: -410 px Y: 704 px Value: 0.00
X: -69.19 mm Y: 118.41 mm

[redacted]

Zoom: 56% Angle: 0
Im: 1/1
Uncompressed

[redacted]

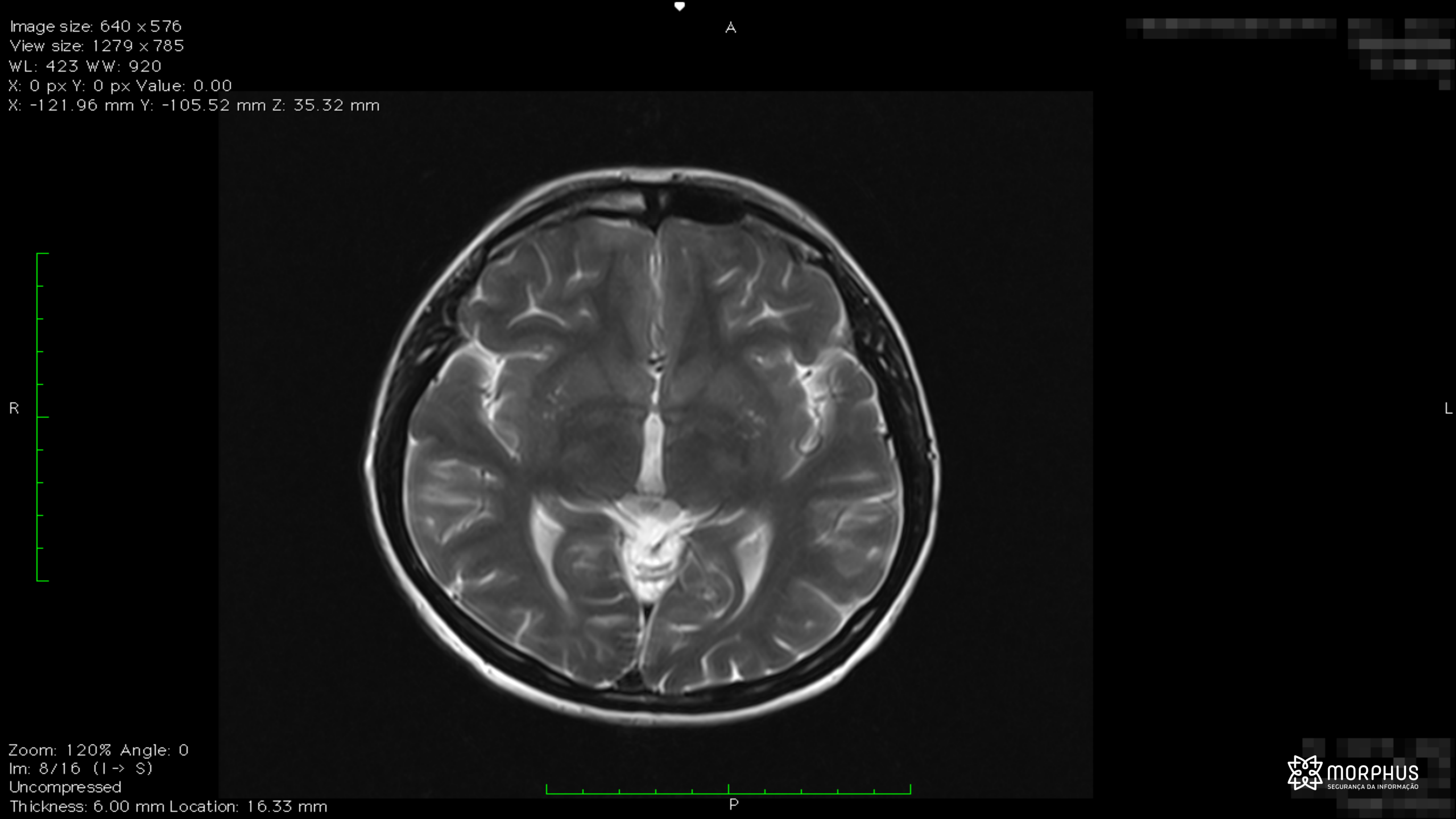


Image size: 640 x 576
View size: 1279 x 785
WL: 423 WW: 920
X: 0 px Y: 0 px Value: 0.00
X: -121.96 mm Y: -105.52 mm Z: 35.32 mm

[redacted]

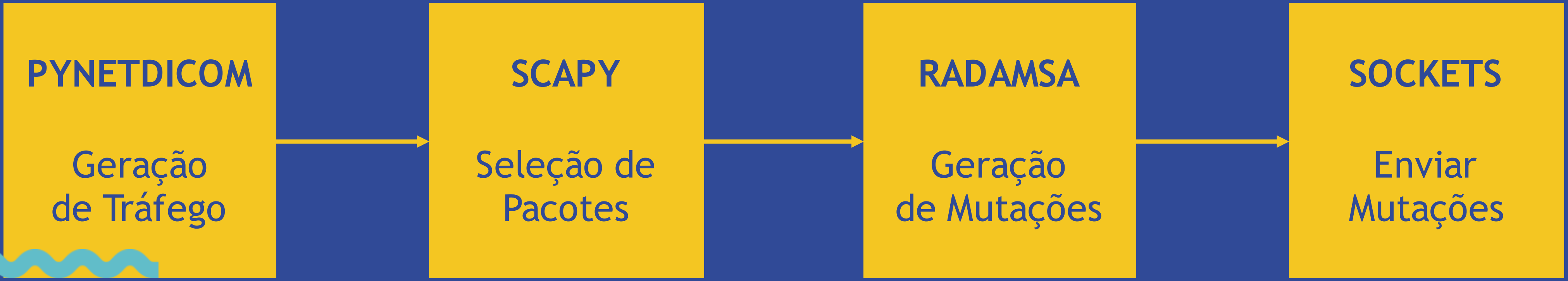
Zoom: 120% Angle: 0
Im: 8/16 (I -> S)
Uncompressed
Thickness: 6.00 mm Location: 16.33 mm

[redacted]

Pentesting DICOM Devices

Fuzzing

1. Gerar tráfego com requisições DICOM
2. Armazenar payload de pacotes desejados
3. Gerar mutações a partir de requisições originais
4. Enviar mutações para alvo e vericar status da conexão



PYNETDICOM

Geração de Tráfego

SCAPY

Seleção de Pacotes

RADAMSA

Geração de Mutações

SOCKETS

Enviar Mutações

DICOM

Conclusões

- Vazamento de dados
- Alteração de dados
- Falta de autenticação
- Tráfego não criptografado
- Gestão de atualização
- Segmentação de rede

Obrigado!

morphuslabs.com
medium.com/@pasknel

MORPHUS
SEGURANÇA DA INFORMAÇÃO