

# User guide

by Nathanaël COTTIN

User guide



This publication may not be reproduced or transmitted in any form without the author consent. Any reference to this publication must explicitly indicate its title, author name and electronic contact information.

Trademarks and copyrighted materials are property of their respective owners.



## Table of content

| Introduction                         |    |
|--------------------------------------|----|
| Features                             | 4  |
| Requirements                         | 4  |
| Overview                             | 5  |
| Usage                                | 6  |
| Selecting appropriate decoding rules | 7  |
| Tree view display                    | 9  |
| Browsing the tree view               | 10 |
| Hiding / showing the source file     |    |
| Interpretation and raw tabs          | 15 |
| Known limitations                    | 17 |
| Available rules                      | 17 |
| Opening huge files                   | 17 |
| Contact                              | 17 |



## Introduction

asnViewer displays user-friendly tree views of ASN.1-encoded files. asnViewer performs a powerful interpretation and matches encoded regions with their corresponding tree view entries.

ASN.1 encodings can be found in many systems, environments and protocols which need data exchange. For example, ASN.1 is part of SNMP and most of security tools dealing with cryptography and digital certificates.



Screen captures are taken from asnViewer version 1.3.1.

### Features

asnViewer decodes BER- and DER-encoded ASN.1 files and displays both a tree view and an hexadecimal view.

## Requirements

asnViewer requires a 1.5 (or newer) JRE. This environment can be freely downloaded at http://java.sun.com. The Windows executable version automatically displays the appropriate link to sun website.



### Overview

asnViewer graphical interface is composed of three parts (fig. 1):

- 1. A floating menu
- 2. A tree view and hexadecimal view of the opened file
- 3. An interpretation / raw view section. The corresponding tabs refer to primitive types only. Constructed types values are not displayed in this section.

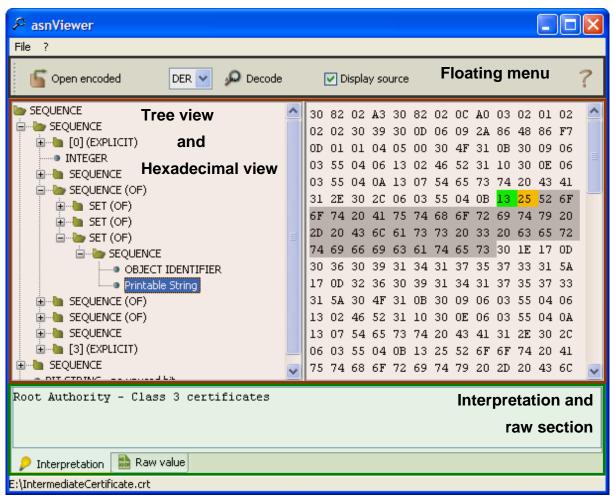


Figure 1



## Usage

Executing asnViewer displays the GUI shown hereafter (fig. 2). First action consists in loading an ASN.1-encoded file by clicking on the "Open encoded" button on the top left hand corner.

| ₽ asnViewer                   |                |                                   |   |
|-------------------------------|----------------|-----------------------------------|---|
| File ?                        |                |                                   |   |
| 🕤 Open encoded                | BER 🔽 🔎 Decode | ✓ Display source                  | ? |
|                               |                | <source activated="" display=""/> |   |
|                               |                |                                   |   |
|                               |                |                                   |   |
|                               |                |                                   |   |
|                               |                |                                   |   |
| 🔎 Interpretation  鼬 Raw       | value          |                                   |   |
| Open an ASN.1 encoded file to | display        |                                   |   |

Figure 2

The selected file is then automatically displayed in hexadecimal format and its decoding tree view is created.

The selected file is not loaded in the hexadecimal view when the "display source" box is unchecked.



## Selecting appropriate decoding rules

Basic Encoding Rules (BER) are selected by default. These rules allow to decode BER, Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

When opening a BER-encoded file using BER specific rules (indefinite length encoding, Boolean values, etc.), the tree view is created (fig. 3).

| ₽ asnViewer                   |                                     |            |
|-------------------------------|-------------------------------------|------------|
| File ?                        |                                     |            |
| 🔓 Open encoded 🛛 🛛 🖉 🔎 Deco   | de 🔽 Display source                 | ?          |
| SEQUENCE                      | 30 80 06 09 2A 86 48 86 F7 0D 01 07 | 02 🔼       |
| OBJECT IDENTIFIER             | AO 80 30 80 02 01 01 31 00 30 80 06 | 09         |
| 🗄 📲 [0] (EXPLICIT)            | 2A 86 48 86 F7 0D 01 07 01 00 00 A0 | 82 💻       |
|                               | 05 D4 30 82 02 A1 30 82 02 OA A0 03 | ; 02       |
|                               | 01 02 02 01 01 30 0D 06 09 2A 86 48 | ; 86       |
|                               |                                     | 09         |
|                               | 06 03 55 04 06 13 02 46 52 31 10 30 |            |
|                               | 06 03 55 04 0A 13 07 54 65 73 74 20 |            |
|                               |                                     | 552<br>179 |
|                               | 20 2D 20 43 6C 61 73 73 20 33 20 63 |            |
|                               |                                     | : 17       |
|                               | OD 30 36 30 39 30 35 30 38 30 33 32 |            |
|                               | 5A 17 OD 32 36 30 39 30 35 30 38 30 |            |
|                               | 32 33 5A 30 4F 31 0B 30 09 06 03 55 |            |
|                               | 06 13 02 46 52 31 10 30 OE 06 03 55 | ; 04 🔽     |
|                               | 1                                   |            |
|                               |                                     |            |
|                               |                                     |            |
| 👂 Interpretation  🚵 Raw value |                                     |            |
| E:\CertificateChain.p7b       |                                     |            |

Figure 3

Changing current decoding rules to DER leads to an error in the tree view creation process (fig. 4) as DER is a subset of BER.



| ₽ asnViewer                                   |                                                                            |      |
|-----------------------------------------------|----------------------------------------------------------------------------|------|
| File ?                                        |                                                                            |      |
| 🔓 Open encoded 🛛 🛛 DER 💌 🔎 Decode             | ☑ Display source                                                           | ?    |
| Decoding error: Indefinite length not allowed | 30 80 06 09 2A 86 48 86 F7 0D 01 07                                        | 02 📩 |
|                                               | AO 80 30 80 02 01 01 31 00 30 80 06                                        | 09 📃 |
|                                               | 2A 86 48 86 F7 0D 01 07 01 00 00 A0                                        | 82 📃 |
|                                               | 05 D4 30 82 02 A1 30 82 02 0A A0 03                                        | 02   |
|                                               | 01 02 02 01 01 30 0D 06 09 2A 86 48                                        | 86   |
|                                               |                                                                            | 09   |
|                                               | 06 03 55 04 06 13 02 46 52 31 10 30                                        |      |
|                                               | 06 03 55 04 0A 13 07 54 65 73 74 20                                        |      |
|                                               | 41 31 2E 30 2C 06 03 55 04 0B 13 25                                        |      |
|                                               |                                                                            | 79   |
|                                               | 20 2D 20 43 6C 61 73 73 20 33 20 63<br>72 74 69 66 69 63 61 74 65 73 30 1E |      |
|                                               | 0D 30 36 30 39 30 35 30 38 30 33 32                                        |      |
|                                               |                                                                            | 33   |
|                                               | 32 33 5A 30 4F 31 0B 30 09 06 03 55                                        |      |
|                                               | 06 13 02 46 52 31 10 30 0E 06 03 55                                        |      |
|                                               |                                                                            |      |
|                                               |                                                                            |      |
|                                               |                                                                            |      |
| 🔎 Interpretation 📑 Raw value                  |                                                                            |      |
| E:\CertificateChain.p7b                       |                                                                            |      |

Figure 4



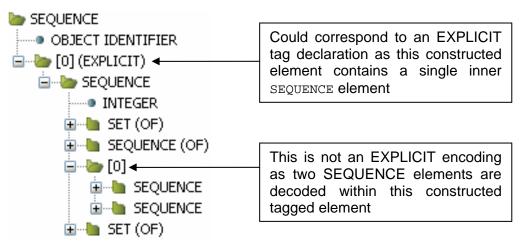
Decoding rules can be selected before loading a file to avoid decoding errors.



## Tree view display

The tree view presents a readable version of the encoded file. asnViewer tries to interpret tags when possible:

- Untagged primitive types are directly recognized
- Untagged constructed types are displayed depending on their inner elements to make a difference between SEQUENCE and SEQUENCE OF objects as well as SET and SET OF objects. If a constructed object comprises two different inner elements tags (an INTEGER and a BOOLEAN for example), asnViewer displays the appropriate type (SEQUENCE or SET) instead of the corresponding collection (SEQUENCE OF or SET OF). The OF suffix is displayed between parenthesis as asnViewer cannot be sure that the decoded element is a collection of similar inner elements (SEQUENCE OF OR SET OF)
- Tagged objects are displayed according to their ASN.1 specification: class and tag value are enclosed between squares ([APPLICATION 0] if class is APPLICATION or [0] if CONTEXT for example). Explicit tagging is proposed when the tagged object is encoded in constructed form and it encloses a single inner (tagged or untagged) object (fig. 5).





A message replaces the tree view decoding in the following cases:

- The selected rules are not able to decode the encoded file (decoding error shown in fig. 4)
- The file contains extra information, no matter where this information is located (security error). Please refer to PowerASN for Java security for more details.



### Browsing the tree view

Clicking on a  $\pm$  sign (or alternatively, double-clicking on a constructed element) displays or hides its inner elements.

Selecting a tree view element highlights its corresponding hexadecimal part in the source file (fig. 6).

| ₽ asnViewer                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| File ?                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                            |
| 🔓 Open encoded 🛛 🛛 🖉 🔎 Decode                                                                                                                           | V Display source                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ?                                                                                                                          |
| SEQUENCE<br>OBJECT IDENTIFIER<br>[0] (EXPLICIT)<br>SEQUENCE<br>INTEGER<br>SET (OF)<br>SEQUENCE (OF)<br>OBJECT IDENTIFIER<br>[0]<br>SET (OF)<br>SET (OF) | 06       03       55       04       06       13       02       46       52       31       10       3         06       03       55       04       0A       13       07       54       65       73       74       3         41       31       2E       30       2C       06       03       55       04       0B       13       3         6F       6F       74       20       41       75       74       68       6F       72       69       3         20       2D       20       43       6C       61       73       73       20       33       20       6         72       74       69       66       69       63       61       74       65       73       30       10 | 06 09<br>A0 82<br>03 02<br>48 86<br>30 09<br>30 0E<br>20 43<br>25 52<br>74 79<br>53 65<br>1E 17<br>32 33<br>30 33<br>55 04 |
| 1                                                                                                                                                       | <u></u>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                            |
| Interpretation Raw value                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                            |
| E:\CertificateChain.p7b                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                            |

Figure 6

Tag-Length-Value components are depicted using different colors:

- Tag (or type) is shown in green
- Length is highlighted in orange (definite length, see fig. 6) or in rose (indefinite length). In case of indefinite length, end flags (double zero) are also displayed in rose (fig. 7)



• Value is always displayed is light gray, independently from the ASN.1 object form.

| ₽ asnViewer                   |            |            |       |       |          |    |     |     |    |     |    |          |     | ×        |
|-------------------------------|------------|------------|-------|-------|----------|----|-----|-----|----|-----|----|----------|-----|----------|
| File ?                        |            |            |       |       |          |    |     |     |    |     |    |          |     |          |
| 🔓 Open encoded 🛛 🛛 🖉 🖉 Decode | [          | <b>v</b> D | ispla | iy so | urce     |    |     |     |    |     |    |          |     | ?        |
| SEQUENCE                      | 30         | 80         | 06    | 09    | 2A       | 86 | 48  | 86  | F7 | OD  | 01 | 07       | 02  | ^        |
| OBJECT IDENTIFIER             | AO         | 80         | 30    | 80    | 02       | 01 | 01  | 31  | 00 | 30  | 80 | 06       | 09  |          |
| 😑 🐚 [0] (EXPLICIT)            | 2A         | 86         | 48    | 86    | F7       | OD | 01  | 07  | 01 | 00  | 00 | AO       | 82  |          |
| E                             | 05         | D4         | 30    | 82    | 02       | Al | 30  | 82  | 02 | OA  | AO | 03       | 02  |          |
|                               | 01         | 02         | 02    | 01    | 01       | 30 | OD  | 06  | 09 | 2A  | 86 | 48       | 86  |          |
|                               | <b>F</b> 7 |            |       |       | 04       |    |     |     |    | 31  |    | 30       |     |          |
| OBJECT IDENTIFIER             |            |            |       |       | 06       |    |     |     |    |     |    |          |     |          |
|                               |            |            |       |       | ΟA       |    |     |     |    |     |    |          |     |          |
|                               |            |            |       |       | 2C       |    |     |     |    |     |    |          |     |          |
|                               |            |            |       |       | 41       |    |     |     |    |     |    | 74       |     |          |
|                               | 11         |            |       |       | 6C       |    | • - | • - |    |     |    |          |     |          |
|                               |            | • -        |       |       | 69       |    |     | • - |    | • = |    |          | - · |          |
|                               |            |            |       |       | 39<br>36 |    |     |     |    |     |    | 32<br>30 |     |          |
|                               |            |            |       |       | 30<br>4F |    |     |     |    |     |    |          |     |          |
|                               | 11         |            |       |       | 4r<br>52 |    |     |     |    |     |    |          |     |          |
|                               | 00         | 10         | 02    | 40    | 52       | 51 | 10  | 50  | OL | 00  | 00 | 55       | 04  | <u> </u> |
|                               |            |            |       |       |          |    |     |     |    |     |    |          |     |          |
|                               |            |            |       |       |          |    |     |     |    |     |    |          |     | - II     |
|                               |            |            |       |       |          |    |     |     |    |     |    |          |     |          |
| 👂 Interpretation  🗎 Raw value |            |            |       |       |          |    |     |     |    |     |    |          |     | _        |
| E:\CertificateChain.p7b       |            |            |       |       |          |    |     |     |    |     |    |          |     |          |

Figure 7



## Hiding / showing the source file

It is possible to show or hide the source file in the hexadecimal view by respectively checking or unchecking the "Display source" box. Hiding the source file hexadecimal view (fig. 8) is mainly used when the tree view needs more horizontal space or when the file loading process raises an out of memory error (in case of huge files only).

Unchecking the "Display source" box before loading a file prevents from loading this file into the hexadecimal view. The file is not loaded in the hexadecimal view until this box is checked.

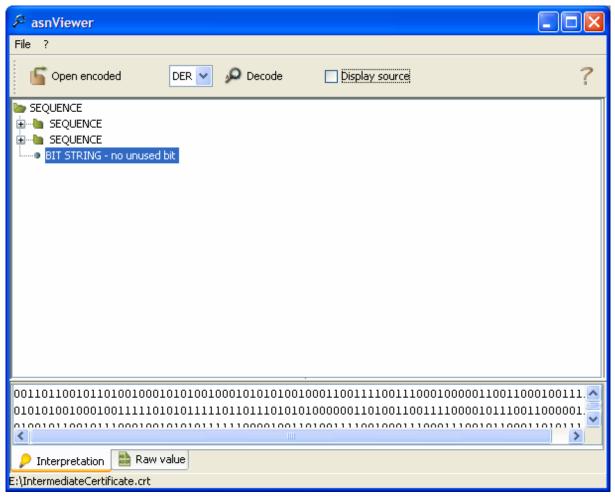


Figure 8





Ĩ

When displaying huge files, it is recommended to uncheck the "Display source" checkbox.

Changing the selected component is the tree view (fig. 9) is reflected to the hexadecimal view (fig. 110) when the "Display source" box is checked. The selected file is loaded into the hexadecimal view if not already loaded. Thus it may take some time to display the source file.

| ₽ asnViewer                                    |                |                |   |
|------------------------------------------------|----------------|----------------|---|
| File ?                                         |                |                |   |
| 🔓 Open encoded                                 | BER 🔽 🔎 Decode | Display source | ? |
| SEQUENCE<br>SEQUENCE<br>BIT STRING - no unused | bit            |                |   |
| 🔎 Interpretation 📑 Raw v                       | alue           |                |   |
| E:\IntermediateCertificate.crt                 |                |                |   |

Figure 9



| ₽ asnViewer File ?             |    |          |        |       |          |    |    |    |    |          |    | -        | )        |   |
|--------------------------------|----|----------|--------|-------|----------|----|----|----|----|----------|----|----------|----------|---|
| 🔓 Open encoded 🛛 📴 🖉 🔎 Decode  |    | <b>.</b> | vispla | iy so | urce     |    |    |    |    |          |    |          |          | ? |
| SEQUENCE                       | 30 | 82       | 02     | АЗ    | 30       | 82 | 02 | 00 | AO | 03       | 02 | 01       | 02       | ^ |
|                                | 02 | 02       | 30     | 39    | 30       | OD | 06 | 09 | 2A | 86       | 48 | 86       | F7       |   |
|                                | OD | 01       | 01     | 04    | 05       | 00 | 30 |    | 31 |          | 30 | 09       | 06       | _ |
| BIT STRING - no unused bit     | 03 |          |        |       | 13       |    |    |    | 31 |          |    | 0E       | 06       | = |
|                                | 03 |          |        |       | 13       |    |    |    |    |          |    |          | 41       |   |
|                                | 31 |          |        |       | 06       |    |    |    |    | 13       |    |          | 6F       |   |
|                                | 6F |          |        |       | 75       |    |    |    | 72 | 69       |    | 79       | 20       |   |
|                                | 2D |          |        |       | 61<br>63 |    |    |    |    | 20<br>30 |    | 65<br>17 |          |   |
|                                |    |          |        |       | 31       |    |    |    |    | 37       |    | 31       | OD<br>۶۸ |   |
|                                | 17 |          |        |       |          | 39 |    |    |    | 37       |    | 37       |          |   |
|                                | 31 |          |        |       | 31       |    |    | 09 |    | 03       |    |          |          |   |
|                                | 13 |          |        |       | 31       |    |    |    |    | 03       |    |          |          |   |
|                                | 13 |          |        | 65    |          | 74 |    | 43 | 41 | 31       |    | 30       |          |   |
|                                | 06 | 03       | 55     | 04    | 0B       | 13 | 25 | 52 | 6F | 6F       | 74 | 20       | 41       |   |
|                                | 75 | 74       | 68     | 6F    | 72       | 69 | 74 | 79 | 20 | 2D       | 20 | 43       | 6C       |   |
|                                |    | -        | -      |       |          | ~~ |    | ~~ | -  |          |    | ~~       |          |   |
|                                |    |          |        |       |          |    |    |    |    |          |    |          |          |   |
|                                |    |          |        |       |          |    |    |    |    |          |    |          |          |   |
| 👂 Interpretation 📑 Raw value   |    |          |        |       |          |    |    |    |    |          |    |          |          |   |
| E:\IntermediateCertificate.crt |    |          |        |       |          |    |    |    |    |          |    |          |          |   |

Figure 10



#### Interpretation and raw tabs

All primitive objects (independently from their tagging) are evaluated in the interpretation and raw section. The interpretation tab (fig. 11) shows the human-readable value of the ASN.1 primitive object (except OCTET STRING ASN.1 objects which may enclose non-printable characters).

| ₽ asnViewer                                    |                                                                                |      |
|------------------------------------------------|--------------------------------------------------------------------------------|------|
| File ?                                         |                                                                                |      |
| 🥤 Open encoded 🛛 🛛 DER 🔽 🔎 Decode              | ✓ Display source                                                               | ?    |
| SEQUENCE                                       | 75 74 68 6F 72 69 74 79 20 2D 20 43 6                                          | 5C 🔼 |
|                                                | 61 73 73 20 33 20 63 65 72 74 69 66 6                                          | 59   |
| E SEQUENCE                                     | 63 61 74 65 73 82 02 30 39 30 OE 06 (                                          | 33   |
| NULL                                           | 55 1D OF 01 01 FF 04 04 03 02 00 OB                                            | 30   |
| <ul> <li>BIT STRING - no unused bit</li> </ul> | OD <mark>06 09</mark> 2A 86 48 86 F7 OD 01 01 04 0                             |      |
|                                                | 00 03 81 81 00 36 5A 45 48 AA 46 79 (                                          |      |
|                                                | 19 89 F5 48 9F 57 DB AA 06 99 E1 73 (                                          |      |
|                                                | 4B 2E 25 5F 84 D3 C8 E3 96 35 E6 E3 8                                          |      |
|                                                | A4 A2 63 FA B4 F7 57 B8 0C 4D 86 6D 4<br>C5 E3 0D 20 1C 40 68 07 05 52 82 C7 9 |      |
|                                                | 3D 3B A4 9D F3 F7 E5 C3 71 39 EA 93 8                                          |      |
|                                                | CB 01 46 C6 62 C1 A7 17 F1 29 22 1E 1                                          |      |
|                                                | 94 99 13 36 E1 5D EA F5 84 BF 7C 52 (                                          | -    |
|                                                | 82 54 EA C3 88 A4 9D 3F AC 8F C7 FB I                                          | A    |
|                                                | E9 4E 24 49 EF 79 56 32 37 29 EC 97 1                                          | Fl   |
|                                                | 40 08 65                                                                       | ~    |
| 1.2.840.113549.1.1.4                           | I                                                                              |      |
| Interpretation Raw value                       |                                                                                |      |
| E:\IntermediateCertificate.crt                 |                                                                                |      |

Figure 11

Each interpreted values is deduced from the source raw value (fig. 12) of the considered ASN.1 primitive object. The raw value is also displayed in the source file hexadecimal view. This tab is of great help when the file could not be loaded in the hexadecimal view (or when "display source" is not checked).



| ♀ asnViewer                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                        |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| File ?                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                        |
| 🔓 Open encoded 🛛 🛛 DER 🔽 🔎 Decode                                               | V Display source                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ?                                                                                                                                      |
| SEQUENCE<br>SEQUENCE<br>OBJECT IDENTIFIER<br>NULL<br>BIT STRING - no unused bit | 75       74       68       6F       72       69       74       79       20       20       20       43       6         61       73       73       20       33       20       63       65       72       74       69       66       6         63       61       74       65       73       82       02       30       39       30       0E       06       0         65       10       0F       01       01       FF       04       04       03       02       00       0E       0         00       06       09       2A       86       48       86       F7       0D       01       01       04       0         00       03       81       81       00       36       5A       45       48       A4       69       E1       73       0         19       89       F5       48       9F       57       DB       AA       69       E1       73       0         4B       2E       25       5F       84       D3       C8       E3       66       60       4       4       A4       A2       6 | 59<br>53<br>30<br>55<br>54<br>57<br>35<br>44<br>77<br>36<br>77<br>37<br>37<br>37<br>37<br>37<br>37<br>37<br>37<br>37<br>37<br>37<br>37 |
|                                                                                 | E9 4E 24 49 EF 79 56 32 37 29 EC 97 1<br>40 08 65                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | F1 🗸                                                                                                                                   |
| 2A 86 48 86 F7 0D 01 01 04                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                        |
| E:\IntermediateCertificate.crt                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                        |

Figure 12

BIT STRING values are interpreted as 0, 1 sequences. The number of unused bits is displayed in the tree view. However, the "raw" tab indicates the number of unused bits as its first hexadecimal couple.



Please note that "Interpretation" and "Raw" tabs only refer to primitive objects.



## **Known limitations**

#### Available rules

asnViewer supports BER and DER rules only. XER is not scheduled as this encoding is intrinsically user-friendly. Other encoding rules will be available depending on PowerASN for Java encoding rules support.

#### **Opening huge files**

Huge files may not be correctly displayed in the hexadecimal view. In this case, the hex view is replaced by <Out of memory>. Moreover, the cursor does not change to a waiting cursor during the opening process, although the corresponding pieces of code are present.

If any idea to replace the current hexadecimal view with another able to display large files, please let me know.

## Contact



For any comment, suggestion or bug fix related to current version of this software, please refer to PowerASN website (http://www.powerasn.com) to get asnViewer appropriate email adress.