Wireless Innovation Forum Contribution

Committee: SSC WG4 CBSD Task Group
Title: WInnForum CBSD/DP UUT Security Test Cases Tutorial
Short Title: WInnForum CBSD/DP UUT Security Test Cases Tutorial
Source:

Idan Raz
Airspan

Date: [27 June 2018]
Distribution: [Members]

Document Summary: Tutorial for the WInnForum CBSD UUT Security Test Cases

Notes of Importance: [Optional. Short statement; please limit to 50 words or less.]

Impacts/Effects: [Optional. Short statement; please limit to 50 words or less.]

Action Desired: [Optional]
Action Required for Closure: [Optional]
Desired Disposition Date: [Day Month Year]

WInnForum CBSD/DP UUT Security Test Cases Tutorial

Version V1.0.0.0

27 June 2018

TERMS, CONDITIONS & NOTICES

This document has been prepared by the SSC Work Group 4 to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the SSC Work Group 4.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Table of Contents

List of Figures

List of Tables

Contributors

The following individuals made significant contributions to this document:

Idan Raz (Airspan)

WInnForum CBSD/DP UUT Security Test Cases Tutorial

1 Introduction

WInnForum SAS Test Harness is developed for test and certification purposes of CBSD/DP UUT. The WInnForum SAS Test Harness is available for download from the GitHub repository https://github.com/Wireless-Innovation-Forum/Citizens-Broadband-Radio-Service-Device

Note: It is recommended to check the GitHub repository as the Test Harness code may have periodic updates to address reported items.

According to [n.3] there are security test cases required which are not implemented in the WInnForum SAS Test Harness available on GitHub. This tutorial describes the execution method of the security test cases described in [n.3]

2 Scope

This document is the tutorial for executing the security test cases for CBSD/Domain Proxy UUT described in [n.3].

3 References

3.1 Normative references

The following referenced documents are necessary for the application of the present document.

[n.1] WINNF-TS-0065 Version V1.1.0, “CBRS Communications Security Technical Specification”, 26 July 2017

[n.2] WINNF-TS-0022 Version V1.1.2, “WInnforum CBRS Certificate Policy Specification”, 6 February 2018

[n.3] WINNF-TS-0122 Version V1.0.0, “Conformance and Performance Test Technical Specification; CBSD/DP as Unit Under Test (UUT)”, 19 December 2017

[n.4] WINNF-IN-0156 Version V1.0.0.1, “WInnForum SAS Test Harness CBSD UUT Tutorial”, 2 March 2018

4 Definitions and abbreviations

4.1 Abbreviations

CBSD	Citizens Broadband Radio Service Device
CBRS	Citizens Broadband Radio Service
CFR	Code of Federal Regulation
CPI	Certified Professional Installer
DP	Domain Proxy
HTTP	Hypertext Transfer Protocol

HTTPS	HTTP over TLS
JSON	JavaScript Object Notation
SAS	Spectrum Access System
TLS	Transport Layer Security

4.2 Definitions

CBRS band: The 3550-3700 MHz Citizens Broadband Radio Service band.

CBSD Registration: The procedure by which a CBSD indicates to a SAS its intention to operate. Successful registration implies a validation by the SAS that the CBSD has been FCC certified and confers on the CBSD the right to be authorized by the SAS to operate in accordance with a Grant. During the registration process, each CBSD provides a fixed location, unique identifiers (e.g., owner information, device information), *Group* membership, and radio-related capabilities. A successful registration procedure concludes with the SAS providing a unique identifier for that CBSD.

CBSD User: The registered entity that has operational responsibility for the CBSD.

Channel: the contiguous frequency range between lower and upper frequency limits.

Citizens Broadband Radio Service Device (CBSD): Fixed Stations, or networks of such stations, that operate on a Priority Access or General Authorized Access basis in the Citizens Broadband Radio Service consistent with Title 47 CFR Part 96. For CBSDs which comprise multiple nodes or networks of nodes, CBSD requirements apply to each node even if network management and communication with the SAS is accomplished via a single network interface.

Domain Proxy (DP): An entity engaging in communications with the SAS on behalf of multiple individual CBSDs or networks of CBSDs. The Domain Proxy can also provide a translational capability to interface legacy radio equipment in the 3650-3700 MHz band with a SAS to ensure compliance with Part 96 rules.

Spectrum Access System (SAS): A system that authorizes and manages use of spectrum for the Citizens Broadband Radio Service.

5 Prerequisites for CBSD/DP UUT Security Test Cases Execution

The method for executing CBSD/DP UUT security test case is via Wireshark. Wireshark is available for download from https://www.wireshark.org/#download and can be installed on Windows and Linux platforms. Please download and install the latest available version from Wireshark website.

5.1 Capturing Packets

5.1.1 Windows Operating System

5.1.1.1 The WinPcap is installed as part of the Wireshark installation

5.1.2 Linux Operating System

It is possible to use Linux tcpdump command for capturing packets and use Wireshark to inspect the file generated by tcpdump.

5.2 Wireshark Display of SSL/TLS Packets of WInnForum SAS Test Harness

The SAS<->CBSD messages are actually TLS protocol messages. In order to view in Wireshark the packets running between WInnForum SAS Test Harness and CBSD/DP UUT do the following:

1. Write the port number appearing in the conf.xml file of the SAS Test Harness (default value appearing is 5000).

2. In Wireshark go to Analyze → "Decode As" menu. Add "TCP Port 5000" to be decoded as SSL. (The port number is according to the conf.xml file. 5000 is the default value).

3. Press "Save" and "OK".

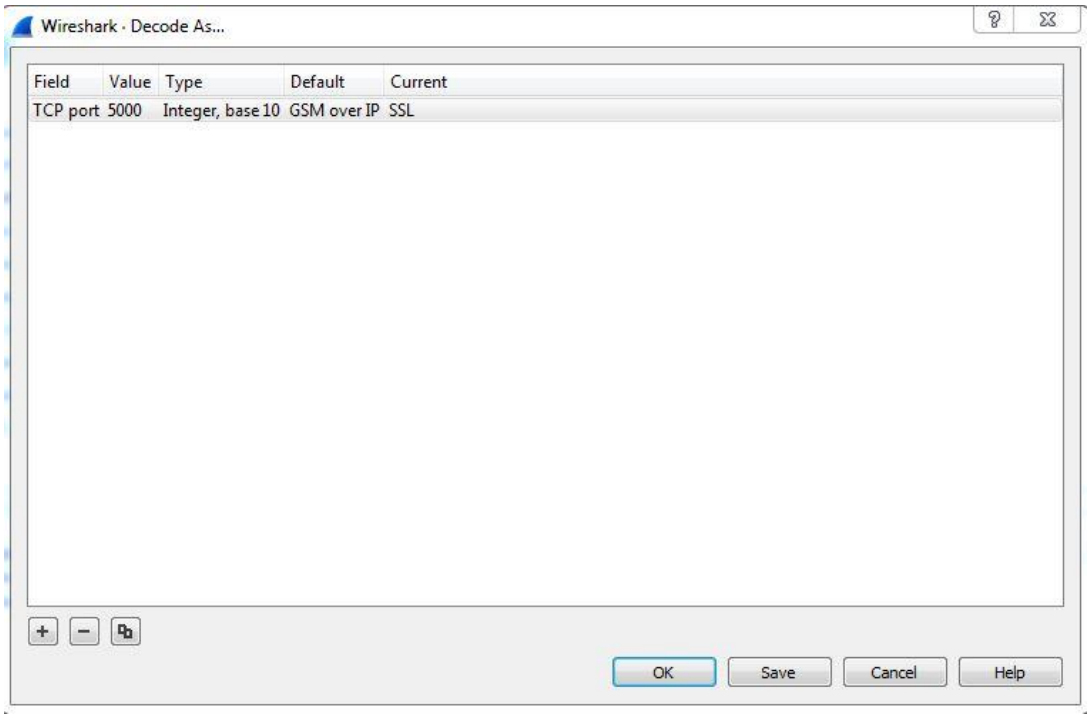

Figure 1: Wireshark "TCP Port 5000 Decode as SSL"

5.3 Wireshark Display of Time Synchronization in Captured Packets

In order to view in Wireshark the captured packets in their UTC time, in Wireshark go to View → Time Display Format and select "UTC Date and Time of Day"

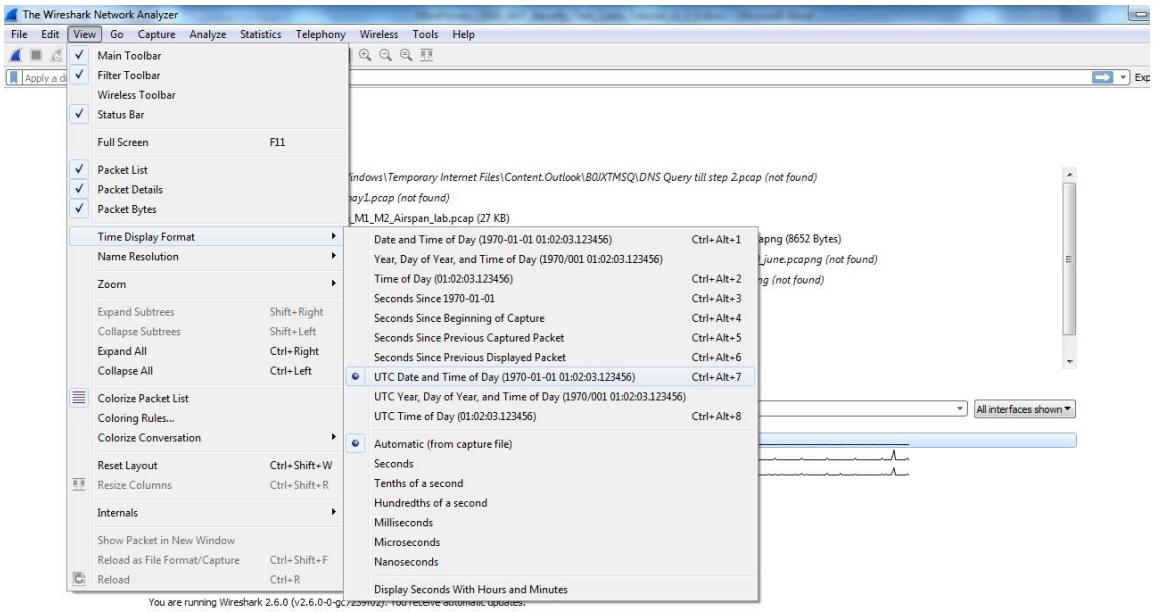

Figure 2: Wireshark UTC Display

5.4 Wireshark Display of WInnForum SAS Test Harness Packets

In order to filter in Wireshark the captured packets related to the SAS Test Harness and CBSD/DP UUT, apply in Wireshark the following filter: ip.addr==<SAS Test Harness IP address> && ssl

<SAS Test Harness IP address> is according to the conf.xml file of SAS Test Harness

6 Executing the CBSD/DP UUT Security Test Cases

6.1 Executing WINNF.FT.C.SCS.1 Successful TLS connection between UUT and SAS Test Harness

Test case [WINNF.FT.C.SCS.1] "Successful TLS connection between UUT and SAS Test Harness" is described in [n.3].

Place in the WInnForum SAS Test Harness the correct SAS Test Harness X.509 certificates for this test case. Edit the conf.xml file appropriately for use of this certificate.

Verify the SAS Test Harness X.509 certificate is the correct X.509 certificate for this test case by inspecting its content as described in the "readme_file_x509_RSA_certs_test_labs.txt" [n.4]. For test case [WINNF.FT.C.SCS.1] the X.509 certificate is the regular SAS Test Harness X.509 certificate used for the Interface Conformance Testing in [n.3]

Activate the WInnForum SAS Test Harness using "StartOfProject.py" as described in [n.4].

Verify in Wireshark the following in the captured packets:

1. Wireshark "Protocol" column shows "TLSv1.2"
2. CBSD/DP UUT sends "Client Hello" message to WInnForum SAS Test Harness
3. WInnForum SAS Test Harness sends "Server Hello" message to CBSD/DP UUT.
    - The "Server Hello" message "Handshake Protocol" IE includes the "Cipher Suite" IE.
    - Verify the "Cipher Suite" shown in Wireshark is one of the following: TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
4. "Application Data" messages are exchanged between WInnForum SAS Test Harness and CBSD/DP UUT.

Verify that WInnForum SAS Test Harness Command Prompt shows Registration Request Message from CBSD/DP UUT

Stop the WInnForum SAS Test Harness before moving to the next test (Close or Exit the WInnForum SAS Test Harness Command Prompt)

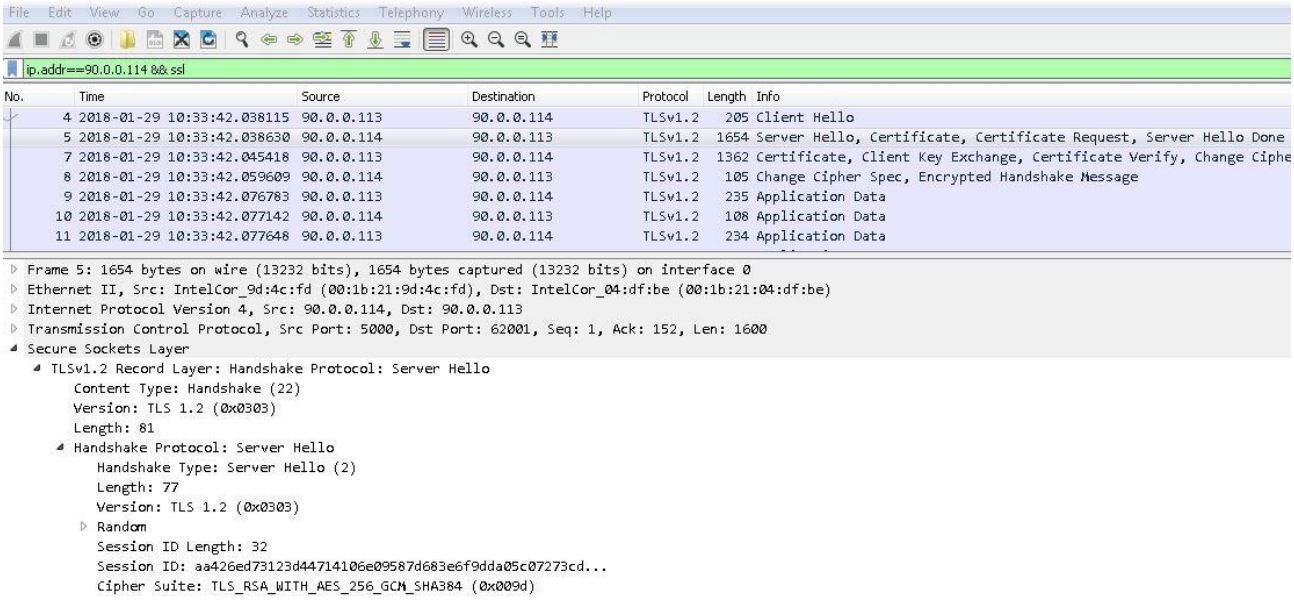

Figure 3: Wireshark Capture Example for Test [WINNF.FT.C.SCS.1]

6.2 Executing WINNF.FT.C.SCS.2 TLS Failure due to Revoked Certificate

Test case [WINNF.FT.C.SCS.2] "TLS failure due to revoked certificate" is described in [n.3].

Place in the WInnForum SAS Test Harness the correct SAS Test Harness X.509 certificates for this test case. Edit the conf.xml file appropriately for use of this certificate.

Verify the SAS Test Harness X.509 certificate is the correct X.509 certificate for this test case by inspecting its content as described in the "readme_file_x509_RSA_certs_test_labs.txt" [n.4]. For test case [WINNF.FT.C.SCS.2] the X.509 certificate has

- Proper Validity time (the X.509 certificate is not expired)
- X.509v3 extension of "Authority Information Access: OCSP - URI: http://ocsp.testharness.cbrstestlab.com"
  (this URI is an example of the OCSP server available for the test lab)
- X.509v3 extension of "CRL Distribution Points: Full Name: URI: http://crlserver.testharness.cbrstestlab.com/crlserver.crl"
  (this URI is an example of the CRL server and CRL file available for the test lab)
- Certificate Serial Number appears as "Revoked" in the CRL file located in the CRL server available for the test lab, or appears as "Revoked" in the OCSP server available for the test lab.

For execution of this test case the CRL file must have proper validity. If this test is intended to be executed when the validity date of the CRL file has expired, a new CRL file with proper validity needs to be generated as described in the "readme_file_x509_RSA_certs_test_labs.txt" [n.4].

For execution of this test case, the test lab also requires an available DNS server to resolve FQDNs of the OCSP server or CRL server.

For this test case apply in Wireshark the following filter: (ip.addr==<SAS Test Harness IP address> && ssl) || dns || ocsp || http

Activate the WInnForum SAS Test Harness using "StartOfProject.py" as described in [n.4].

Verify in Wireshark the following in the captured packets:

1. Wireshark "Protocol" column shows "TLSv1.2"

2. CBSD/DP UUT sends "Client Hello" message to WInnForum SAS Test Harness

3. WInnForum SAS Test Harness sends "Server Hello" message to CBSD/DP UUT.

    - The "Server Hello" message "Handshake Protocol" IE includes the "Cipher Suite" IE.

    - Verify the "Cipher Suite" shown in Wireshark is one of the following:
      TLS_RSA_WITH_AES_128_GCM_SHA256,
      TLS_RSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

4. CBSD/DP UUT performs DNS resolution for the FQDN of the CRL server, or OCSP server, or both listed in the X.509v3 extensions described above for the X.509 certificate of SAS Test Harness.

5. CBSD/DP UUT:

    - Download the CRL file according to the full URI listed in X.509v3 extension of "CRL Distribution Points" described above.

    OR

    - Send to the OCSP server an OCSP "Request" message containing the certificate serial number, and OCSP server replies.

    OR

    - Both CRL file download and OCSP transaction as described above.

6. "Application Data" messages are not seen between WInnForum SAS Test Harness and CBSD/DP UUT.

7. CBSD/DP UUT may send a TLS "Alert" message to WInnForum SAS Test Harness notifying of rejecting the TLS connection before attempting to establish the TLS connection again.

Verify that WInnForum SAS Test Harness Command Prompt does not show any Request Message from CBSD/DP UUT

Stop the WInnForum SAS Test Harness before moving to the next test (Close or Exit the WInnForum SAS Test Harness Command Prompt)

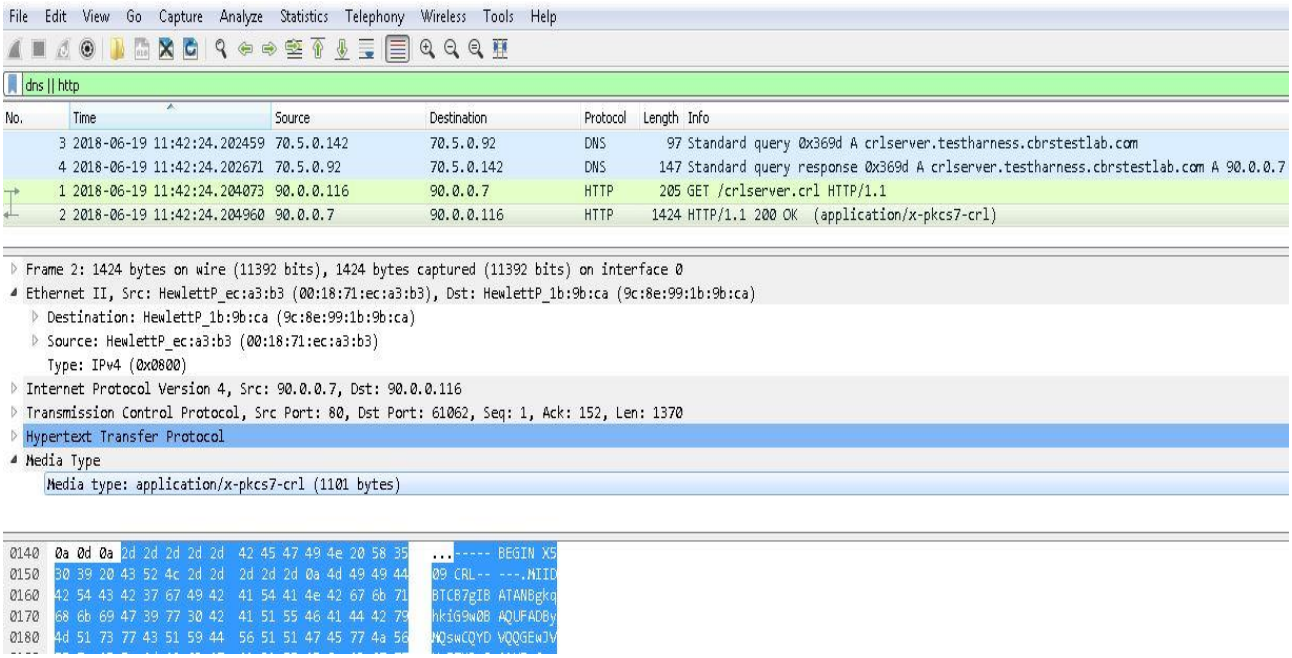

Figure 4: Wireshark Capture Example Test [WINNF.FT.C.SCS.2] – DNS Resolution of CRL Server Followed by CRL File Retrieval

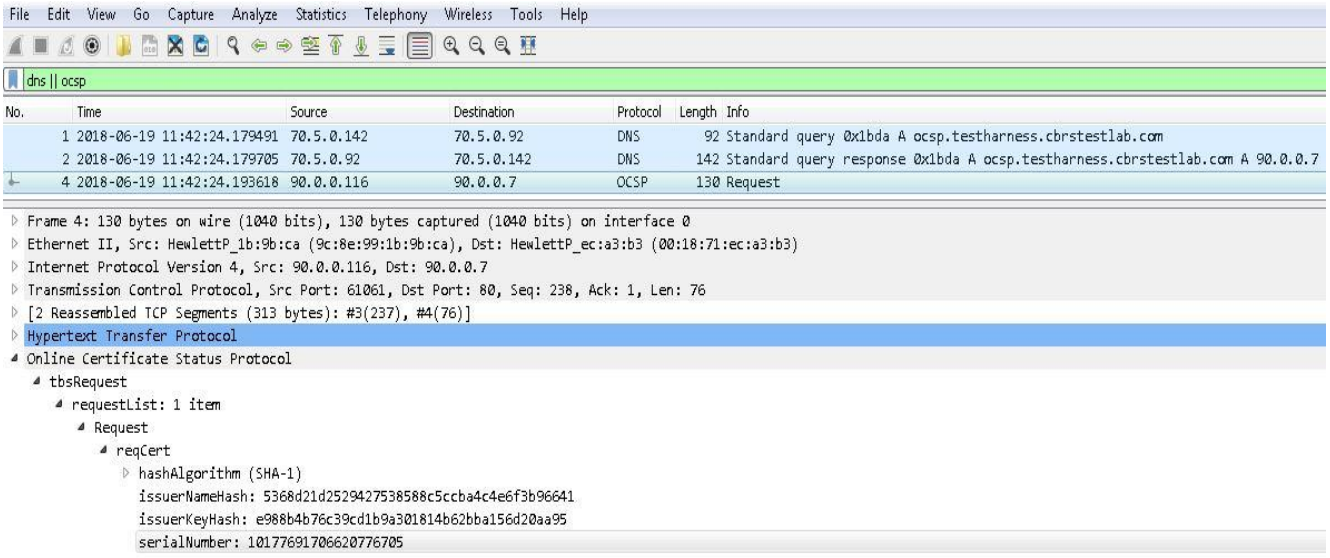

Figure 5: Wireshark Capture Example for Test [WINNF.FT.C.SCS.2] - DNS Resolution of OCSP Server Followed by OCSP Request

The following shows a proposed lab setup for executing test case WINNF.FT.C.SCS.2. Test lab may combine several entities into a single machine based on its IT capabilities.

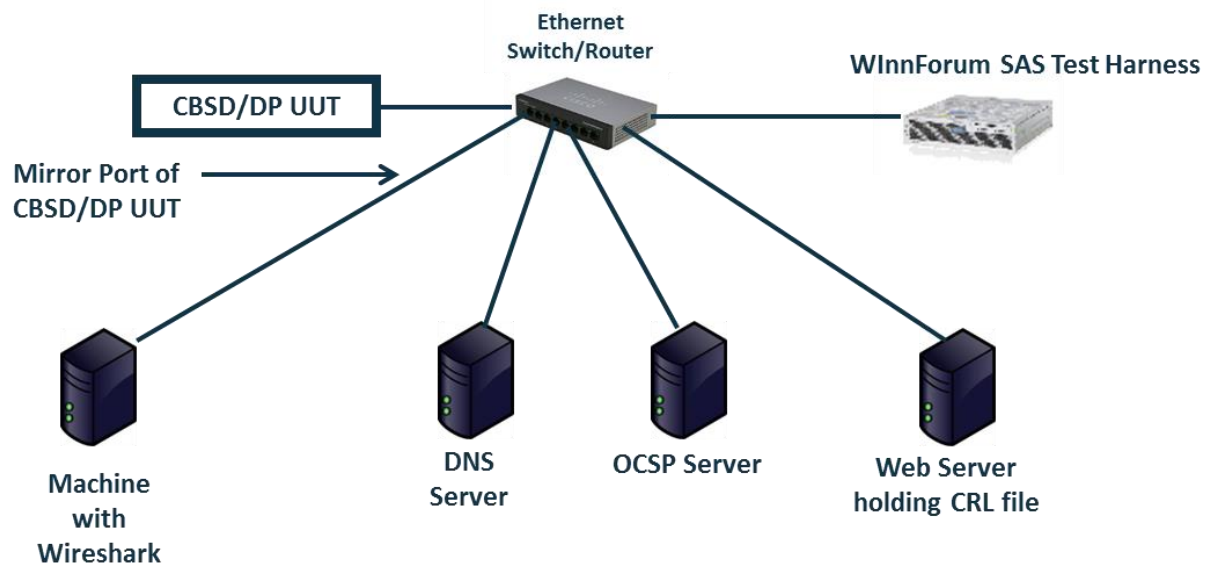

Figure 6: Proposed Test Lab Setup for Test [WINNF.FT.C.SCS.2]

6.3 Executing WINNF.FT.C.SCS.3 TLS Failure due to Expired Server Certificate

Test case [WINNF.FT.C.SCS.3] “TLS failure due to expired server certificate” is described in [n.3].

Place in the WInnForum SAS Test Harness the correct SAS Test Harness X.509 certificates for this test case. Edit the conf.xml file appropriately for use of this certificate.

Verify the SAS Test Harness X.509 certificate is the correct X.509 certificate for this test case by inspecting its content as described in the “readme_file_x509_RSA_certs_test_labs.txt” [n.4]. For test case [WINNF.FT.C.SCS.3] the X.509 certificate has

- Expired Validity time. The date appearing in the “Not After” parameter of the X.509 certificate has passed.

Activate the WInnForum SAS Test Harness using “StartOfProject.py” as described in [n.4].

Verify in Wireshark the following in the captured packets:

1. Wireshark “Protocol” column shows “TLSv1.2”

2. CBSD/DP UUT sends “Client Hello” message to WInnForum SAS Test Harness

3. WInnForum SAS Test Harness sends “Server Hello” message to CBSD/DP UUT.

    - The “Server Hello” message “Handshake Protocol” IE includes the “Cipher Suite” IE.

    - Verify the “Cipher Suite” shown in Wireshark is one of the following:
      TLS_RSA_WITH_AES_128_GCM_SHA256,
      TLS_RSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

4. “Application Data” messages are not seen between WInnForum SAS Test Harness and CBSD/DP UUT.

5. CBSD/DP UUT may send a TLS “Alert” message to WInnForum SAS Test Harness notifying of rejecting the TLS connection before attempting to establish the TLS connection again.

Verify that WInnForum SAS Test Harness Command Prompt does not show any Request Message from CBSD/DP UUT

Stop the WInnForum SAS Test Harness before moving to the next test (Close or Exit the WInnForum SAS Tes Harness Command Prompt)

6.4 Executing WINNF.FT.C.SCS.4 TLS Failure when SAS Test Harness Certificate is issued by an Unknown CA

Test case [WINNF.FT.C.SCS.4] "TLS failure when SAS Test Harness certificate is issued by an unknown CA" is described in [n.3].

Place in the WInnForum SAS Test Harness the correct SAS Test Harness X.509 certificates for this test case. Edit the conf.xml file appropriately for use of this certificate.

Verify the SAS Test Harness X.509 certificate is the correct X.509 certificate for this test case by inspecting its content as described in the "readme_file_x509_RSA_certs_test_labs.txt" [n.4]. For test case [WINNF.FT.C.SCS.4] the X.509 certificate has

- PKI chain which is not known to the CBSD/DP UUT, and is different from the PKI chain of the SAS Test Harness X.509 certificate used in test WINNF.FT.C.SCS.1.

Activate the WInnForum SAS Test Harness using "StartOfProject.py" as described in [n.4]

Verify in Wireshark the following in the captured packets:

1. Wireshark "Protocol" column shows "TLSv1.2"

2. CBSD/DP UUT sends "Client Hello" message to WInnForum SAS Test Harness

3. WInnForum SAS Test Harness sends "Server Hello" message to CBSD/DP UUT.

    - The "Server Hello" message "Handshake Protocol" IE includes the "Cipher Suite" IE.

    - Verify the "Cipher Suite" shown in Wireshark is one of the following:
      TLS_RSA_WITH_AES_128_GCM_SHA256,
      TLS_RSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

4. "Application Data" messages are not seen between WInnForum SAS Test Harness and CBSD/DP UUT.

5. CBSD/DP UUT may send a TLS "Alert" message to WInnForum SAS Test Harness notifying of rejecting the TLS connection before attempting to establish the TLS connection again.

Verify that WInnForum SAS Test Harness Command Prompt does not show any Request Message from CBSD/DP UUT

Stop the WInnForum SAS Test Harness before moving to the next test (Close or Exit the WInnForum SAS Test Harness Command Prompt)

6.5 Executing WINNF.FT.C.SCS.5 TLS Failure when Certificate at the SAS Test Harness is Corrupted

Test case [WINNF.FT.C.SCS.5] "TLS failure when certificate at the SAS Test Harness is corrupted" is described in [n.3].

Place in the WInnForum SAS Test Harness the correct SAS Test Harness X.509 certificates for this test case. Edit the conf.xml file appropriately for use of this certificate.

Verify the SAS Test Harness X.509 certificate is the correct X.509 certificate for this test case by inspecting its content as described in the "readme_file_x509_RSA_certs_test_labs.txt" [n.4]. For test case [WINNF.FT.C.SCS.5] the X.509 certificate has

- Invalid Signature as described in the "readme_file_x509_RSA_certs_test_labs.txt" [n.4].

Activate the WInnForum SAS Test Harness using "StartOfProject.py" as described in [n.4].

Verify in Wireshark the following in the captured packets:

1. Wireshark "Protocol" column shows "TLSv1.2"

2. CBSD/DP UUT sends "Client Hello" message to WInnForum SAS Test Harness

3. WInnForum SAS Test Harness sends "Server Hello" message to CBSD/DP UUT.

    - The "Server Hello" message "Handshake Protocol" IE includes the "Cipher Suite" IE.

    - Verify the "Cipher Suite" shown in Wireshark is one of the following:
      TLS_RSA_WITH_AES_128_GCM_SHA256,
      TLS_RSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

4. "Application Data" messages are not seen between WInnForum SAS Test Harness and CBSD/DP UUT.

5. CBSD/DP UUT may send a TLS "Alert" message to WInnForum SAS Test Harness notifying of rejecting the TLS connection before attempting to establish the TLS connection again.

Verify that WInnForum SAS Test Harness Command Prompt does not show any Request Message from CBSD/DP UUT

Stop the WInnForum SAS Test Harness before moving to the next test (Close or Exit the WInnForum SAS Test Harness Command Prompt)