

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

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]

1
2
3
4
5
6
7
8
9
10
11
12
13
14

**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 It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the SSC Work Group 4.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.

Wireless Innovation Forum TM and SDR Forum TM are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

1		
2	TERMS, CONDITIONS & NOTICES.....	i
3	Contributors	iv
4	1 Introduction.....	1
5	2 Scope.....	1
6	3 References.....	1
7	3.1 Normative references	1
8	4 Definitions and abbreviations	1
9	4.1 Abbreviations.....	1
10	4.2 Definitions.....	2
11	5 Prerequisites for CBSB/DP UUT Security Test Cases Execution.....	2
12	5.1 Capturing Packets	3
13	5.1.1 Windows Operating System	3
14	5.1.2 Linux Operating System	3
15	5.2 Wireshark Display of SSL/TLS Packets of WinnForum SAS Test Harness.....	3
16	5.3 Wireshark Display of Time Synchronization in Captured Packets	4
17	5.4 Wireshark Display of WinnForum SAS Test Harness Packets	4
18	6 Executing the CBSB/DP UUT Security Test Cases	4
19	6.1 Executing WINNF.FT.C.SCS.1 Successful TLS connection between UUT and SAS	
20	Test Harness.....	4
21	6.2 Executing WINNF.FT.C.SCS.2 TLS Failure due to Revoked Certificate	6
22	6.3 Executing WINNF.FT.C.SCS.3 TLS Failure due to Expired Server Certificate	10
23	6.4 Executing WINNF.FT.C.SCS.4 TLS Failure when SAS Test Harness Certificate is	
24	issued by an Unknown CA.....	11
25	6.5 Executing WINNF.FT.C.SCS.5 TLS Failure when Certificate at the SAS Test Harness	
26	is Corrupted.....	12
27		

1

List of Figures

2	Figure 1: Wireshark “TCP Port 5000 Decode as SSL”	3
3	Figure 2: Wireshark UTC Display	4
4	Figure 3: Wireshark Capture Example for Test [WINNF.FT.C.SCS.1].....	6
5	Figure 4: Wireshark Capture Example Test [WINNF.FT.C.SCS.2] – DNS Resolution of CRL	
6	Server Followed by CRL File Retrieval	8
7	Figure 5: Wireshark Capture Example for Test [WINNF.FT.C.SCS.2] - DNS Resolution of	
8	OCSP Server Followed by OCSP Request	9
9	Figure 6: Proposed Test Lab Setup for Test [WINNF.FT.C.SCS.2]	9

10

List of Tables

11 No table of figures entries found.

1

Contributors

2 The following individuals made significant contributions to this document:

3 Idan Raz (Airspan)

4

1 WinnForum CBSD/DP UUT Security Test Cases Tutorial

2 1 Introduction

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

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

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

11 2 Scope

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

14 3 References

15 3.1 Normative references

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

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

19 [n.2] WINNF-TS-0022 Version V1.1.2, “Winnforum CBRS Certificate Policy Specification”,
20 6 February 2018

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

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

25 4 Definitions and abbreviations

26 4.1 Abbreviations

27 CBSD Citizens Broadband Radio Service Device

28 CBRS Citizens Broadband Radio Service

29 CFR Code of Federal Regulation

30 CPI Certified Professional Installer

31 DP Domain Proxy

32 HTTP Hypertext Transfer Protocol

1	HTTPS	HTTP over TLS
2	JSON	JavaScript Object Notation
3	SAS	Spectrum Access System
4	TLS	Transport Layer Security

5

6 **4.2 Definitions**

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

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

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

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

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

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

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

28 **5 Prerequisites for CBSD/DP UUT Security Test Cases Execution**

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

1 **5.1 Capturing Packets**

2 *5.1.1 Windows Operating System*

3 5.1.1.1 The WinPcap is installed as part of the Wireshark installation

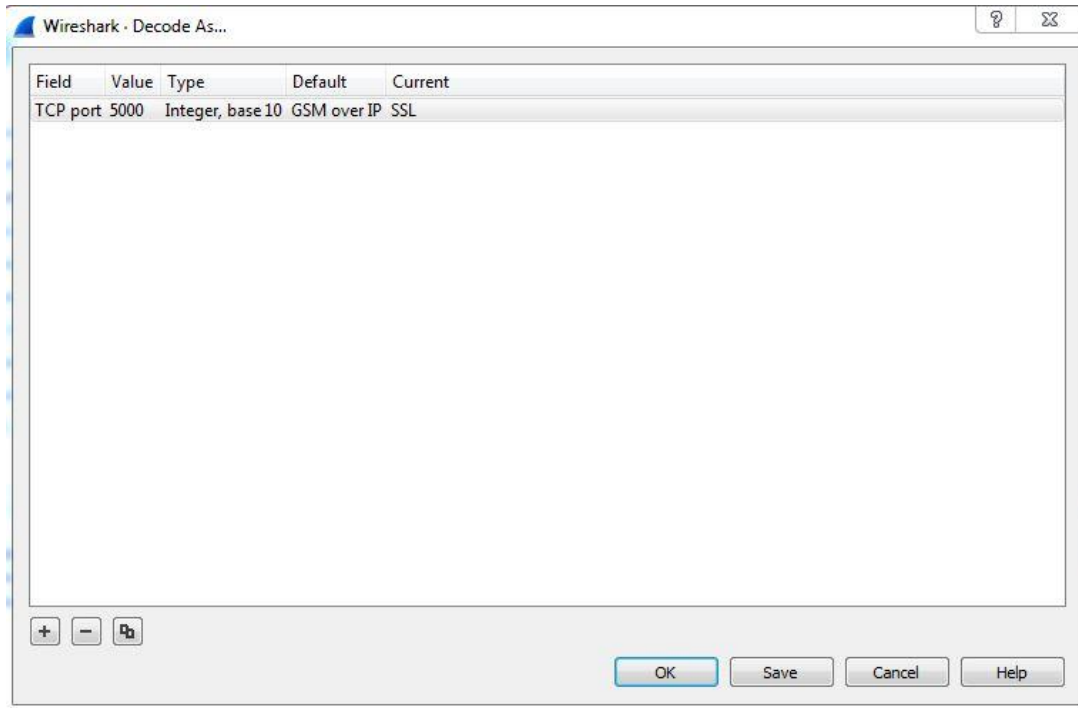
4 *5.1.2 Linux Operating System*

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

7 **5.2 Wireshark Display of SSL/TLS Packets of WinnForum SAS Test Harness**

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

- 11 1. Write the port number appearing in the conf.xml file of the SAS Test Harness (default
12 value appearing is 5000).
- 13 2. In Wireshark go to Analyze → “Decode As” menu. Add “TCP Port 5000” to be decoded
14 as SSL. (The port number is according to the conf.xml file. 5000 is the default value).
- 15 3. Press “Save” and “OK”.



16

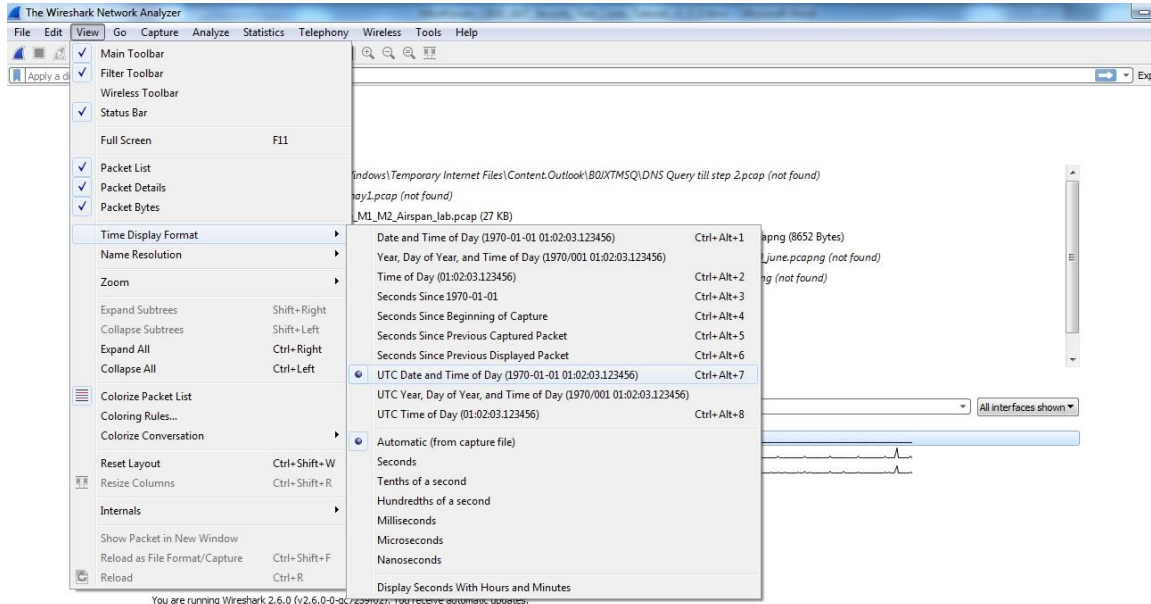
17

Figure 1: Wireshark “TCP Port 5000 Decode as SSL”

18

1 **5.3 Wireshark Display of Time Synchronization in Captured Packets**

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



4
 5 **Figure 2: Wireshark UTC Display**

6 **5.4 Wireshark Display of WinnForum SAS Test Harness Packets**

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

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

11 **6 Executing the CBS/DP UUT Security Test Cases**

12 **6.1 Executing WINNF.FT.C.SCS.1 Successful TLS connection between UUT and SAS Test
 13 Harness**

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

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

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

- 1 Activate the WinnForum SAS Test Harness using “StartOfProject.py” as described in [n.4].
- 2 Verify in Wireshark the following in the captured packets:
 - 3 1. Wireshark “Protocol” column shows “TLSv1.2”
 - 4 2. CBSD/DP UUT sends “Client Hello” message to WinnForum SAS Test Harness
 - 5 3. WinnForum SAS Test Harness sends “Server Hello” message to CBSD/DP UUT.
 - 6 • The “Server Hello” message “Handshake Protocol” IE includes the “Cipher
 - 7 Suite” IE.
 - 8 • Verify the “Cipher Suite” shown in Wireshark is one of the following:
 - 9 TLS_RSA_WITH_AES_128_GCM_SHA256,
 - 10 TLS_RSA_WITH_AES_256_GCM_SHA384,
 - 11 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
 - 12 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
 - 13 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - 14 4. “Application Data” messages are exchanged between WinnForum SAS Test Harness and
 - 15 CBSD/DP UUT.
- 16 Verify that WinnForum SAS Test Harness Command Prompt shows Registration Request
- 17 Message from CBSD/DP UUT
- 18 Stop the WinnForum SAS Test Harness before moving to the next test (Close or Exit the
- 19 WinnForum SAS Test Harness Command Prompt)
- 20
- 21

CBSD UUT Security Test Cases Tutorial

The image shows a Wireshark capture of a TLS handshake. The packet list pane shows 11 packets. Packet 5 (1654 bytes) is the Server Hello, Certificate, Certificate Request, Server Hello Done. Packet 6 (1362 bytes) is the Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message. Packet 7 (235 bytes) is the Application Data. Packet 8 (108 bytes) is the Application Data. Packet 9 (234 bytes) is the Application Data.

No.	Time	Source	Destination	Protocol	Length	Info
4	2018-01-29 10:33:42.038115	90.0.0.113	90.0.0.114	TLSv1.2	205	Client Hello
5	2018-01-29 10:33:42.038630	90.0.0.114	90.0.0.113	TLSv1.2	1654	Server Hello, Certificate, Certificate Request, Server Hello Done
6	2018-01-29 10:33:42.045418	90.0.0.113	90.0.0.114	TLSv1.2	1362	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
7	2018-01-29 10:33:42.059609	90.0.0.114	90.0.0.113	TLSv1.2	235	Application Data
8	2018-01-29 10:33:42.076783	90.0.0.113	90.0.0.114	TLSv1.2	108	Application Data
9	2018-01-29 10:33:42.077142	90.0.0.114	90.0.0.113	TLSv1.2	234	Application Data
10	2018-01-29 10:33:42.077142	90.0.0.114	90.0.0.113	TLSv1.2	108	Application Data
11	2018-01-29 10:33:42.077648	90.0.0.113	90.0.0.114	TLSv1.2	234	Application Data

Frame 5: 1654 bytes on wire (13232 bits), 1654 bytes captured (13232 bits) on interface 0
Ethernet II, Src: IntelCor_9d:4c:fd (00:1b:21:9d:4c:fd), Dst: IntelCor_04:df:be (00:1b:21:04:df:be)
Internet Protocol Version 4, Src: 90.0.0.114, Dst: 90.0.0.113
Transmission Control Protocol, Src Port: 5000, Dst Port: 62001, Seq: 1, Ack: 152, Len: 1600
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 81
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 77
Version: TLS 1.2 (0x0303)
Random
Session ID Length: 32
Session ID: aa426ed73123d44714106e09587d683e6f9dda05c07273cd...
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

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].

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

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

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

6 Verify in Wireshark the following in the captured packets:

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

8 2. CBS/D/DP UUT sends “Client Hello” message to WinnForum SAS Test Harness

9 3. WinnForum SAS Test Harness sends “Server Hello” message to CBS/D/DP UUT.

10 • The “Server Hello” message “Handshake Protocol” IE includes the “Cipher
11 Suite” IE.

12 • Verify the “Cipher Suite” shown in Wireshark is one of the following:
13 TLS_RSA_WITH_AES_128_GCM_SHA256,
14 TLS_RSA_WITH_AES_256_GCM_SHA384,
15 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
16 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
17 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

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

21 5. CBS/D/DP UUT:

22 • Download the CRL file according to the full URI listed in X.509v3 extension of
23 “CRL Distribution Points” described above.

24 OR

25 • Send to the OCSP server an OCSP “Request” message containing the certificate
26 serial number, and OCSP server replies.

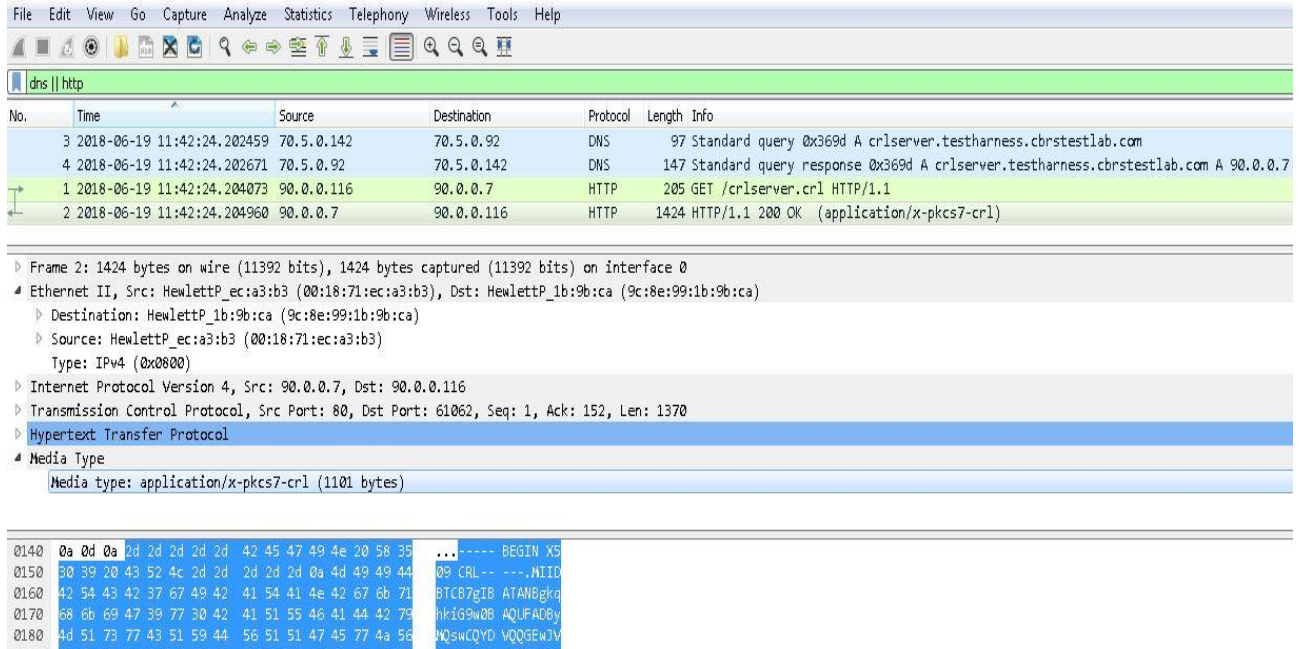
27 OR

28 • Both CRL file download and OCSP transaction as described above.

29 6. “Application Data” messages are not seen between WinnForum SAS Test Harness and
30 CBS/D/DP UUT.

CBSD UUT Security Test Cases Tutorial

- 1 7. CBS/D/DP UUT may send a TLS “Alert” message to WinnForum SAS Test Harness
- 2 notifying of rejecting the TLS connection before attempting to establish the TLS
- 3 connection again.
- 4 Verify that WinnForum SAS Test Harness Command Prompt does not show any Request
- 5 Message from CBS/D/DP UUT
- 6 Stop the WinnForum SAS Test Harness before moving to the next test (Close or Exit the
- 7 WinnForum SAS Test Harness Command Prompt)



8
9 **Figure 4: Wireshark Capture Example Test [WINNF.FT.C.SCS.2] – DNS Resolution of CRL Server**
10 **Followed by CRL File Retrieval**

CBSD UUT Security Test Cases Tutorial

The image shows a Wireshark capture of network traffic. The top pane shows a list of packets. Packet 4 is selected, showing details for the Online Certificate Status Protocol (OCSP) request. The details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
1	2018-06-19 11:42:24.179491	70.5.0.142	70.5.0.92	DNS	92	Standard query 0x1bda A obsp.testharness.cbrstestlab.com
2	2018-06-19 11:42:24.179705	70.5.0.92	70.5.0.142	DNS	142	Standard query response 0x1bda A obsp.testharness.cbrstestlab.com A 90.0.0.7
4	2018-06-19 11:42:24.193618	90.0.0.116	90.0.0.7	OCSP	130	Request

The details pane for the selected packet (Frame 4) shows the following structure:

- Frame 4: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
- Ethernet II, Src: HewlettP_lb:9b:ca (9c:8e:99:1b:9b:ca), Dst: HewlettP_ec:a3:b3 (00:18:71:ec:a3:b3)
- Internet Protocol Version 4, Src: 90.0.0.116, Dst: 90.0.0.7
- Transmission Control Protocol, Src Port: 61061, Dst Port: 80, Seq: 238, Ack: 1, Len: 76
- [2 Reassembled TCP Segments (313 bytes): #3(237), #4(76)]
- Hypertext Transfer Protocol
- Online Certificate Status Protocol
 - tbsRequest
 - requestList: 1 item
 - Request
 - reqCert
 - hashAlgorithm (SHA-1)
 - issuerNameHash: 5368d21d2529427538588c5ccba4c4e6f3b96641
 - issuerKeyHash: e988b4b76c39cd1b9a301814b62bba156d20aa95
 - serialNumber: 10177691706620776705

1

2

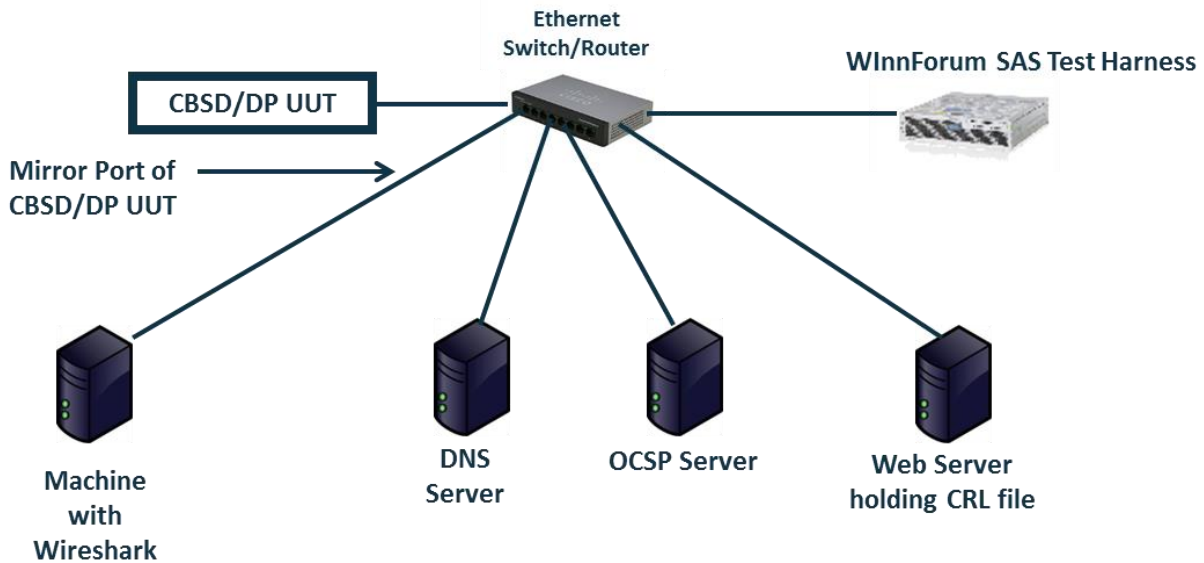
3

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

4

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.

5



6

7

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

8

9

1 **6.3 Executing WINNF.FT.C.SCS.3 TLS Failure due to Expired Server Certificate**

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

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

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

- 9
 - 10 • Expired Validity time. The date appearing in the “Not After” parameter of the X.509
certificate has passed.

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

12 Verify in Wireshark the following in the captured packets:

- 13 1. Wireshark “Protocol” column shows “TLSv1.2”
- 14 2. CBS/D/DP UUT sends “Client Hello” message to WinnForum SAS Test Harness
- 15 3. WinnForum SAS Test Harness sends “Server Hello” message to CBS/D/DP UUT.
- 16
 - 17 • The “Server Hello” message “Handshake Protocol” IE includes the “Cipher
Suite” IE.
 - 18 • Verify the “Cipher Suite” shown in Wireshark is one of the following:
19 TLS_RSA_WITH_AES_128_GCM_SHA256,
20 TLS_RSA_WITH_AES_256_GCM_SHA384,
21 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
22 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
23 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 24 4. “Application Data” messages are not seen between WinnForum SAS Test Harness and
25 CBS/D/DP UUT.
- 26 5. CBS/D/DP UUT may send a TLS “Alert” message to WinnForum SAS Test Harness
27 notifying of rejecting the TLS connection before attempting to establish the TLS
28 connection again.

29 Verify that WinnForum SAS Test Harness Command Prompt does not show any Request
30 Message from CBS/D/DP UUT

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

1 **6.4 Executing WINNF.FT.C.SCS.4 TLS Failure when SAS Test Harness Certificate is**
2 **issued by an Unknown CA**

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

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

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

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

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

13 Verify in Wireshark the following in the captured packets:

- 14 1. Wireshark “Protocol” column shows “TLSv1.2”
15 2. CBSDDP UUT sends “Client Hello” message to WinnForum SAS Test Harness
16 3. WinnForum SAS Test Harness sends “Server Hello” message to CBSDDP UUT.
17 • The “Server Hello” message “Handshake Protocol” IE includes the “Cipher
18 Suite” IE.
19 • Verify the “Cipher Suite” shown in Wireshark is one of the following:
20 TLS_RSA_WITH_AES_128_GCM_SHA256,
21 TLS_RSA_WITH_AES_256_GCM_SHA384,
22 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
23 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
24 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
25 4. “Application Data” messages are not seen between WinnForum SAS Test Harness and
26 CBSDDP UUT.
27 5. CBSDDP UUT may send a TLS “Alert” message to WinnForum SAS Test Harness
28 notifying of rejecting the TLS connection before attempting to establish the TLS
29 connection again.

30 Verify that WinnForum SAS Test Harness Command Prompt does not show any Request
31 Message from CBSDDP UUT

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

1 **6.5 Executing WINNF.FT.C.SCS.5 TLS Failure when Certificate at the SAS Test**
2 **Harness is Corrupted**

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

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

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

- 10 • Invalid Signature as described in the “readme_file_x509_RSA_certs_test_labs.txt” [n.4].

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

12 Verify in Wireshark the following in the captured packets:

- 13 1. Wireshark “Protocol” column shows “TLSv1.2”
- 14 2. CBS/D/DP UUT sends “Client Hello” message to WinnForum SAS Test Harness
- 15 3. WinnForum SAS Test Harness sends “Server Hello” message to CBS/D/DP UUT.
 - 16 • The “Server Hello” message “Handshake Protocol” IE includes the “Cipher
17 Suite” IE.
 - 18 • Verify the “Cipher Suite” shown in Wireshark is one of the following:
19 TLS_RSA_WITH_AES_128_GCM_SHA256,
20 TLS_RSA_WITH_AES_256_GCM_SHA384,
21 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
22 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
23 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 24 4. “Application Data” messages are not seen between WinnForum SAS Test Harness and
25 CBS/D/DP UUT.
- 26 5. CBS/D/DP UUT may send a TLS “Alert” message to WinnForum SAS Test Harness
27 notifying of rejecting the TLS connection before attempting to establish the TLS
28 connection again.

29 Verify that WinnForum SAS Test Harness Command Prompt does not show any Request
30 Message from CBS/D/DP UUT

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