Protecting Medical Data: The Risk of DICOM File Attacks on PACS Servers

- Canaan Kao, Chizuru Toyama
- Threat Research, TXOne Networks Inc.

- April 18, 2025 @CYBERSEC 2025

Who are we?

Canaan Kao

- Threat Research Director at TXOne Networks Inc.
- DPI/IDS/IPS engineer since 2001.
- Led the anti-botnet project for MoECC at NTHU (2009–2013) and organized the Botnet of Taiwan (BoT) workshops (2009–2014).
- Speaker at HITCON 2014 CMT, HITCON 2015 CMT, and HITCON 2019.

Chizuru Toyama

- Senior Threat Researcher at TXOne Networks Inc.
- Over a decade of experience in the security industry.
- Specialized in ICS vulnerability research and acknowledged in multiple ICS-CERT advisories

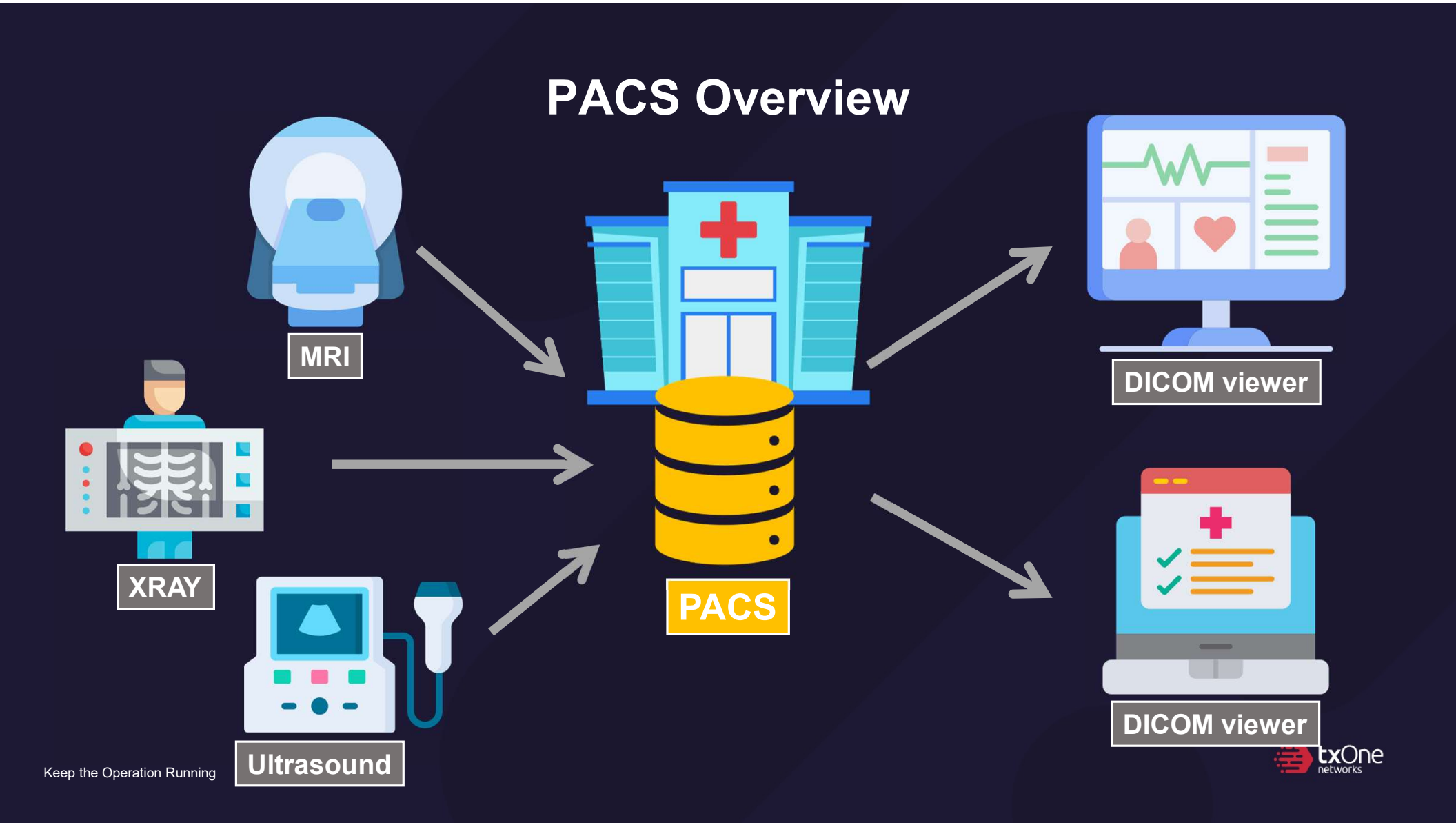
Contents

Introduction to PACS and DICOM

What is PACS Server?

- Picture Archiving and Communication System (PACS)
- PACS server is a network-based system used to store, retrieve, manage, and distribute medical images electronically.
- It replaces traditional film-based methods, providing a more effic ient and accessible way to handle medical imaging data

PACS Overview

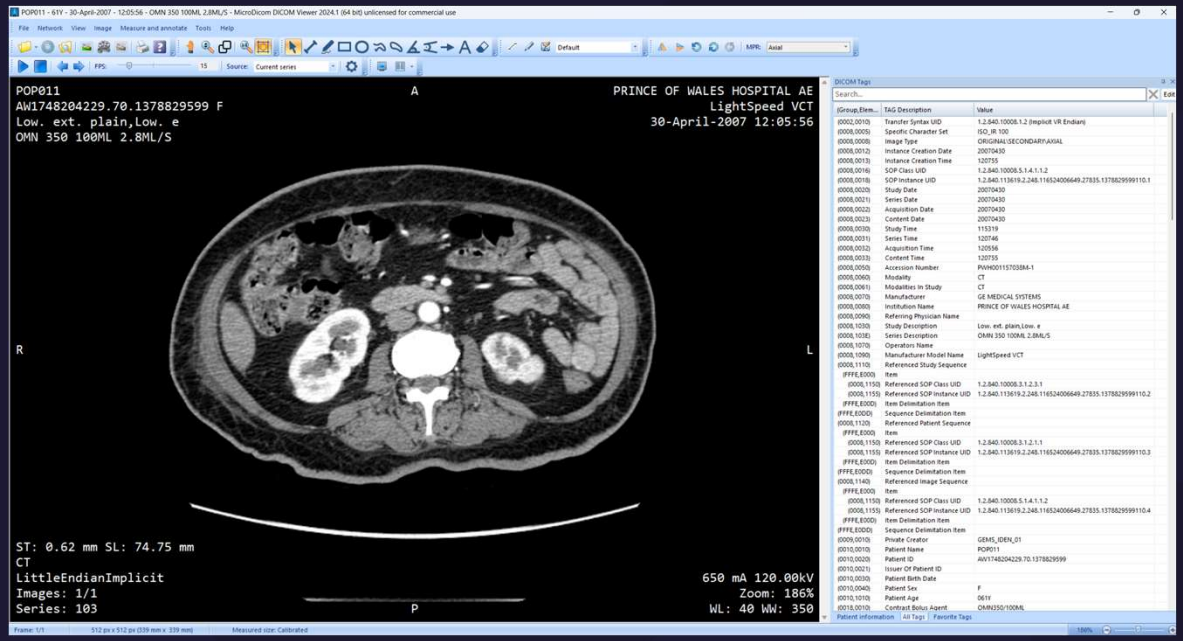


Keep the Operation Running

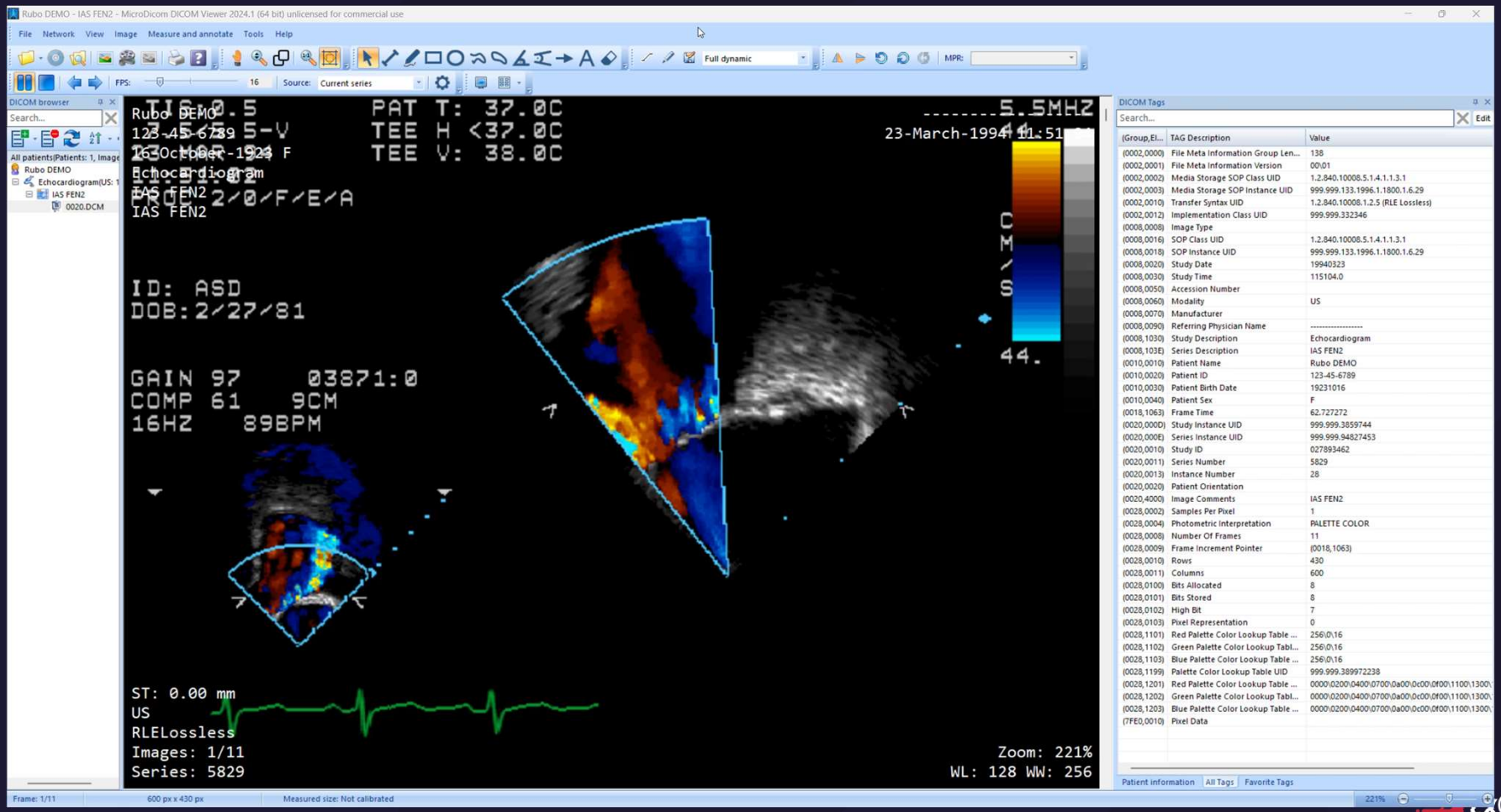
txOne networks

What is DICOM File?

- Digital Imaging and Communications in Medicine (DICOM)
- DICOM files facilitate the exchange of medical images and information between different systems and devices, ensuring compatibility and interoperability in medical imaging.

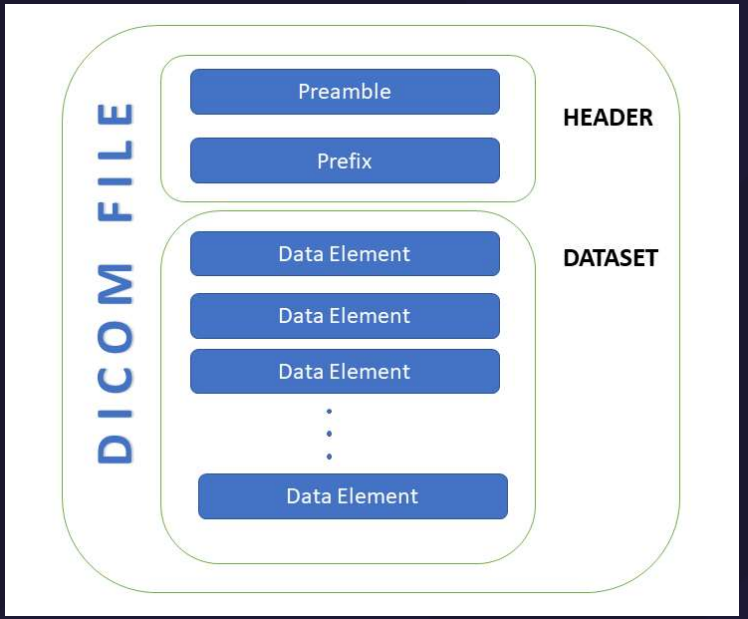


Examples of DICOM file



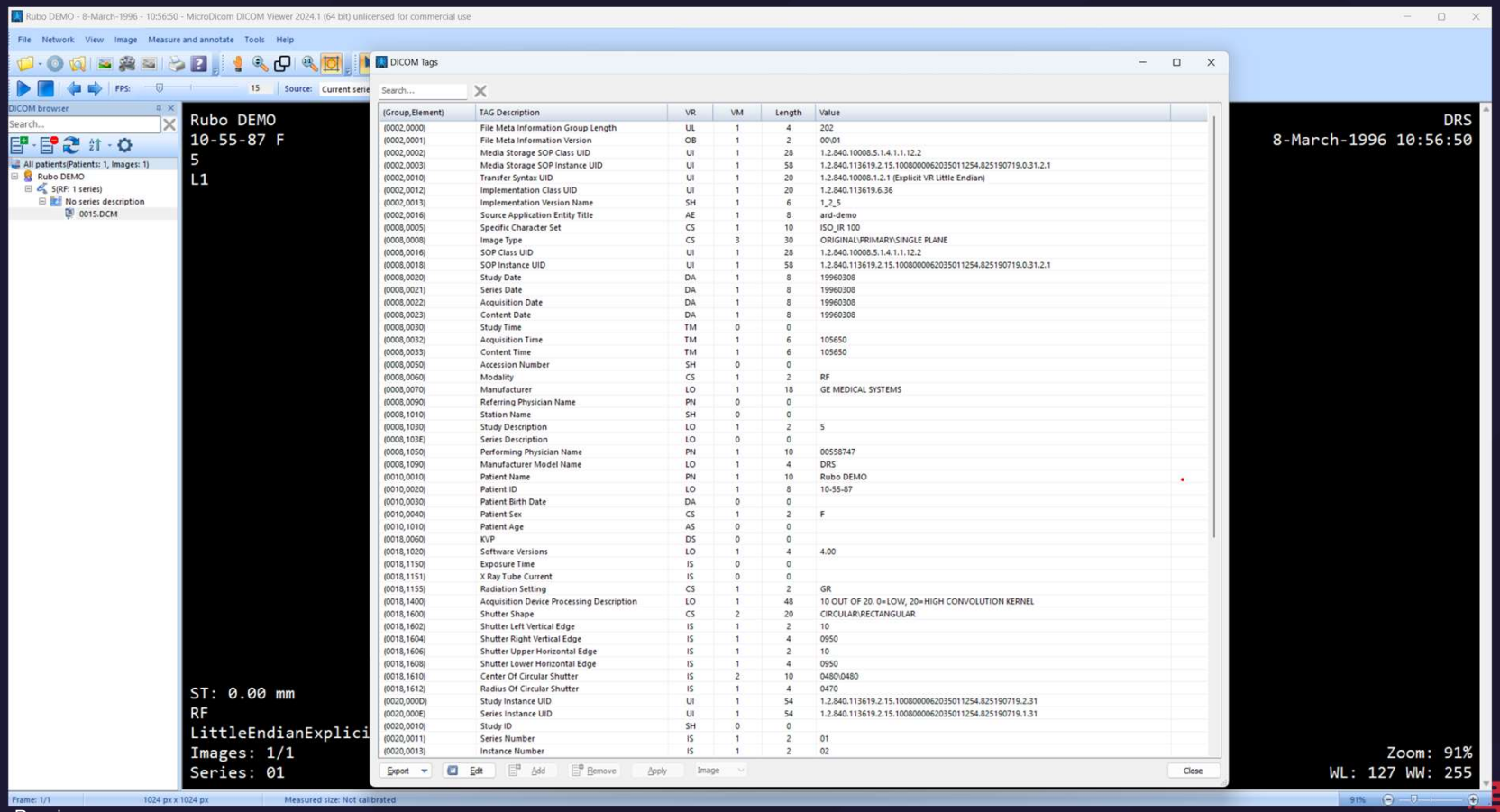
DICOM File Structure

- **Structure**: DICOM file consists of a Header and a Data Set:
  - Header: The header of a DICOM file includes a 128-byte File Preamble, a 4-byte DICOM prefix ("DICM"), and File Meta Elements
  - Data Set: The Data contains the actual medical data
- **Data Elements**: DICOM files store information as uniquely tagged data elements, including key details like patient ID and modality (e.g., MRI, CT).
- **UIDs**: Unique Identifiers (UIDs) such as SOP/Series/Study Instance UID uniquely identify images, series, and studies within DICOM files.



https://www.vladsiv.com/dicom-file-format-basics/

DICOM Data Tags



DICOM Tags

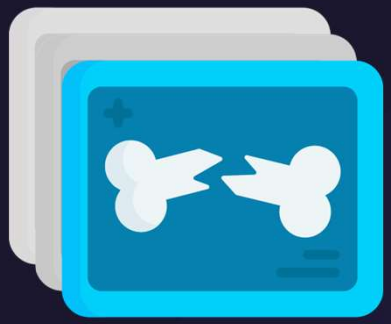
Search...

(Group,Element)	TAG Description	VR	VM	Length	Value
(0002,0000)	File Meta Information Group Length	UL	1	4	202
(0002,0001)	File Meta Information Version	OB	1	2	00\01
(0002,0002)	Media Storage SOP Class UID	UI	1	28	1.2.840.10008.5.1.4.1.1.12.2
(0002,0003)	Media Storage SOP Instance UID	UI	1	58	1.2.840.113619.2.15.1008000062035011254.825190719.0.31.2.1
(0002,0010)	Transfer Syntax UID	UI	1	20	1.2.840.10008.1.2.1 (Explicit VR Little Endian)
(0002,0012)	Implementation Class UID	UI	1	20	1.2.840.113619.6.36
(0002,0013)	Implementation Version Name	SH	1	6	1_2_5
(0002,0016)	Source Application Entity Title	AE	1	8	ard-demo
(0008,0005)	Specific Character Set	CS	1	10	ISO_IR 100
(0008,0008)	Image Type	CS	3	30	ORIGINAL\PRIMARY\SINGLE PLANE
(0008,0016)	SOP Class UID	UI	1	28	1.2.840.10008.5.1.4.1.1.12.2
(0008,0018)	SOP Instance UID	UI	1	58	1.2.840.113619.2.15.1008000062035011254.825190719.0.31.2.1
(0008,0020)	Study Date	DA	1	8	19960308
(0008,0021)	Series Date	DA	1	8	19960308
(0008,0022)	Acquisition Date	DA	1	8	19960308
(0008,0023)	Content Date	DA	1	8	19960308
(0008,0030)	Study Time	TM	0	0	
(0008,0032)	Acquisition Time	TM	1	6	105650
(0008,0033)	Content Time	TM	1	6	105650
(0008,0050)	Accession Number	SH	0	0	
(0008,0060)	Modality	CS	1	2	RF
(0008,0070)	Manufacturer	LO	1	18	GE MEDICAL SYSTEMS
(0008,0090)	Referring Physician Name	PN	0	0	
(0008,1010)	Station Name	SH	0	0	
(0008,1030)	Study Description	LO	1	2	5
(0008,103E)	Series Description	LO	0	0	
(0008,1050)	Performing Physician Name	PN	1	10	00558747
(0008,1090)	Manufacturer Model Name	LO	1	4	DRS
(0010,0010)	Patient Name	PN	1	10	Rubo DEMO
(0010,0020)	Patient ID	LO	1	8	10-55-87
(0010,0030)	Patient Birth Date	DA	0	0	
(0010,0040)	Patient Sex	CS	1	2	F
(0010,1010)	Patient Age	AS	0	0	
(0018,0060)	KVP	DS	0	0	
(0018,1020)	Software Versions	LO	1	4	4.00
(0018,1150)	Exposure Time	IS	0	0	
(0018,1151)	X Ray Tube Current	IS	0	0	
(0018,1155)	Radiation Setting	CS	1	2	GR
(0018,1400)	Acquisition Device Processing Description	LO	1	48	10 OUT OF 20. 0=LOW, 20=HIGH CONVOLUTION KERNEL
(0018,1600)	Shutter Shape	CS	2	20	CIRCULAR\RECTANGULAR
(0018,1602)	Shutter Left Vertical Edge	IS	1	2	10
(0018,1604)	Shutter Right Vertical Edge	IS	1	4	0950
(0018,1606)	Shutter Upper Horizontal Edge	IS	1	2	10
(0018,1608)	Shutter Lower Horizontal Edge	IS	1	4	0950
(0018,1610)	Center Of Circular Shutter	IS	2	10	0480\0480
(0018,1612)	Radius Of Circular Shutter	IS	1	4	0470
(0020,000D)	Study Instance UID	UI	1	54	1.2.840.113619.2.15.1008000062035011254.825190719.2.31
(0020,000E)	Series Instance UID	UI	1	54	1.2.840.113619.2.15.1008000062035011254.825190719.1.31
(0020,0010)	Study ID	SH	0	0	
(0020,0011)	Series Number	IS	1	2	01
(0020,0013)	Instance Number	IS	1	2	02

Export Edit Add Remove Apply Image Close

How DICOM file are organized

Patient → Study → Series → SOP Instance



Transmission of DICOM file

DICOM Protocol

- Standard for handling, storing, transmitting, and viewing medical imaging information (e.g. C-STORE, C-FIND, and C-MOVE)

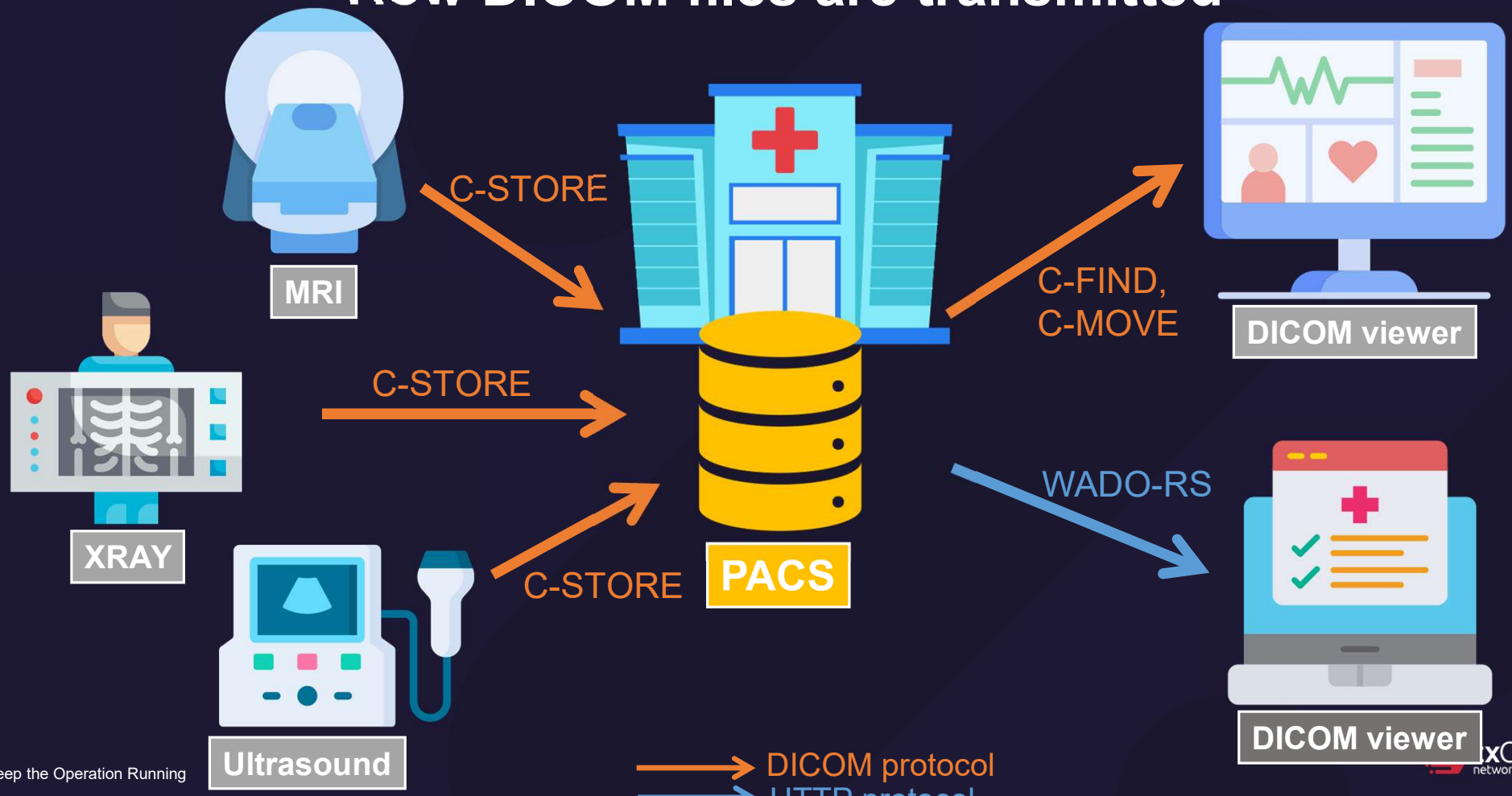
HTTP/WADO

- HTTP and WADO (Web Access to DICOM Objects) for transmitting DICOM files over the web.

Vendor-Specific Protocols

- additional protocols implemented by vendors for DICOM file transmission (e.g. osirix:// and sante://)

How DICOM files are transmitted



Keep the Operation Running

DICOM protocol

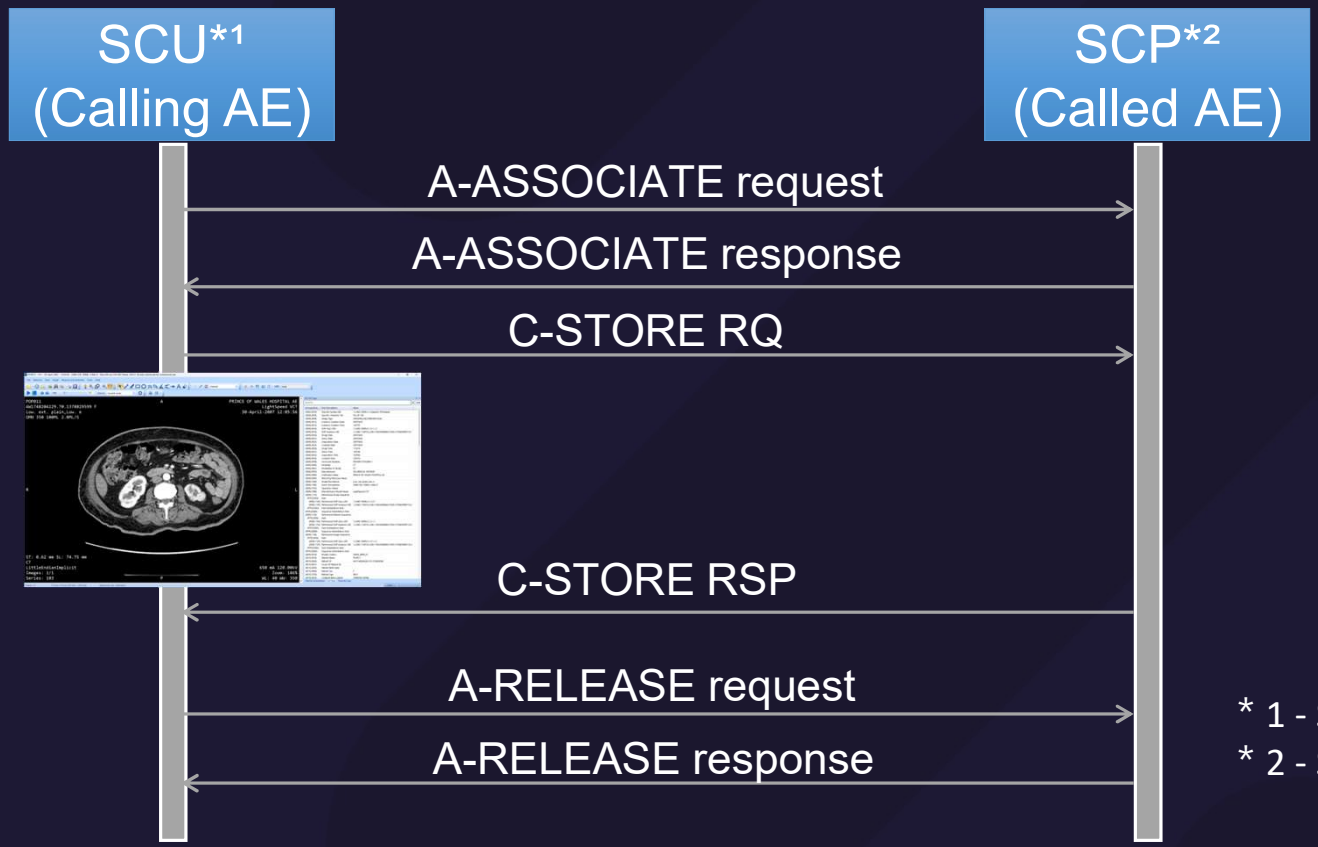
The DICOM protocol is a standard for handling, storing, transmitting, and viewing medical imaging information.

Purpose: The DICOM protocol ensures that medical imaging devices and systems from different manufacturers can communicate and exchange data seamlessly.

Services: DICOM defines various services like C-STORE (for storing images), C-FIND (for querying information), and C-MOVE (for transferring images).

Interoperability: By adhering to DICOM standards, healthcare providers can ensure that imaging data is accessible and usable across different systems and devices.

DICOM Protocol (C-STORE)

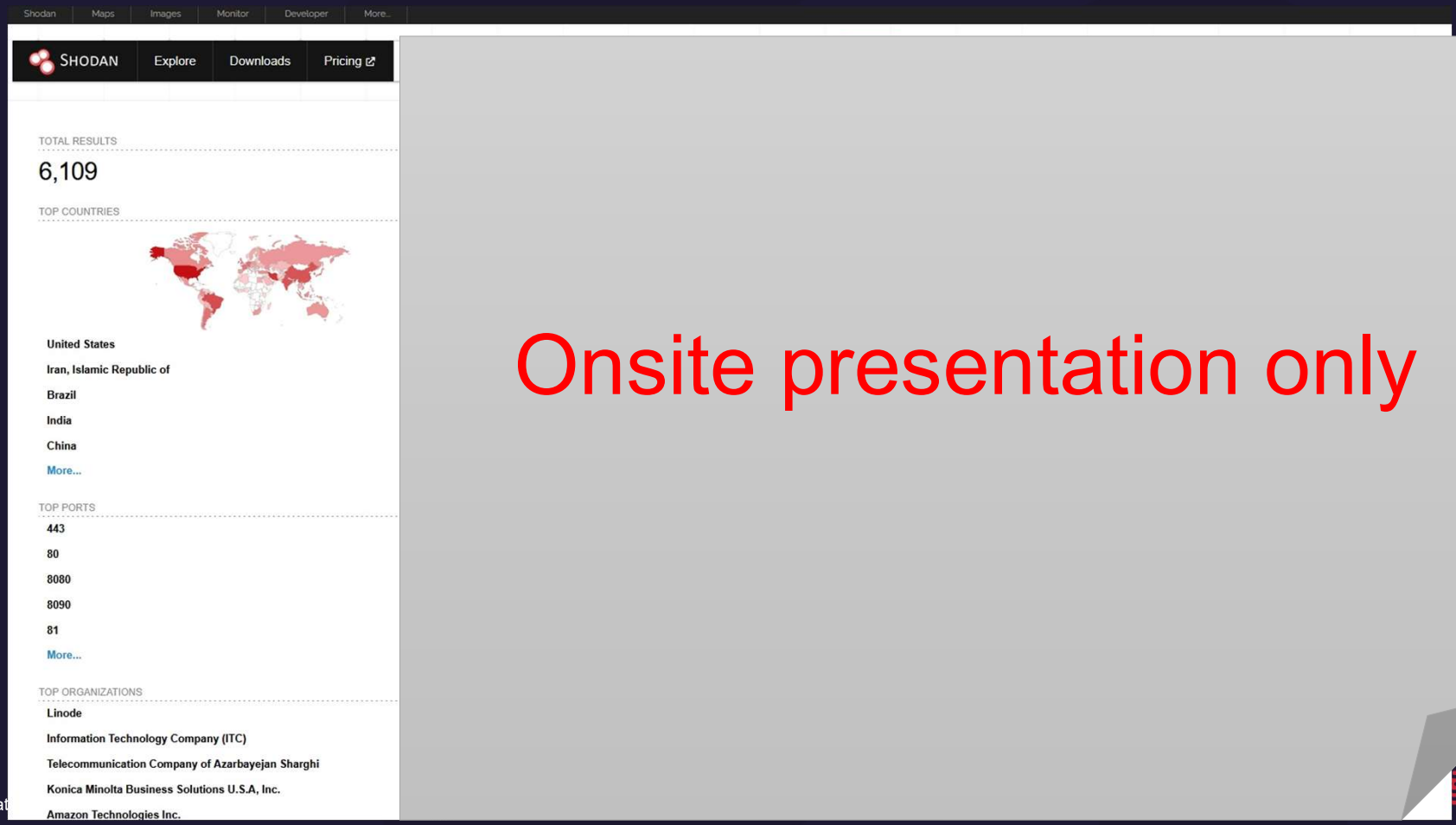


* 1 - Service Class User
* 2 - Service Class Provider

txOne networks

Exposed PACS and DICOM

Exposed PACS servers

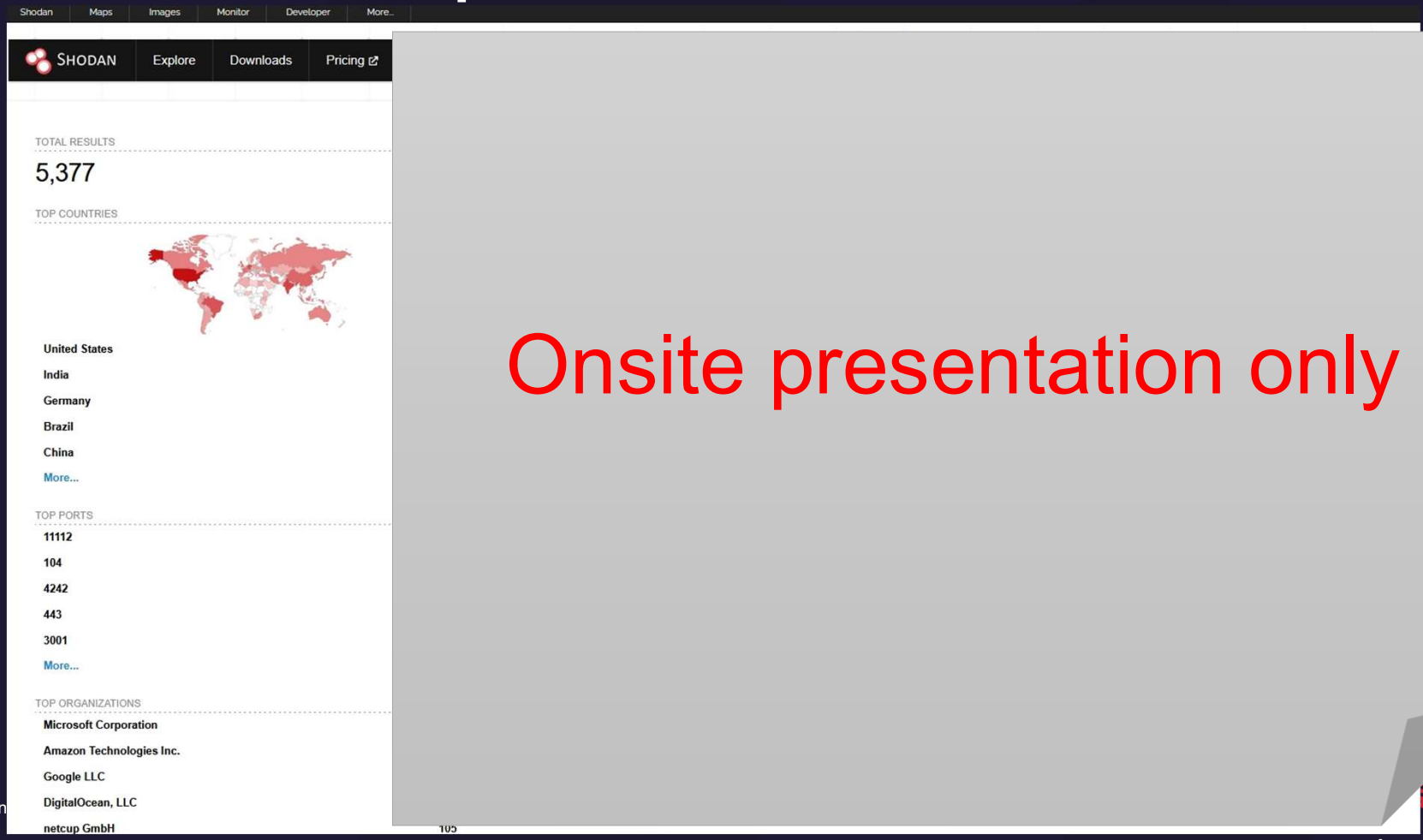


Onsite presentation only

txOne networks

As of 4/1/2025

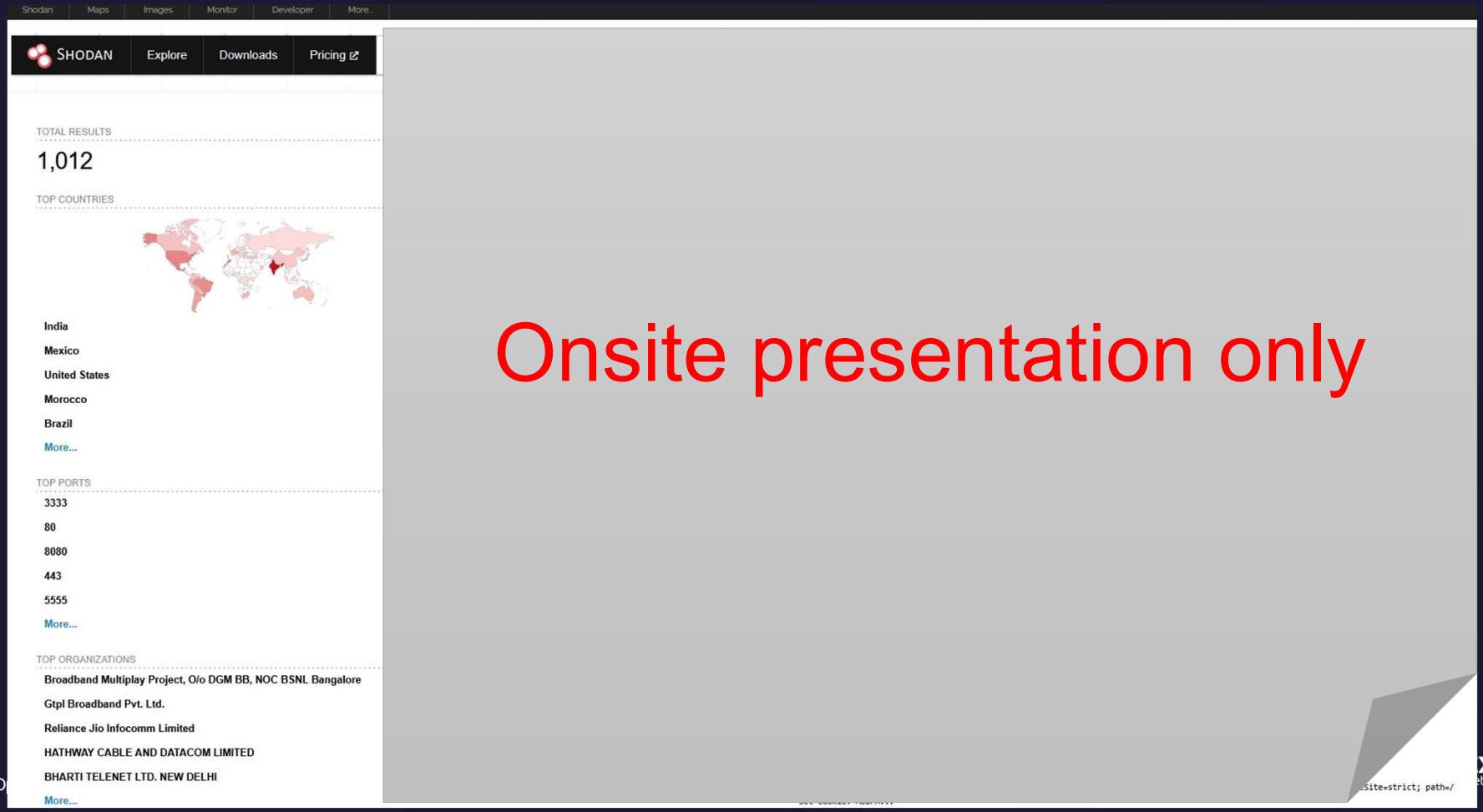
Exposed DICOM nodes



Onsite presentation only

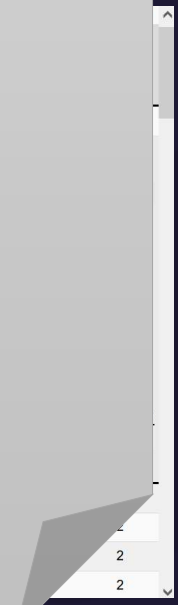
As of 4/1/2025

Exposed Osirix PACS Servers

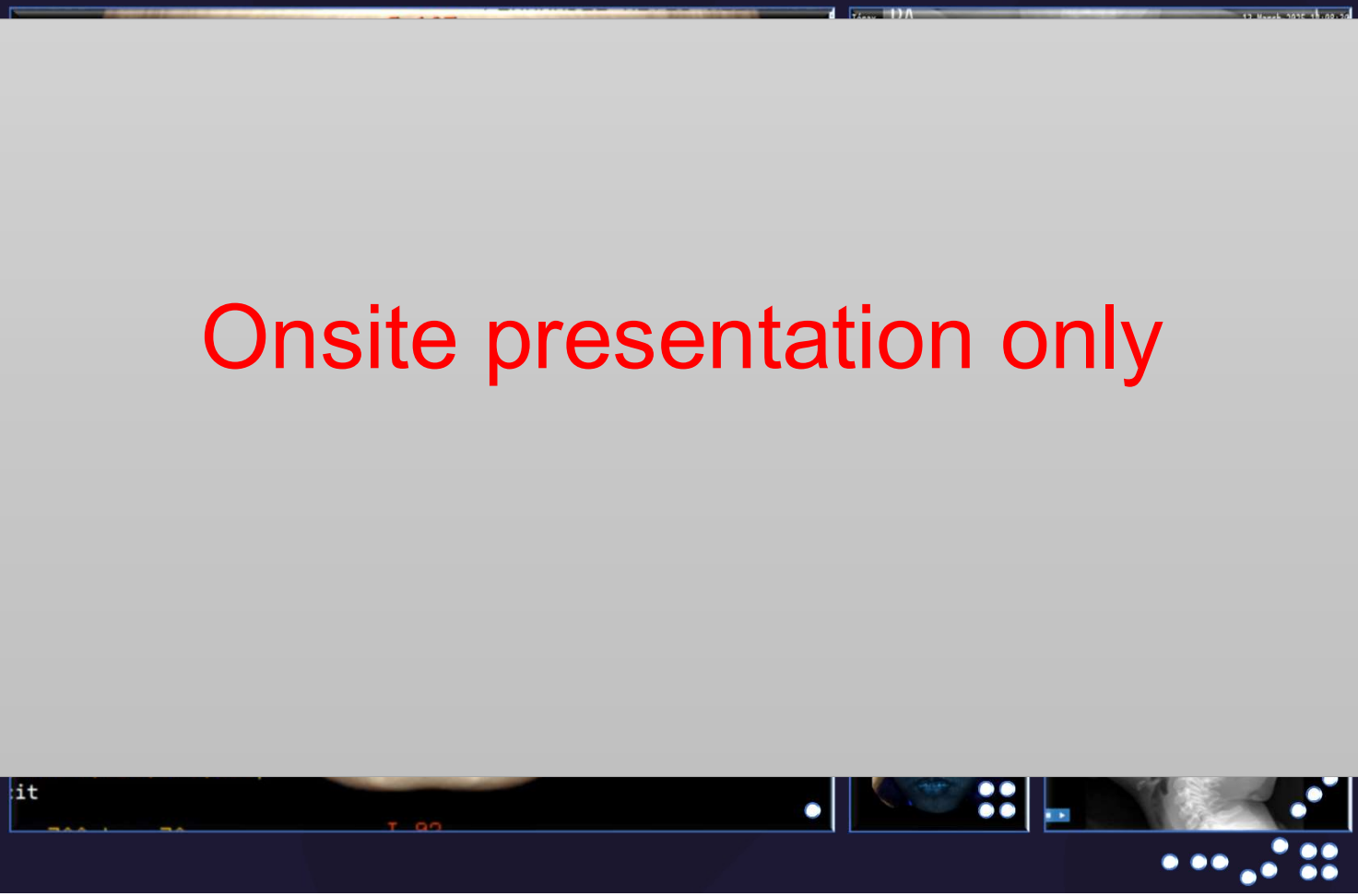


Patient records on the Internet

Onsite presentation only



DICOM files on the Internet



Vulnerabilities in PACS and DICOM

Osirix DICOM Viewer / PACS server

- Exclusive for macOS
- Advanced 2D/3D/4D Visualization
- Full PACS Server Capabilities
- DICOM Worklist & HL7 Support

txOne networks

Found Vulnerabilities in Osirix PACS servers

Onsite presentation only

How Osirix PACS server can be attacked

MedDream PACS server

- Cross-Platform Compatibility
- Web-Based Viewer
- Full DICOM Support
- Cloud & Local PACS Support
- Multi-Modality Support

txOne networks

Found Vulnerabilities in MedDream PACS servers

Onsite presentation only

- CVE-2025-3481: DICOM C-STORE Stack-based Buffer Overflow Remote Code Execution Vulnerability (CVSSv3: 9.8)

Onsite presentation only

- CVE-2025-3482: DICOM C-STORE Stack-based Buffer Overflow Remote Code Execution Vulnerability (CVSSv3: 9.8)

Onsite presentation only

- CVE-2025-3483: DICOM C-STORE Stack-based Buffer Overflow Remote Code Execution Vulnerability (CVSSv3: 9.8)

Onsite presentation only

- CVE-2025-3484: DICOM C-STORE Stack-based Buffer Overflow Remote Code Execution Vulnerability (CVSSv3: 9.8)

Update to MedDream PACS Server version 7.3.5.860 or above

How MedDream PACS server can be attacked

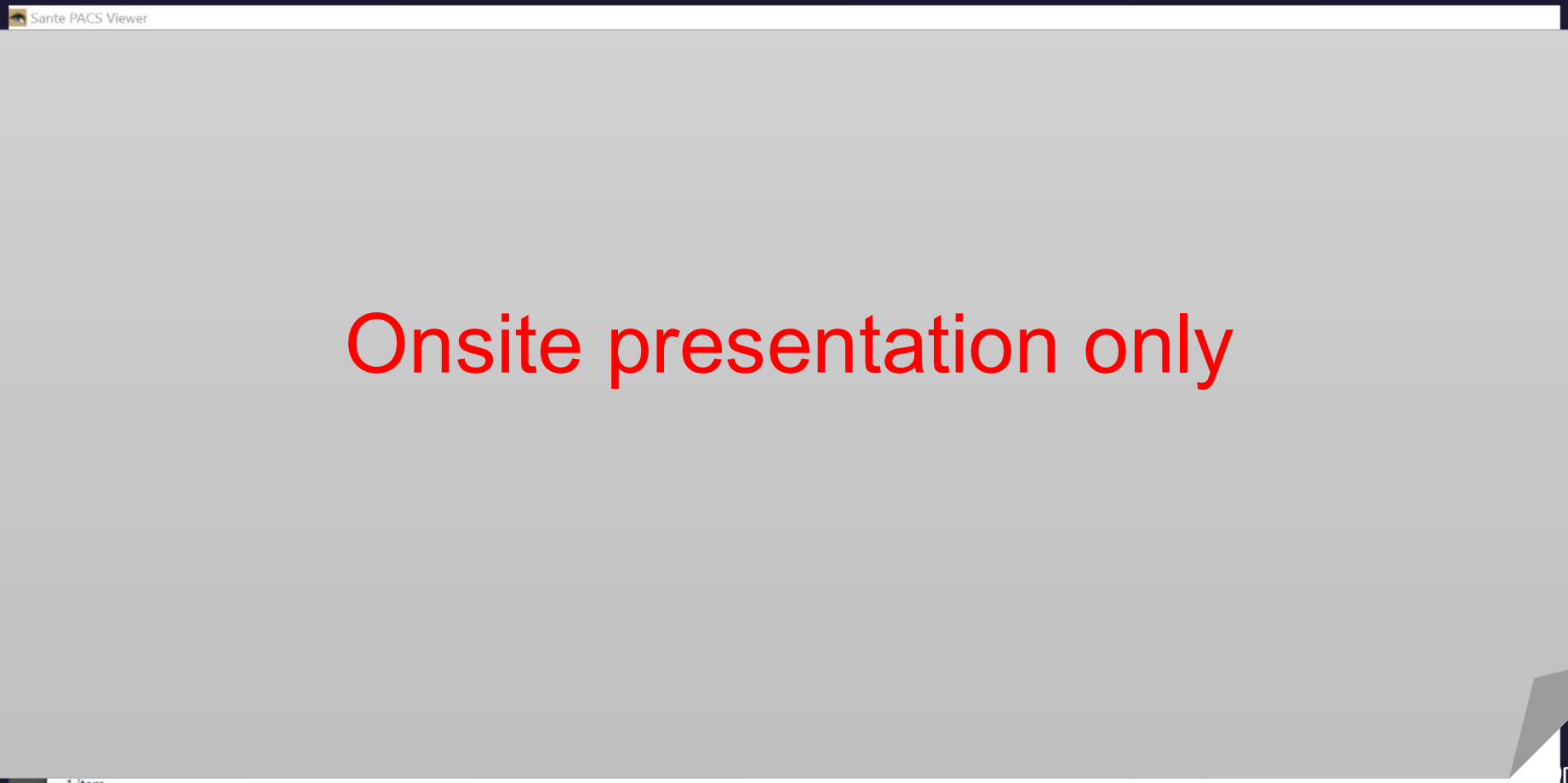
Onsite presentation only

Sante PACS server

- Windows-Based PACS Server
- Full DICOM Support
- Web-Based Viewer
- Multi-Modality Support

txOne networks

How a DICOM file is stored in Sante PACS server



Found Vulnerabilities in Sante PACS servers

Onsite presentation only

- **CVE-2025-0573**: DCM File Parsing Directory Traversal Arbitrary File Write Vulnerability (CVSSv3: 5.3)
- **CVE-2025-0572**: Web Portal DCM File Parsing Directory Traversal Arbitrary File Write Vulnerability (CVSSv3: 4.3)

Onsite presentation only

- **CVE-2025-0568**: DCM File Parsing Memory Corruption Denial-of-Service Vulnerability (CVSSv3: 7.5)
- **CVE-2025-0570**: Web Portal DCM File Parsing Memory Corruption Denial-of-Service Vulnerability (CVSSv3: 6.5)

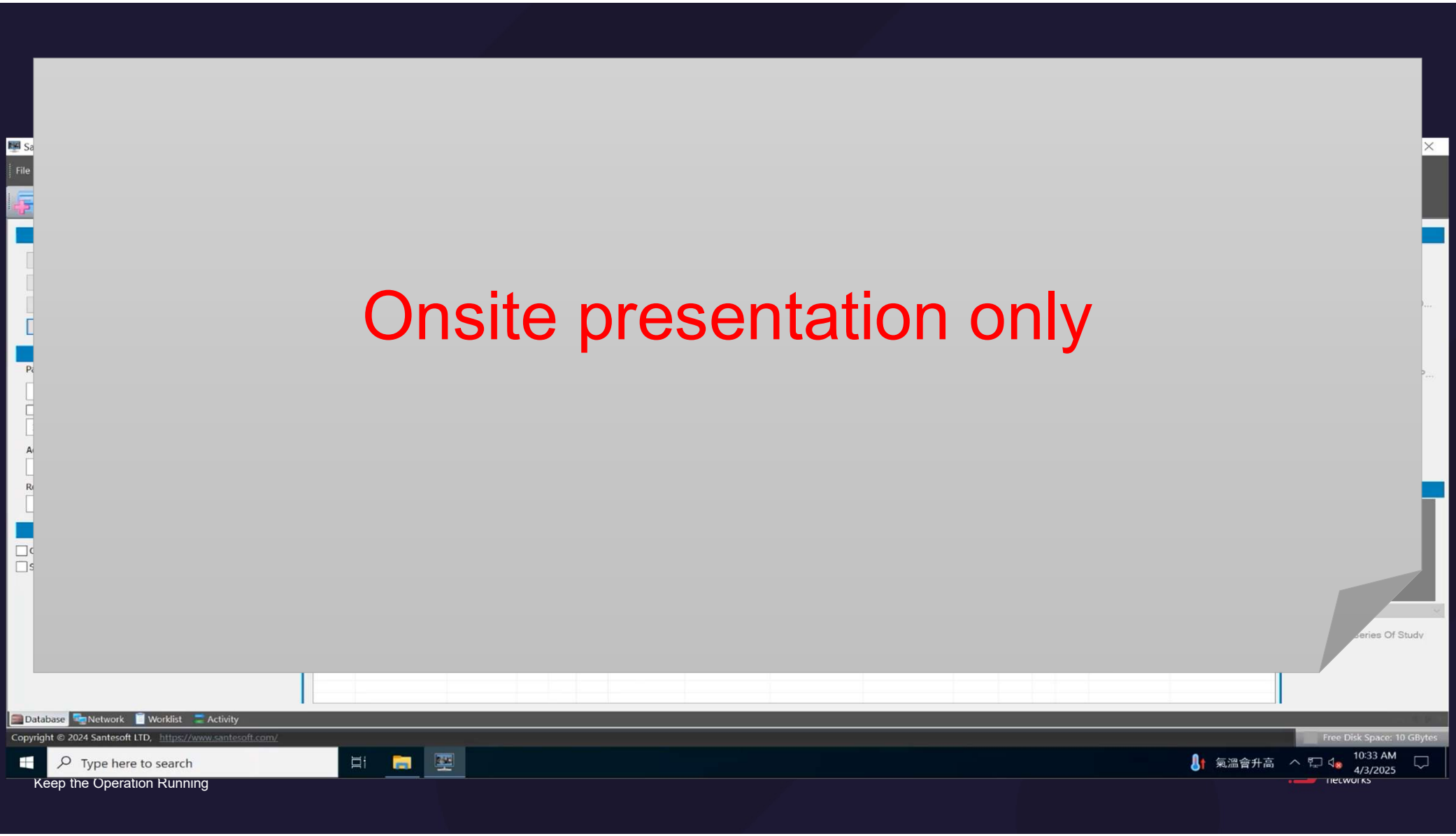
Onsite presentation only

- **CVE-2025-0569**: DCM File Parsing Memory Corruption Denial-of-Service Vulnerability (CVSSv3: 7.5)
- **CVE-2025-0571**: Web Portal DCM File Parsing Memory Corruption Denial-of-Service Vulnerability (CVSSv3: 6.5)

Others

- **CVE-2025-0574**: URL path Memory Corruption Denial-of-Service Vulnerability (CVSSv3: 8.2)

Update to Sante PACS Server version 4.0.10 or above



Keep the Operation Running

Mitigations on PACS and DICOM

Use Firewalls and VPNs

- Place PACS servers behind firewalls and require a Virtual Private Network (VPN) for remote access

✔ **Restrict incoming DICOM communication**
✔ **Enforce TLS encryption**
✔ **Use Application Entity (AE) titles and IP filtering**

Update and Patch Systems

- Keep all PACS servers up to date with the latest security patches and updates to protect against known vulnerabilities.

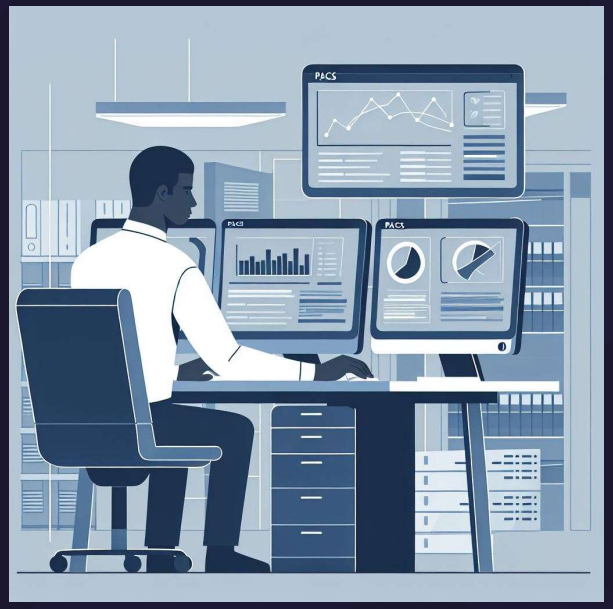
Access Control

- Ensure that only authorized personnel can access and modify DICOM files.

- ✔ **Role-Based Access Control (RBAC)**
- ✔ **Multi-Factor Authentication (MFA)**
- ✔ **Strong Password Policies**

Continuous Monitoring

- Regularly monitor the PACS server for any unusual activity or potential security breaches.



- ✓ **Audit Logs & User Activity Tracking**
- ✓ **Access Control Monitoring**
- ✓ **Network Traffic Analysis**

Educate Staff

Train healthcare and IT staff on the importance of PACS security and the risks associated with exposed servers and DICOM files.

- ✔ Recognizing **phishing attempts** and suspicious activity.
- ✔ Ensuring **secure access** to the system.
- ✔ Following **hospital policies** for data protection and compliance.

txOne networks

Thank you for listening

Contact:

- Canaan Kao (canaan_kao@txone.com)
- Chizuru Toyama (chizuru_Toyama@txone.com)

txOne networks

掃描QR Code到 TXOne 攤位

#P105 挑戰 6.0秒急停 送精美好禮


txOne
networks