

|  |
| --- |
| CCSDS NETWORK LAYER SECURITY ADAPTATION PROFILE Test |

DRAFT CCSDS Record

CCSDS 356.1-Y-1

Yellow Book

March 2016

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This document is therefore subject to CCSDS document management and change control procedures, which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

<http://www.ccsds.org/>

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of this publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

* Agenzia Spaziale Italiana (ASI)/Italy.
* British National Space Centre (BNSC)/United Kingdom.
* Canadian Space Agency (CSA)/Canada.
* Centre National d’Etudes Spatiales (CNES)/France.
* China National Space Administration (CNSA)/People’s Republic of China.
* Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
* European Space Agency (ESA)/Europe.
* Federal Space Agency (FSA)/Russian Federation.
* Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
* Japan Aerospace Exploration Agency (JAXA)/Japan.
* National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

* Austrian Space Agency (ASA)/Austria.
* Belgian Federal Science Policy Office (BFSPO)/Belgium.
* Chinese Academy of Sciences (CAS)/China.
* Chinese Academy of Space Technology (CAST)/China.
* China Satellite Launch and Tracking Control General, (CLTC)/China.
* Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
* Departamento De Ciência E Tecnologia Aeroespacial (DCTA)/Brazil.
* Danish National Space Center (DNSC)/Denmark.
* Electronics and Telecommunications Research Institute (ETRI)/Korea
* European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
* European Telecommunications Satellite Organization (EUTELSAT)/Europe.
* Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand
* Hellenic National Space Committee (HNSC)/Greece.
* Institute of Space Research (IKI)/Russian Federation.
* Indian Space Research Organization (ISTRAC)/India.
* Korea Aerospace Research Institute (KARI)/Korea.
* KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary
* Ministry of Communications (MOC)/Israel.
* Naval Center for Space Technology (NCST)/USA.
* National Institute of Information and Communications Technology (NICT)/Japan.
* National Oceanic and Atmospheric Administration (NOAA)/USA.
* National Space Agency of the Republic of Kazakhstan (Kazcosmos) (NSARK)/ Republic of Kazakhstan.
* National Space Organization (NSPO)/ Taiwan.
* South African National Space Agency (SANSA)/ South Africa.
* Swedish Space Corporation (SSC)/Sweden.
* Swiss Space Office (SSO)/Swiss Confederation.
* Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
* Central Research Institute of Machine Building (TsNIIMash)/ Russian Federation.
* The Scientific and Technological Research Council of Turkey (TUBITAK)/ Turkey
* United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | **Title and Issue** | **Date** | **Status** |
| CCSDS 000.1-R-1 | CCSDS NETWORK LAYER SECURITY ADAPTATION PROFILE, Draft CCSDS Record, Issue 1 | August 2013 | Current draft |
|  |  |  |  |
|  |  |  |  |

CONTENTS

Section Page

[DOCUMENT CONTROL 5](#_Toc442251371)

[CONTENTS 6](#_Toc442251372)

[1 Introduction 6](#_Toc442251373)

[2 Overview 8](#_Toc442251380)

[3 Summary of interoperability and comparability testing 8](#_Toc442251381)

[4 Algorithm testing goals 8](#_Toc442251382)

[5 testS details 9](#_Toc442251395)

[6 Compatablit testing between NASA and CNES 13](#_Toc442251420)

[7 Observations: 37](#_Toc442251422)

**Tables Page**

[Table 5‑1: Test items 9](#_Toc444262782)

[Table 5‑2: IPsec Tests 9](#_Toc444262783)

[Table 6-1: Compatibility tests and results 14](#_Toc444262782)

[Figure 6.1 CNES-NASA test setup 14](#_Toc402442592)

# Introduction

## Purpose

The purpose of this document is to describe the compatibility testing conducted for the CCSDS Network Layer Security Adaptation Profile.

## Scope

The scope of this document is the testing results of the Network Layer Security Adaptation Profile which will be implemented and used for CCSDS missions.

## Applicability

This recommendation applies to any CCSDS mission using the Internet Protocol and requiring end-to-end confidentiality, authentication, or integrity from the sender to the receiver regardless of the number of intermediate hops between them.

## Rationale

Many CCSDS missions require security services to protect commanding (command authentication, command confidentiality, command integrity) and payload data (confidentiality, integrity). Missions using the Internet Protocol (IP) may utilize link layer security services such as the Space Data Link Security (SDLS) Protocol (reference [8]) which provides hop-by-hop security between two points (e.g., a ground station and a satellite). If end-to-end security is required, such as between a principal investigator and a payload instrument onboard a spacecraft through intermediary hops, then the IP Security (IPsec) protocol should be used. CCSDS has documented a “profile” of IPsec for use by CCSDS missions. This document discusses interoperability testing of the CCSDS profile.

## Document structure

This document describes the tests, configurations tested and not tested, and test results from the Network Layer Security Adaptation Profile interoperability testing.

## References

The following documents are informative references used to accomplish testing.

1. Internet Engineering Task Force (IETF); Kent, S; Seo, K; Security Architecture for the Internet Protocol; Request for Comments (RFC) 4301; <http://datatracker.ietf.org/doc/rfc4301>; December 2005.
2. IETF; Kent, S; IP Authentication Header; RFC 4302; <http://datatracker.ietf.org/doc/rfc432>; December 2005.
3. IETF; Kent, S; IP Encapsulating Security Payload (ESP); RFC 4303; <http://datatracker.ietf.org/doc/rfc4303>; December 2005.
4. IETF; Kaufman, C; Internet Key Exchange (IKEv2) RFC 4306; <http://datatracker.ietf.org/doc/rfc4306>; December 2005.
5. IETF; Shacham, A; Monsour, B; Pereira, R; Thomas M; IP Payload Compression Protocol (IPComp); Request for Comments (RFC) 3173; <http://datatracker.ietf.org/doc/rfc3173>; September 2001.
6. CCSDS; CCSDS Cryptographic Algorithms; CCSDS 352.0-B-1; Blue Book; Issue 1; November 2012.
7. CCSDS; IP over CCSDS Space Links; CCSDS 702.1-B-1; Blue Book; Issue 1; September 2012.
8. CCSDS; Space Data Link Security Protocol; CCSDS 355.0-B-1; Blue Book; Issue 1; September 2015.

# Overview

Many CCSDS missions require security services such as confidentiality, integrity, and authentication to protect spacecraft commands, software uploads, engineering telemetry, and science payload data.

IPsec consists of two protocols: the Authentication Header (AH) and the Encapsulating Security Payload (ESP). AH provides only authentication and integrity services for the security payload and portions of the IP header. However, AH does not provide confidentiality. ESP, on the other hand, provides confidentiality, integrity, and authentication. The CCSDS Network Layer Security Adaptation Profile supports only ESP.

# Summary of interoperability and compatability testing

IPsec compatibility testing was successful; however, some challenges were encountered which did not allow for a complete testing of all planned parameters. Some of the issues were that some commercial vendors no longer support various IPsec options as specified in the CCSDS Network Layer Security Adaptation Profile. Palo Alto firewall and routers do not support manual keying. In addition, institutional security policies would not allow some modes to be tested, Centre National d’Etudes Spatiales (CNES) firewall policy restrictions also do not support IP Compression. Also due to the firewall restrictions non-tunnel modes required a null hash which made it a tunnel. IP compression is being removed from future IETF Transport Layer Security RFC’s.

Connectivity between National Aeronautics and Space Administration (NASA) and CNES was successfully established.

# Algorithm testing goals

## General

This profile adopts RFC 4301 and RFC 4303 except as specified in 4.2 through 4.12, below.

## Supported protocols

## For CCSDS mission implementations, IPsec shall support only ESP.

## ESP mode

## For CCSDS mission implementations, IPsec shall support only tunnel mode.

## ESP authenticated encryption service

For CCSDS mission implementations, IPsec shall support confidentiality and integrity security service (authenticated encryption).

## ESP Integrity service

For CCSDS mission implementations, IPsec shall support an integrity-only service.

## ESP non-authenticated encryption

For CCSDS mission implementations, only authenticated encryption shall be used.

## ESP manual key management

For CCSDS mission implementations, IPsec shall support manual key management.

## ESP Automatic key management

For CCSDS mission implementations, IPsec shall support automated key management as described in RFC 4306 with an extension to inhibit rekey or to rekey only upon command.

NOTE: this extension is required to ensure that a rekey does not occur during a critical phase of the mission potentially resulting in a system lockout or loss of mission.

## ESP cipher suite

For CCSDS mission implementations, IPsec shall employ the algorithms described in the CCSDS Cryptographic Algorithms recommendations.

# testS details

The testing between CNES and NASA end-points was carried out over the Internet. NASA Glenn Research utilized a facility outside the NASAs firewall to ease connectivity and provide flexibility in testing various options. CNES’s efforts were complicated because they had no external access. For security reasons, they had to work within the CNES firewall and its policies. This was further complicated by a change in the CNES firewall, equipment, software and support contracts which dramatically affected their network configurations. These changes impacted the types of traffic, allowable methods and encryption keying.

Table 5‑1: Test items

|  |  |
| --- | --- |
| NASA: | CNES: |
| Cisco 3825 router IOS 15.01 | Palo Alto 5000 router PAN OS 6.0 |
| Netgear hub | Endpoint: Windows laptop |
| Endpoint: ThinkPadG41: Ubuntu v12 | Monitoring Software WireShark v1.12.6 |
| Monitoring Software WireShark v1.12.6 | Putty |

Table 1 Equipment and software utilized during testing.

Table 5‑2: IPsec Tests

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IPV4 Test #** | **ESP** | **Tunnel** | **Integrity** | **Authenticated Encryption** | **Confidentiality** | **Manual Key** | **Auto Key** | **No Rekey** | **NASA** | **CNES** |
| 1 | X | X | X | X |  | X |  |  | Pass | Fail |
| 2 | X | X | X |  | X | X |  |  | Pass | Fail |
| 3 | X | X | X |  |  |  | X | X | Pass | Pass |
| 4 | X | X | X |  | X |  | X | X | Pass | Pass |



Table 5-2 synopsizes the IPsec modes performed and results from local testing.

CNES Palo Alto firewall and routers do not support manual keying. CNES firewall policy restrictions also do not support IP Compression. IP compression is being removed from future IETF TLS RFC’s.

## IPV4 Authenticated Manual Key #1

### Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using authentication and manual keying. Endpoint one will encrypt data using a 128-bit test key. The resultant cipher data will be sent to a second endpoint recipient via a network connection. The recipient will use the same 128-bit test key to decrypt the cipher text.

Pre shared IPV4 addresses of firewalls and end points not provided in this document.

Pre shared Keying: 128-Bit Key: 000102030405060708090a0b0c0d0e0f

### Expected Results

Encryption/decrypted numbers match or off by one and tunnel established the test is successful.

## IPV4 Confidentiality Manual Key #3

### Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using confidentiality and manual keying. Endpoint one will encrypt data using a 128-bit test key. The resultant cipher data will be sent to a second endpoint recipient via a network connection. The recipient will use the same 128-bit test key to decrypt the cipher text.

Pre shared IPV4 addresses of firewalls and endpoints not provided in this document.

Pre shared Keying: 128-Bit Key: 000102030405060708090a0b0c0d0e0f

### Expected Results

Encryption/decrypted numbers match or off by one and tunnel established the test is successful.

## IPV4 Authenticated Automatic Keying #5

### Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using authentication and automatic keying with no rekeying. Endpoints will use a certificate server to acquire the same 128-bit public key and then negotiate the private key.

Pre shared IPV4 addresses of firewalls and endpoints not provided in this document.

128-Bit Key: 000102030405060708090a0b0c0d0e0f

### Expected Results

The resultant encryption/decrypted logs match, the test is successful.

## IPV4 Confidentiality Automatic Keying #7

### Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using authentication and automatic keying with no re-keying. Endpoints will use a certificate server to acquire the same 128-bit public key and then negotiate the private key.

Pre shared IPV4 addresses of firewalls and endpoints not provided in this document.

Pre shared Keying: 128-Bit Key: 000102030405060708090a0b0c0d0e0f

### Expected Results

If the resultant encryption/decrypted logs match, the test is successful.

# Compatablity testing between NASA and CNES

Compatibility testing is used to measure how well software applications or hardware devices function in concert with relevant hardware, software, operating systems or network environments.



Figure 6.1 CNES-NASA test setup

CNES and NASA agreed to only test the IPV4 configurations. Appropriate documentation was exchanged between CNES and NASA in order to configure the path and encrypt the tunnel.

Table 6‑1: Compatibility tests and results

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IPV4 Test #** | **ESP** | **Tunnel** | **Integrity** | **Authenticated Encryption** | **Confidentiality** | **Manual Key** | **Auto Key** | **No Rekey** | **Interoperability Test** |
| 1 | X | X | X | X |  | X |  |  | Fail |
| 2 | X | X | X |  | X | X |  |  | Fail |
| 3 | X | X | X | X |  |  | X | X | Pass |
| 4 | X | X | X |  | X |  | X | X | Pass |



Table 6.1 is the summary of the IPsec tests modes performed and results from compatibility testing between CNES and NASA.

## IPV4 Compatibility test results

The following are the log validating the tests conducted.

|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Network Layer Security Adaptation Profile |
| 3. | Test Case: | 1, Authenticated Manual Key |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: | Okechukwu Mezu |
| 9. | Results (Pass, Partial Pass, Fail): | Fail |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: | CNES manual keying not supported. |

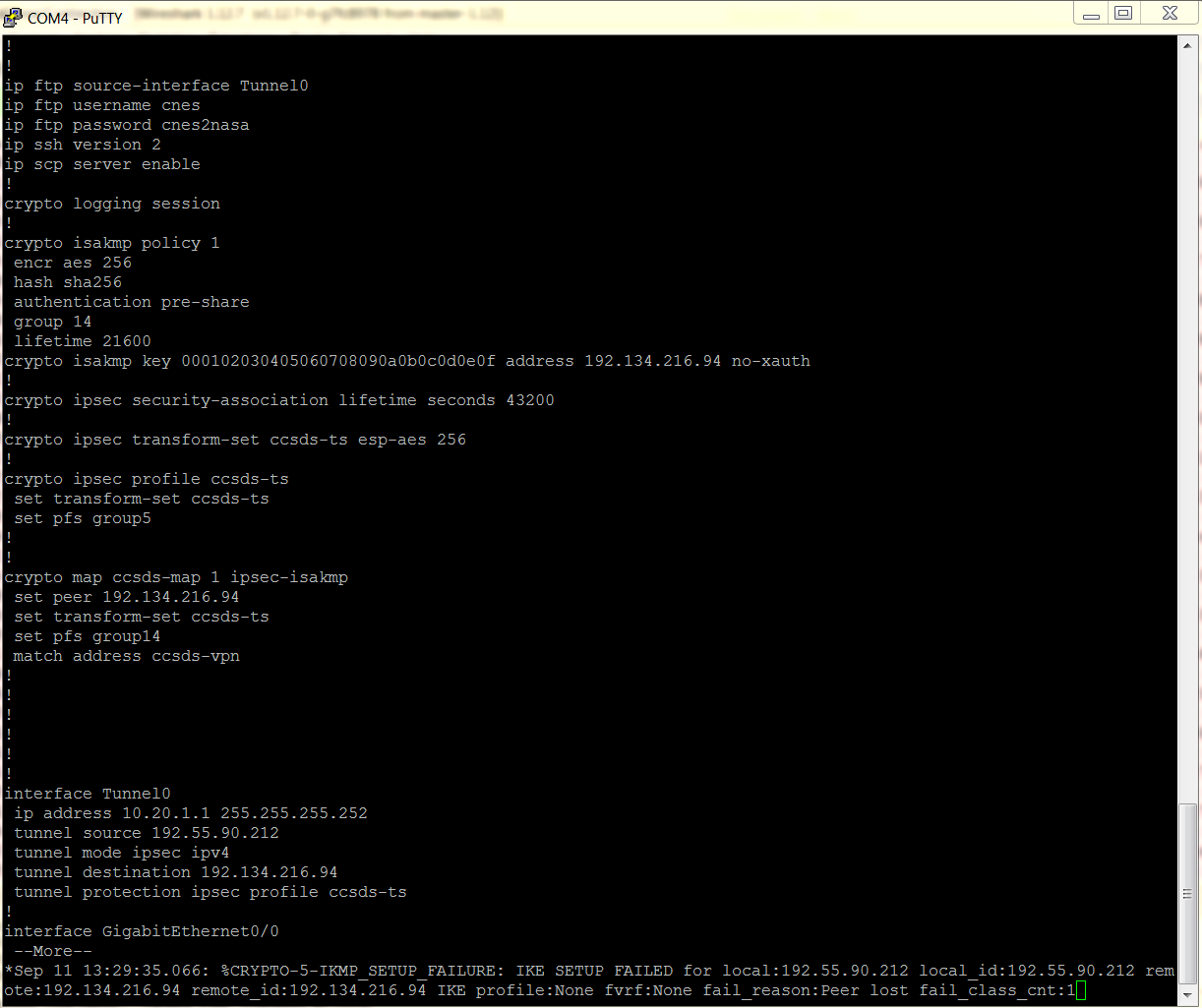
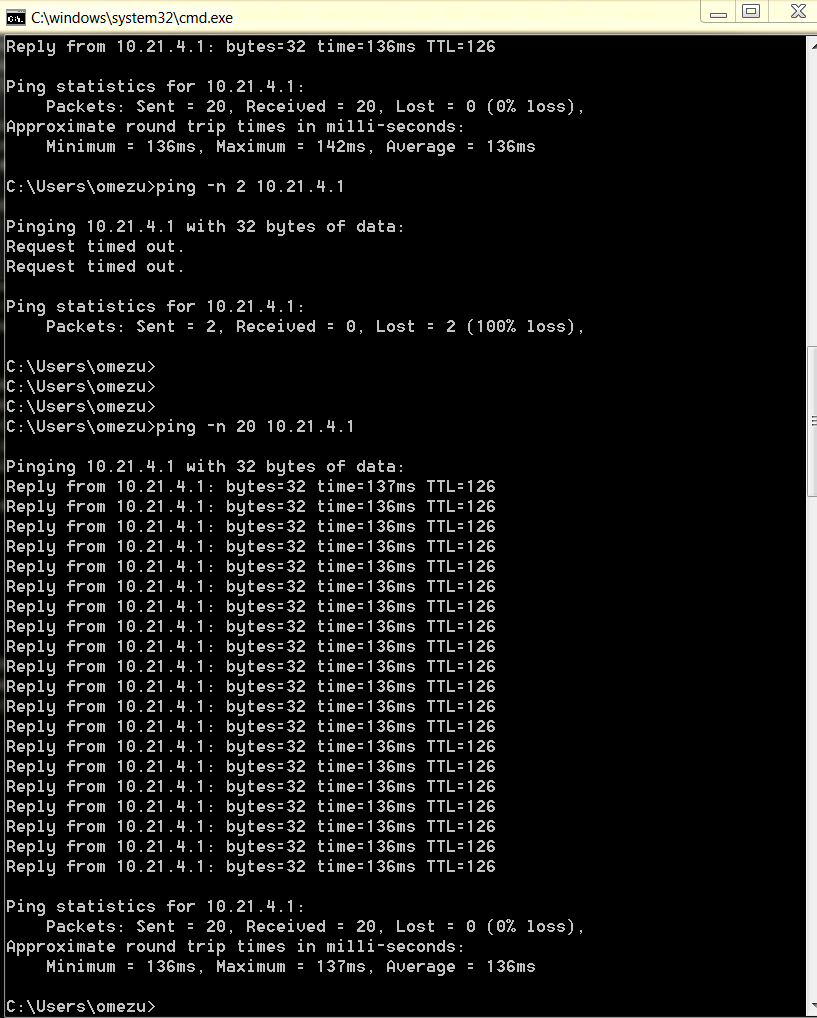
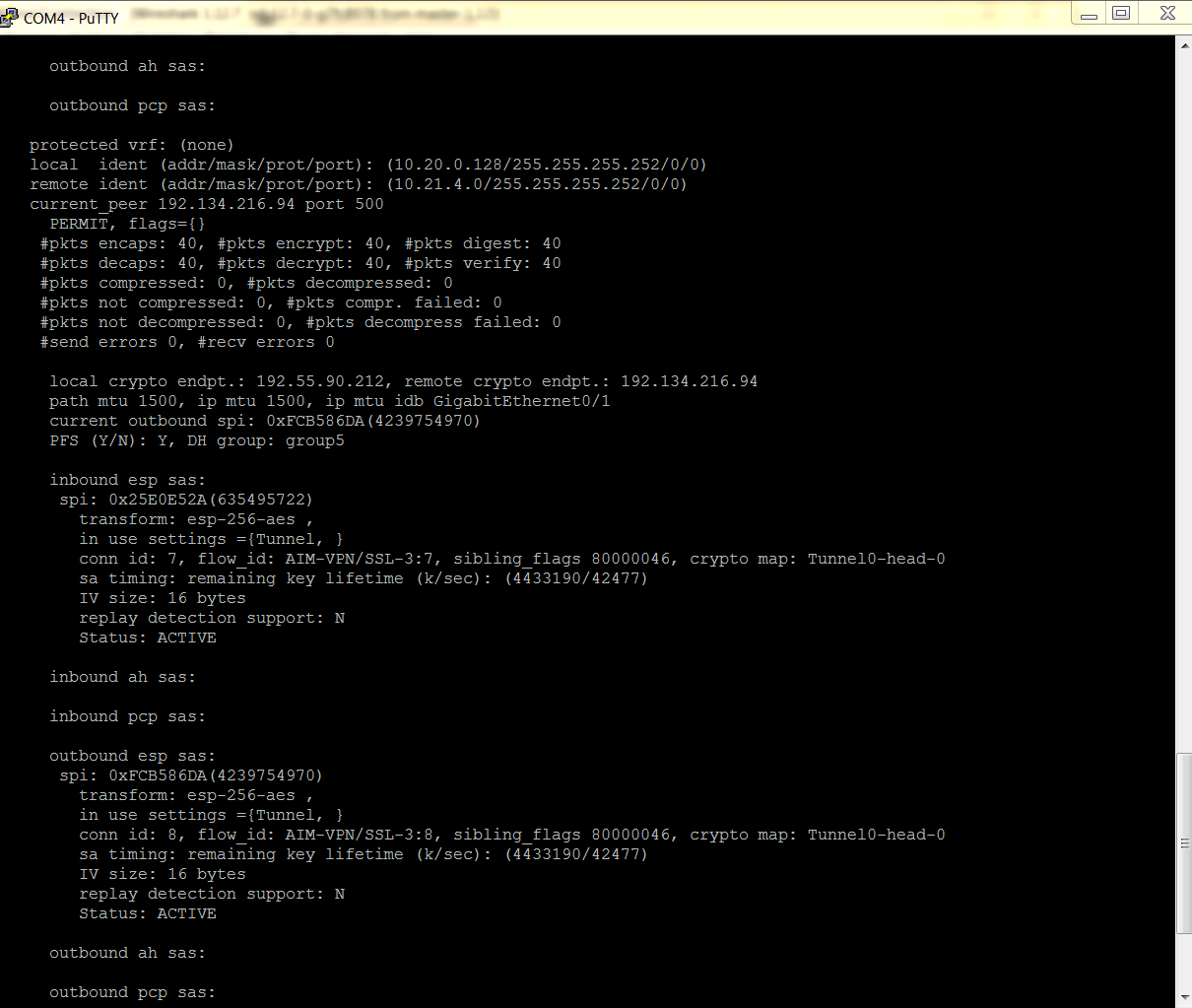
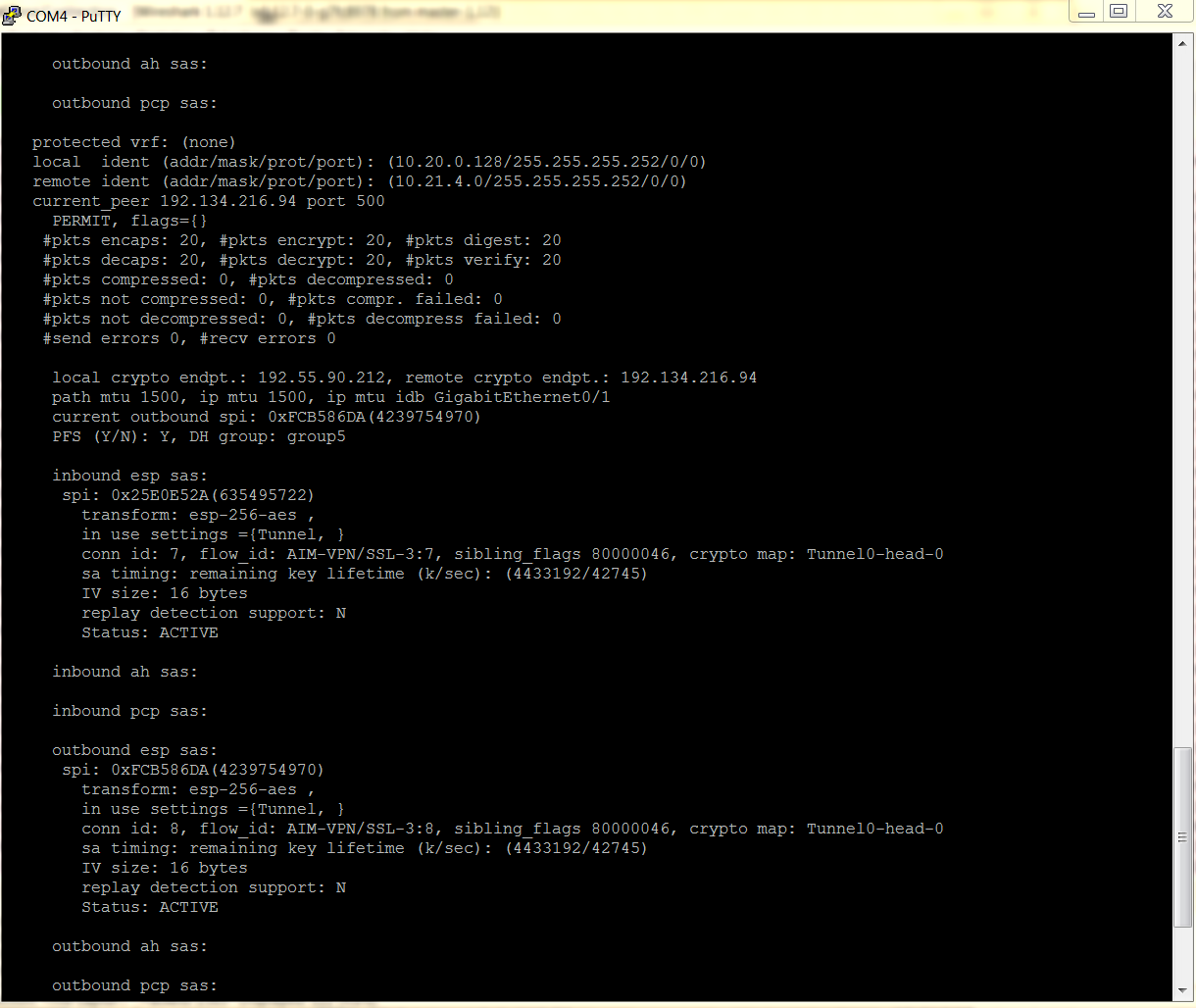
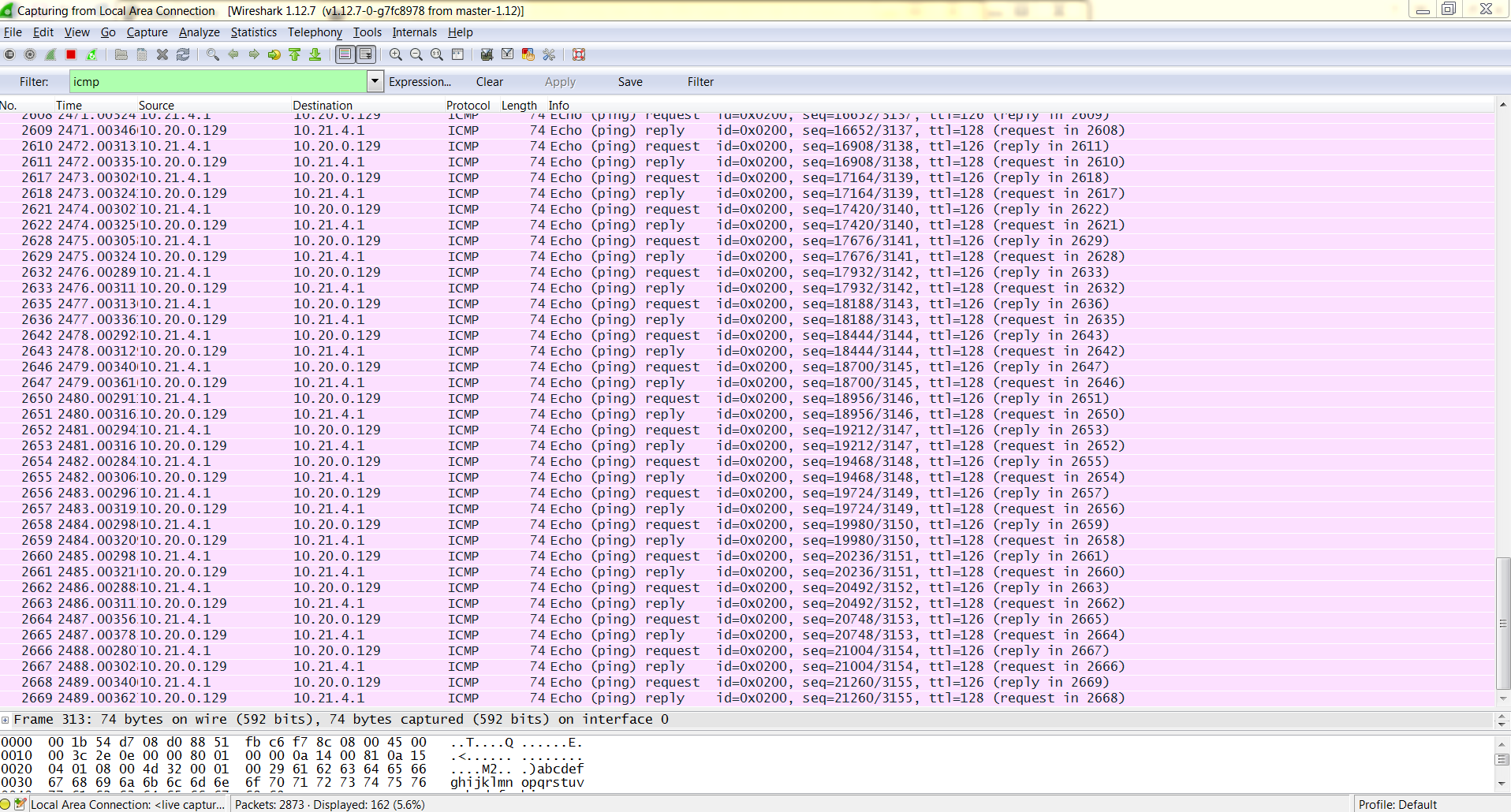
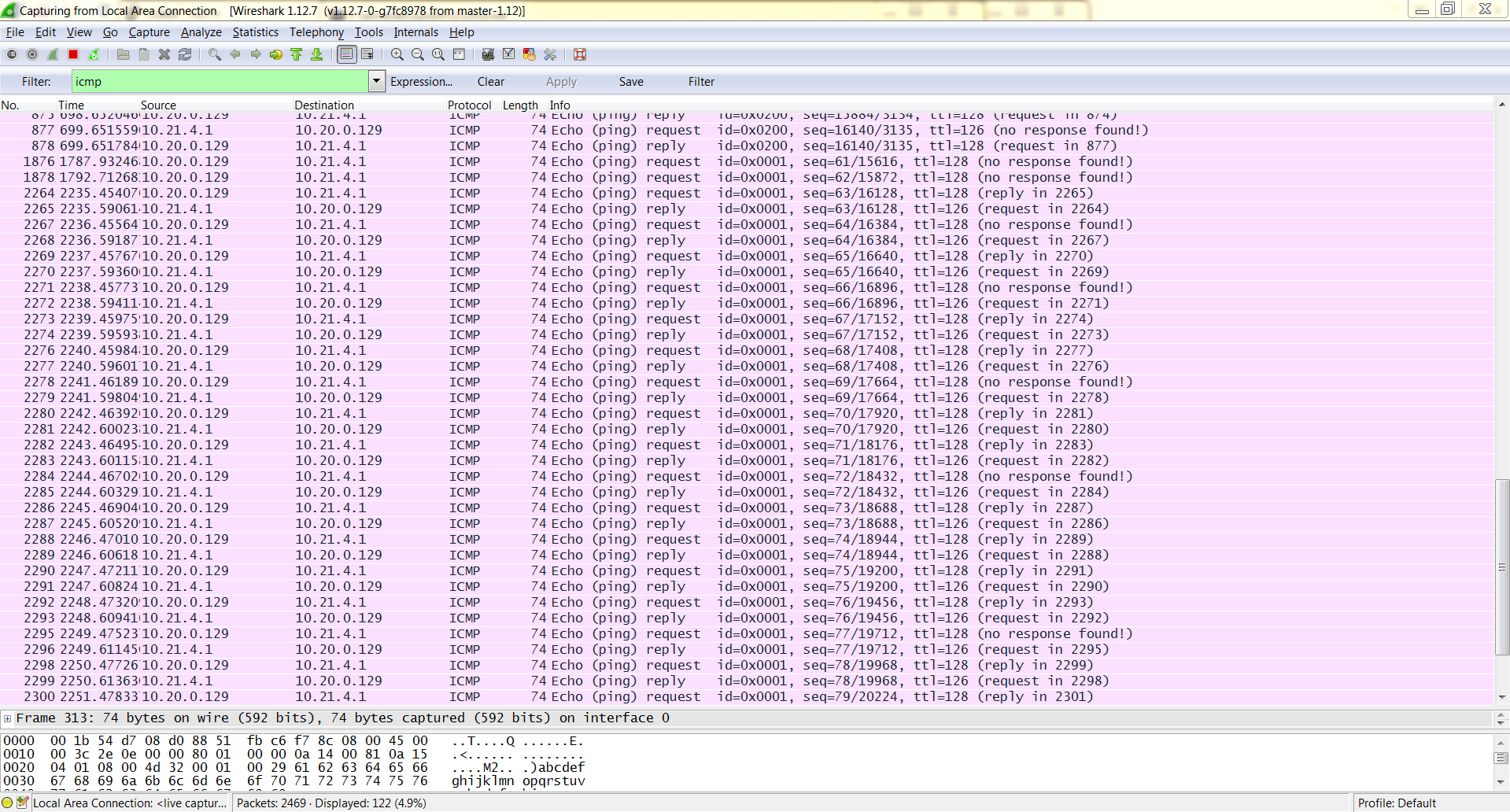
No logs from testing:



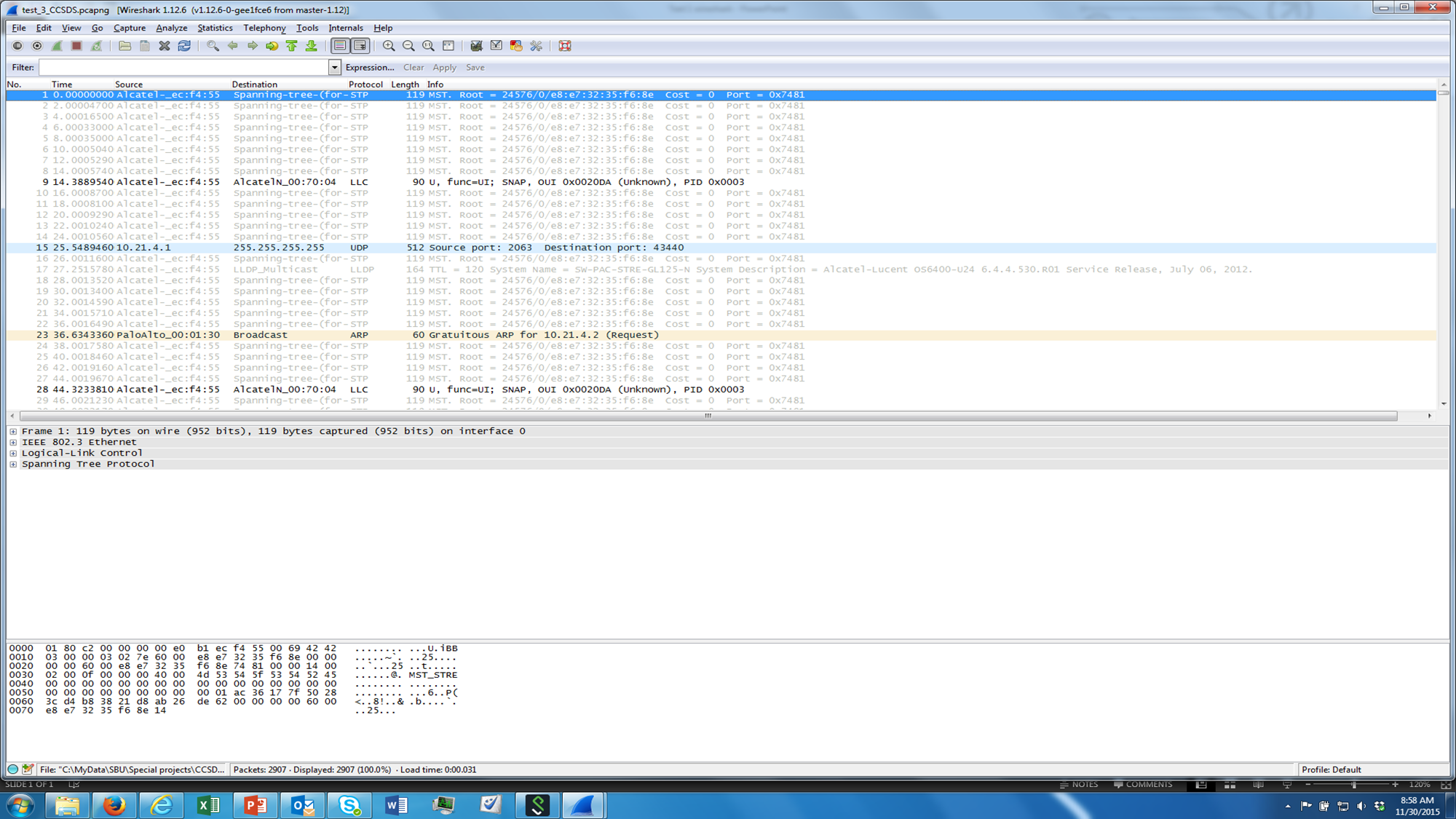
|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Network Layer Security Adaptation Profile |
| 3. | Test Case: | 3, Confidentiality Manual Key |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: | Okechukwu Mezu |
| 9. | Results (Pass, Partial Pass, Fail): | Fail |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: | CNES manual keying not supported. |

No Logs from testing:

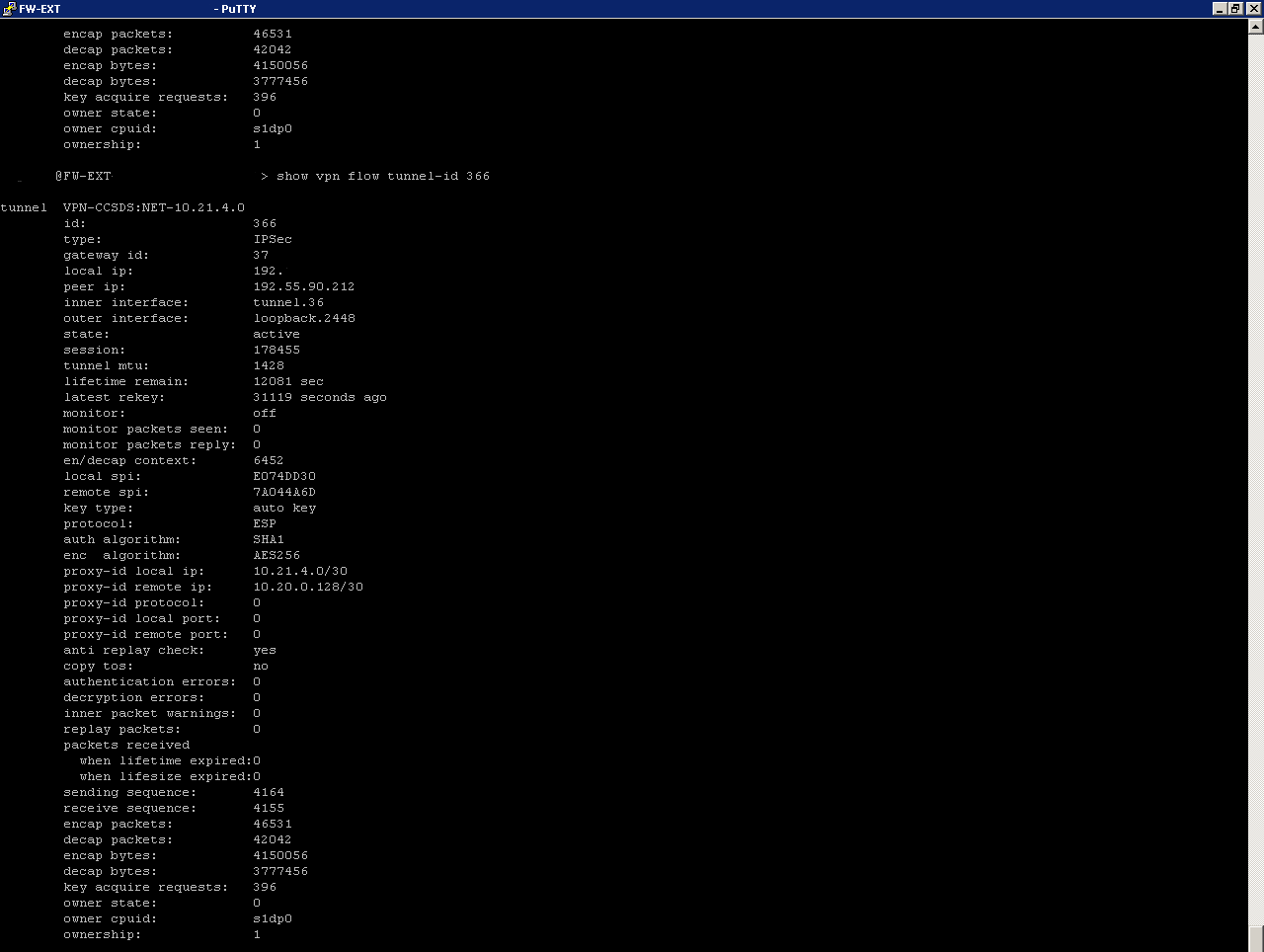
|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Network Layer Security Adaptation Profile |
| 3. | Test Case: | 5, Authenticated Automatic Keying |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: | Okechukwu Mezu |
| 9. | Results (Pass, Partial Pass, Fail): | Partial Pass |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: | CNES firewall policy restrictions, Phase one tunnel requires HASH, entered null HASH |

The following are the log validating the test conducted: NASA:

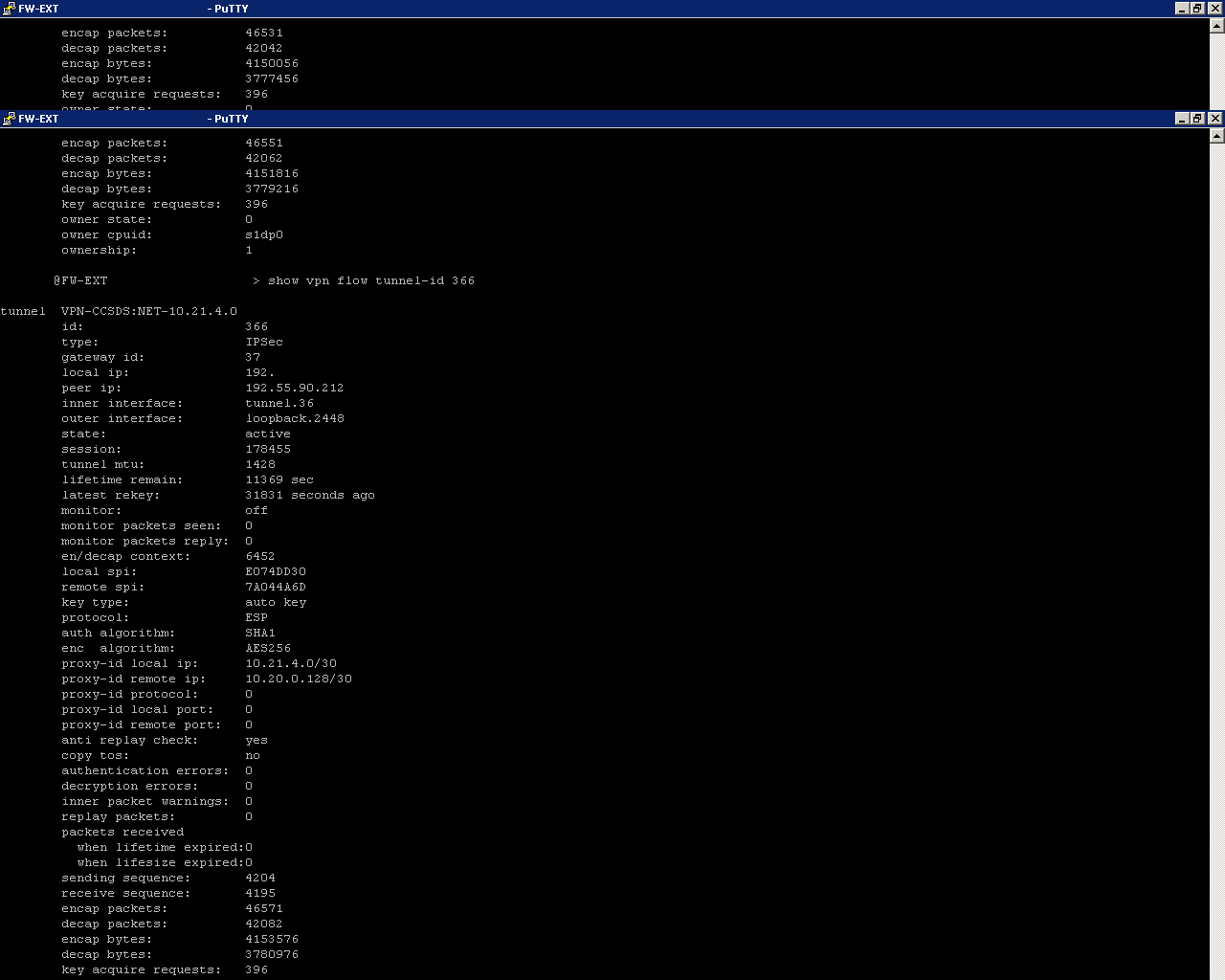
CNES:



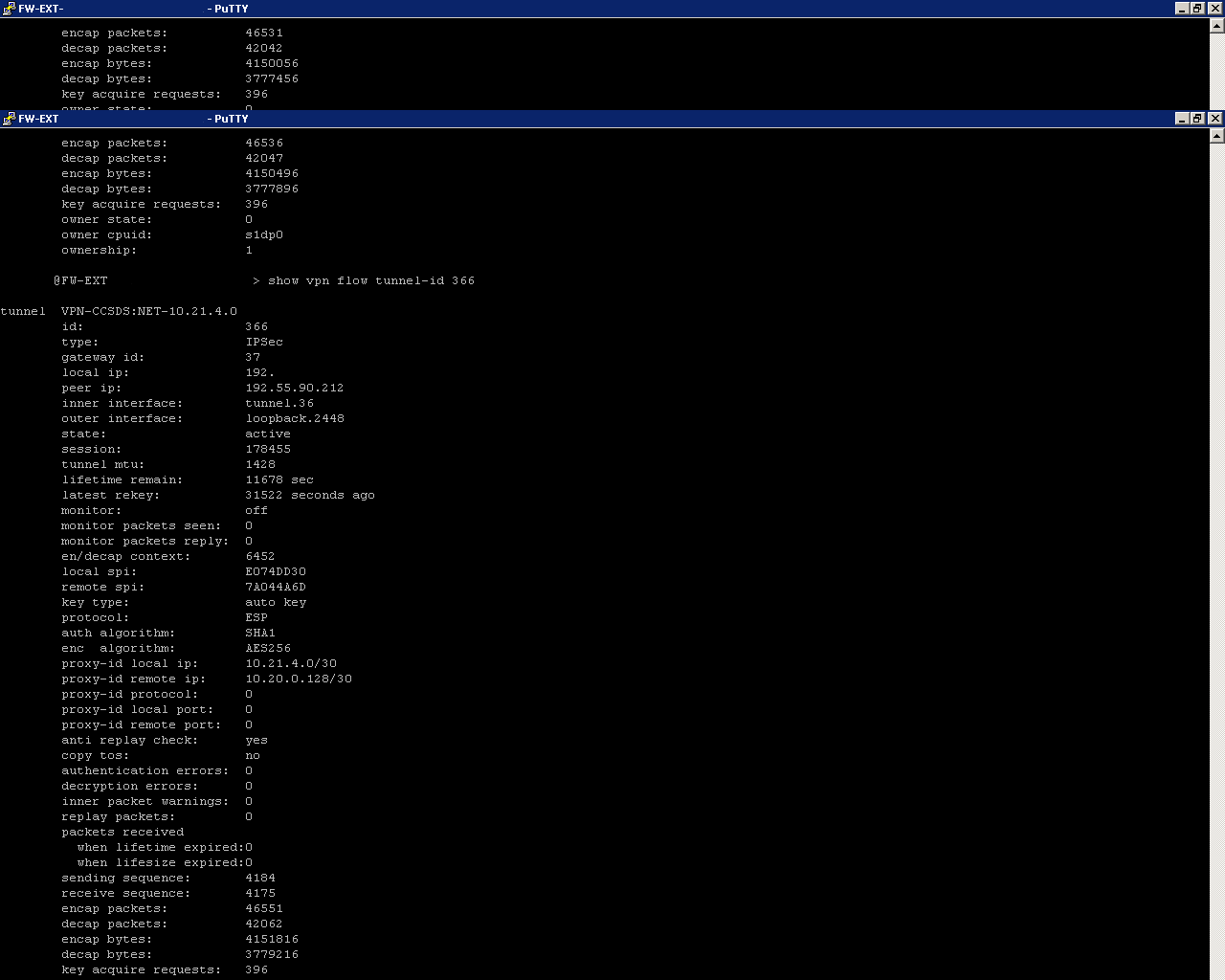
Bytes and Packets counters before traffic:



Bytes and Packets counters after ping from CNES:



Bytes and Packets counters after ping from NASA:

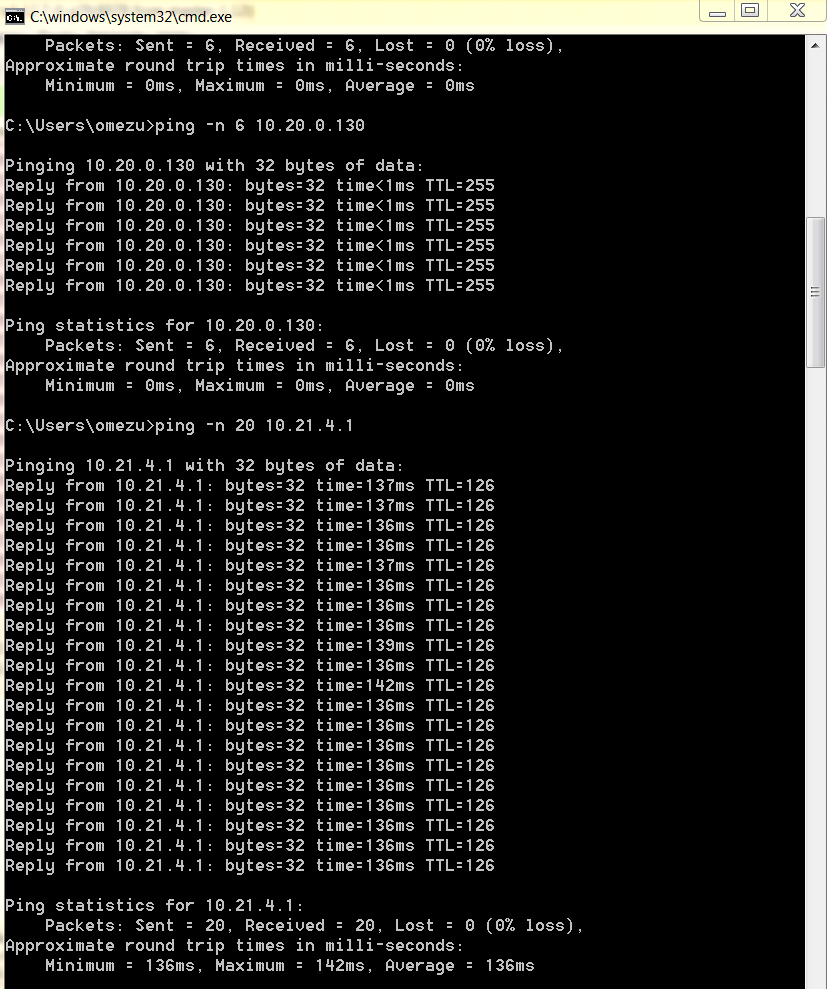
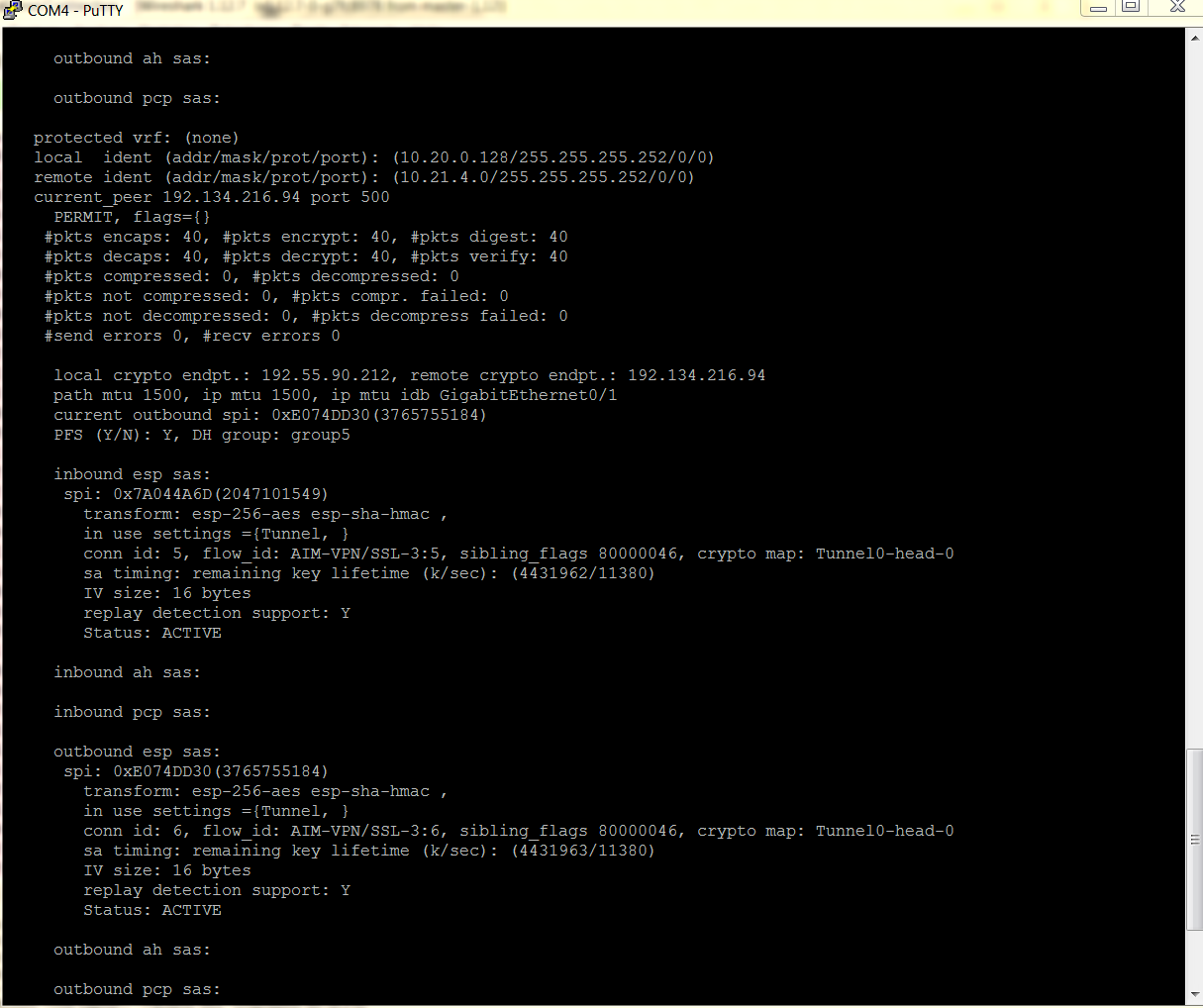
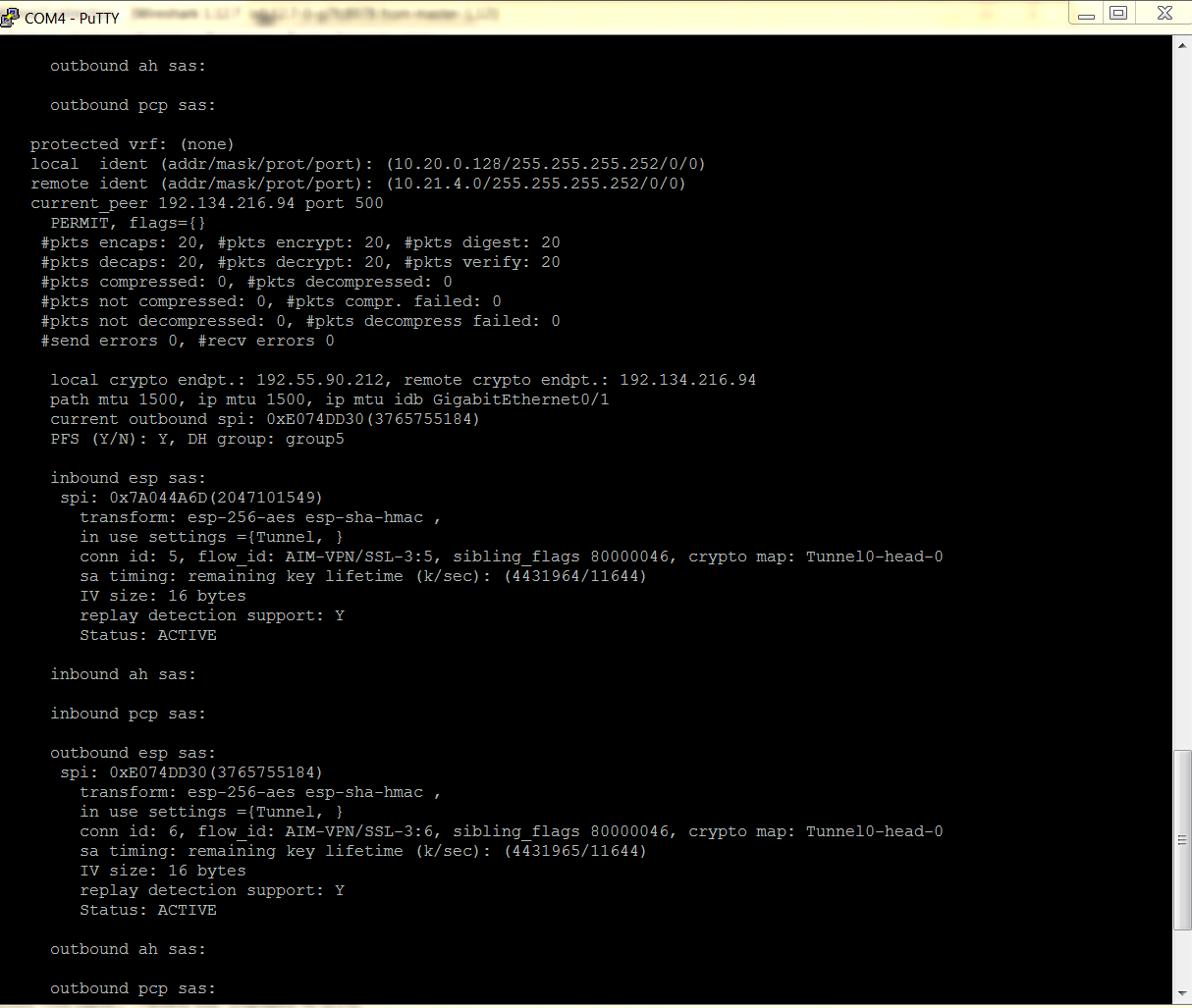
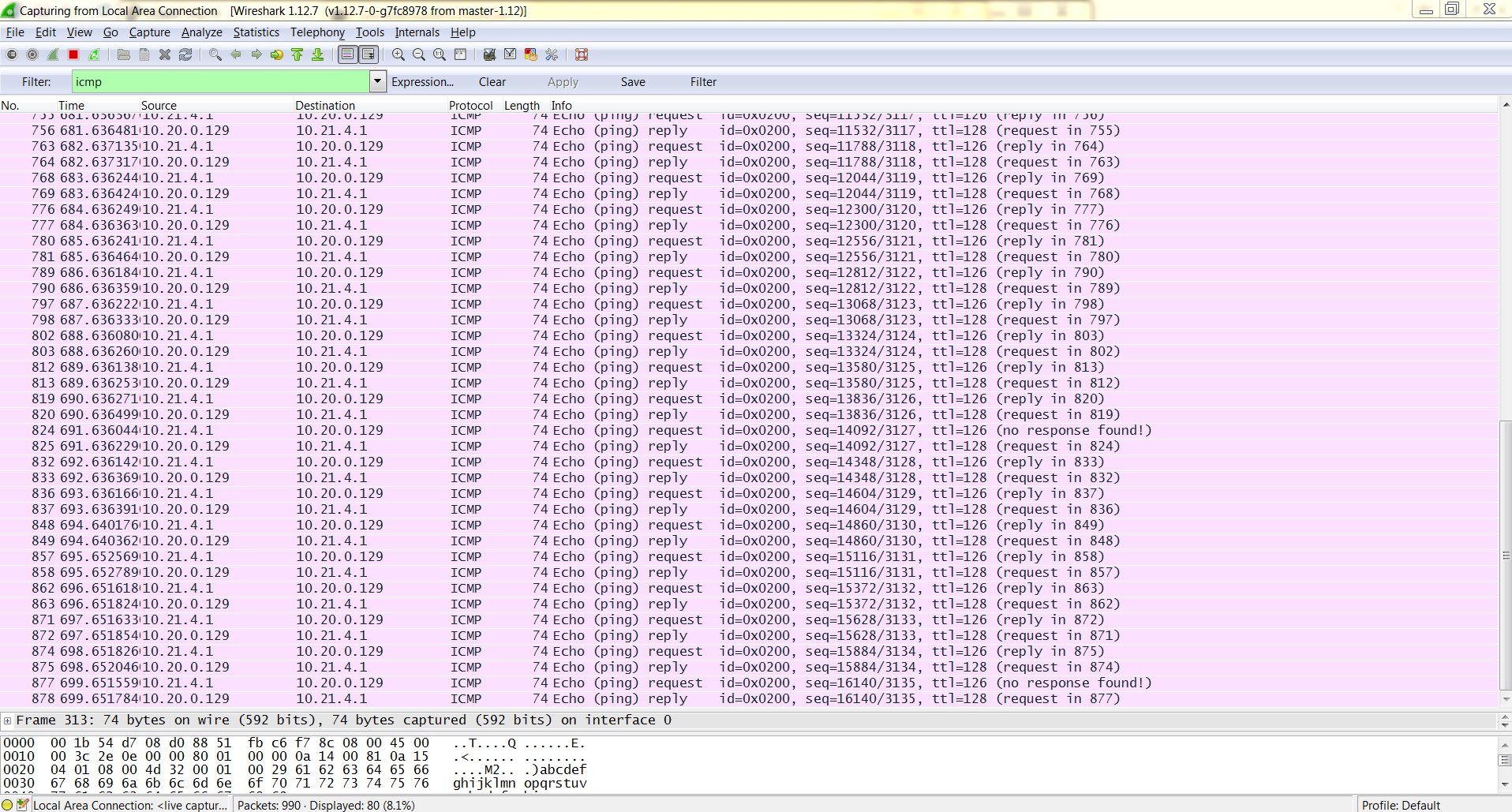




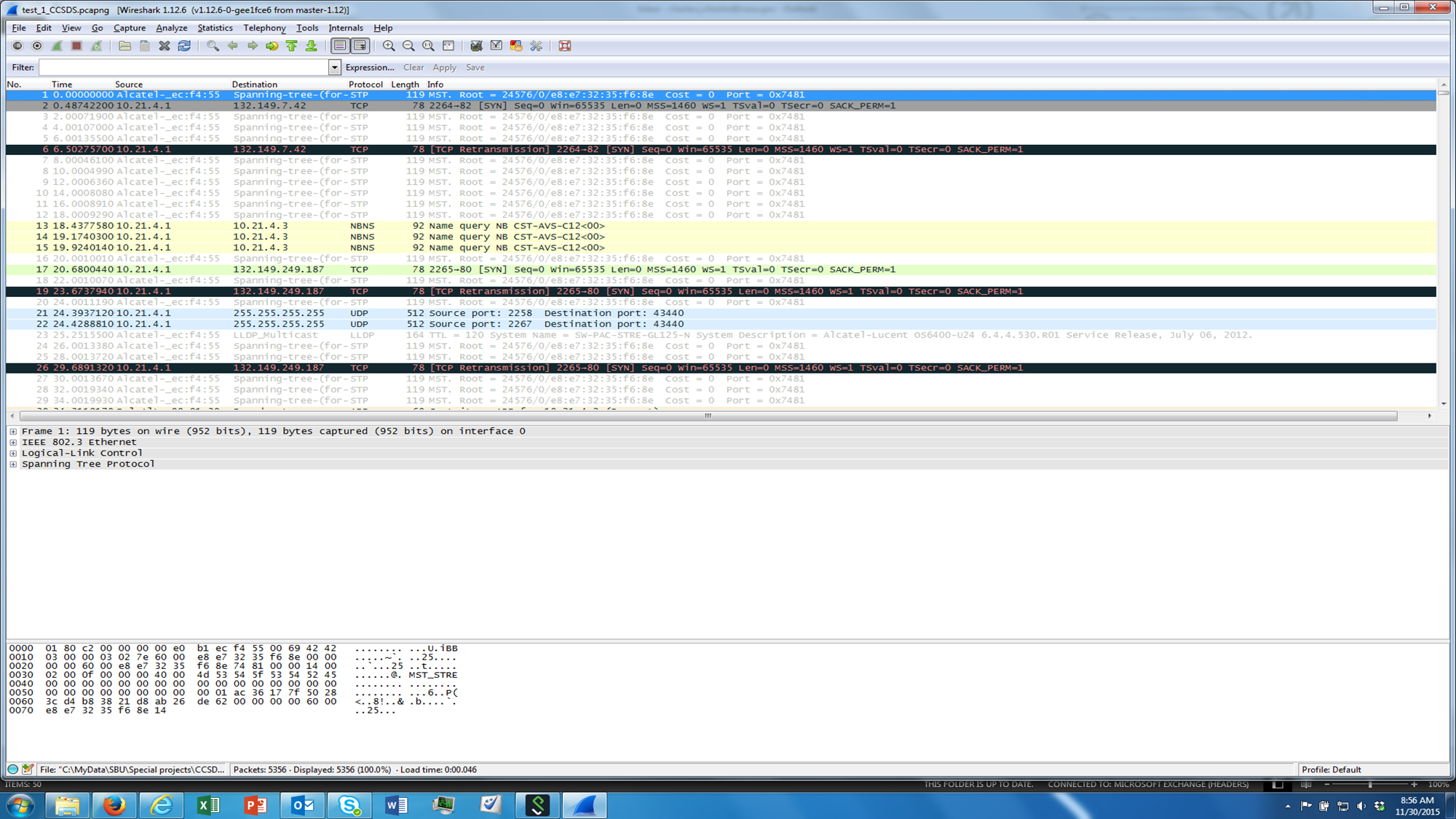
|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Network Layer Security Adaptation Profile |
| 3. | Test Case: | 7, Confidentiality Automatic Keying |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: | Okechukwu Mezu |
| 9. | Results (Pass, Partial Pass, Fail): | **Pass** |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: |  |

The following are the log validating the test conducted:

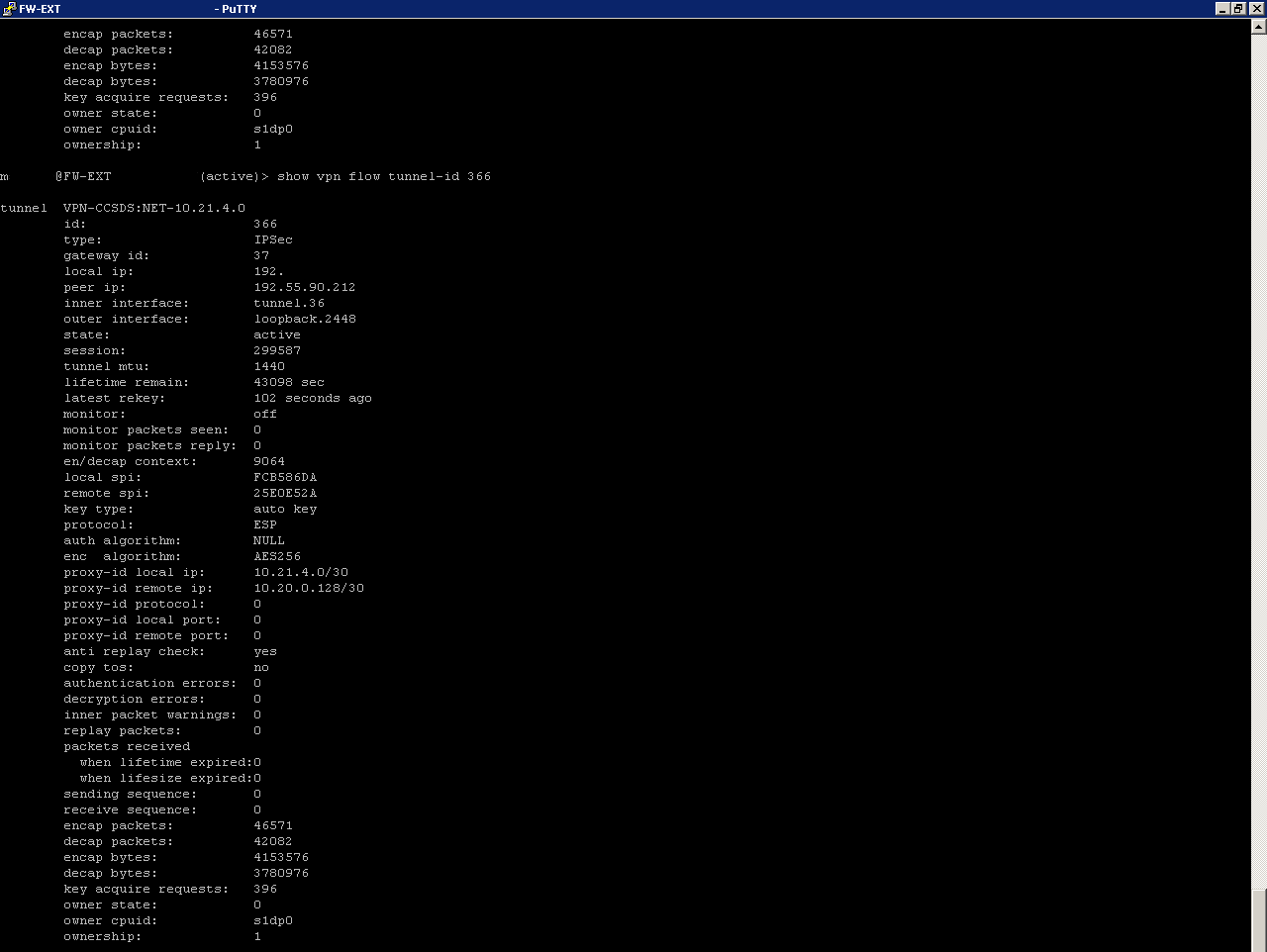
NASA:



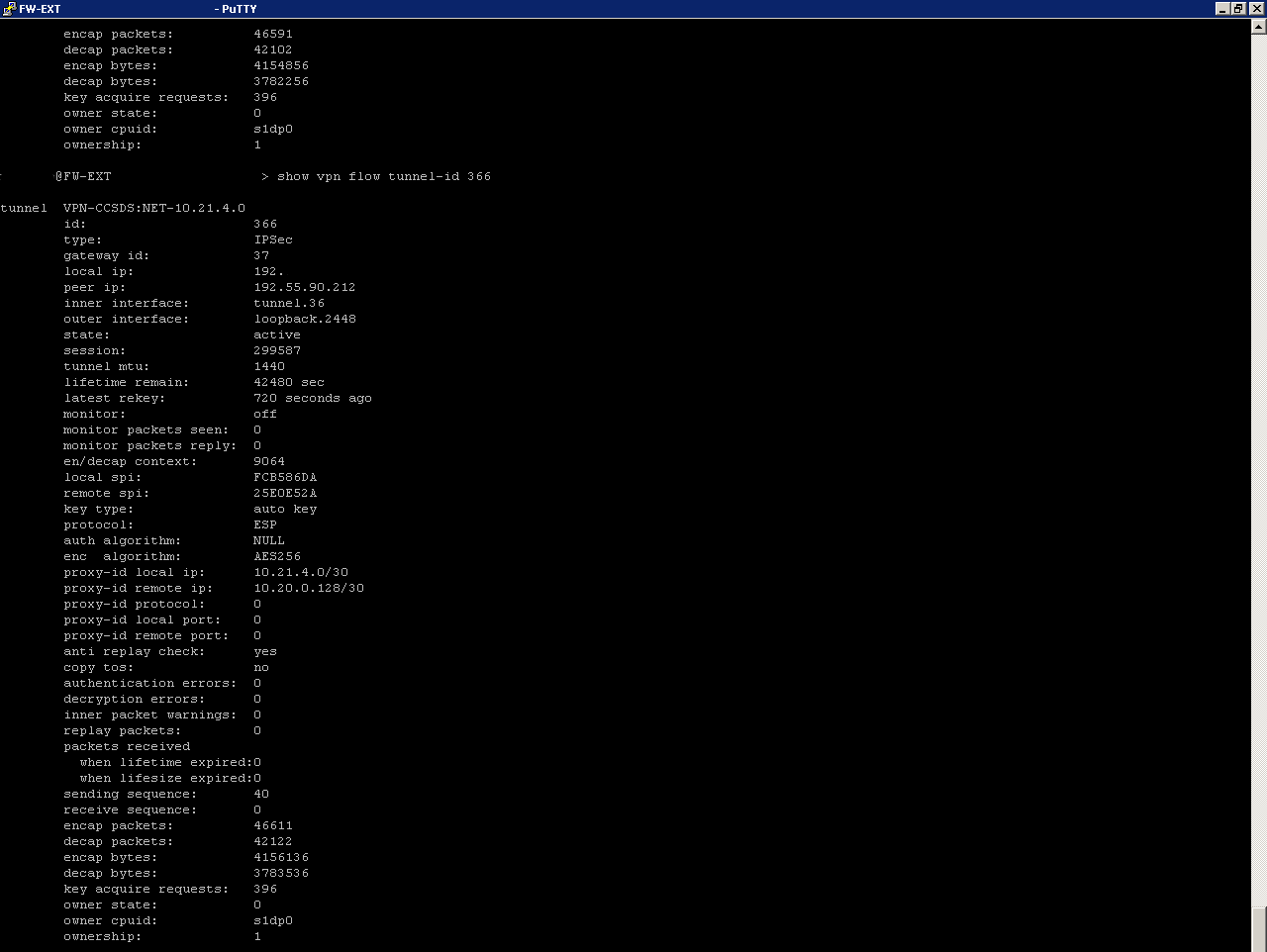
CNES:



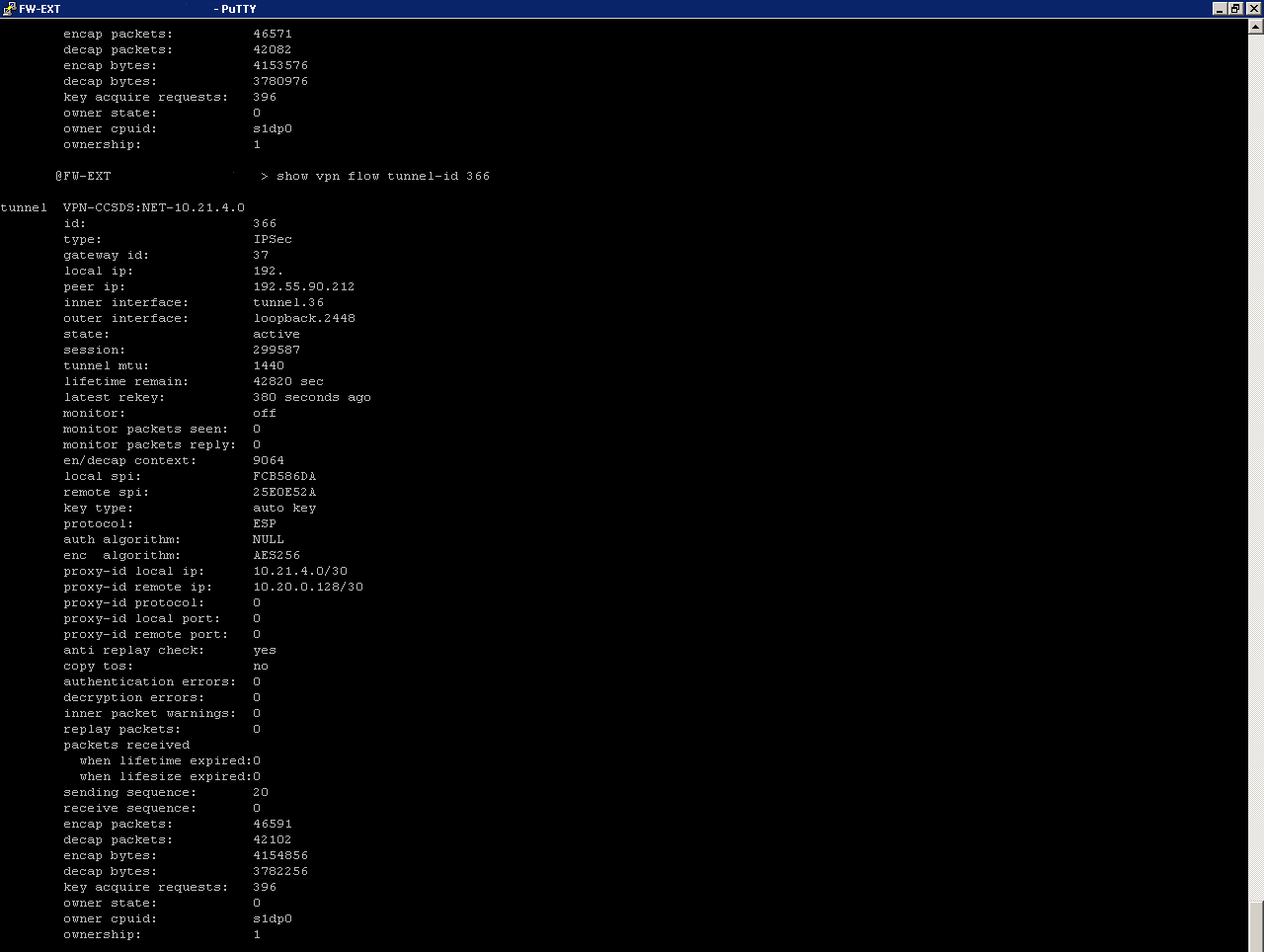
Bytes and Packets counters before traffic:



Bytes and Packets counters after ping from CNES:



Bytes and Packets counters after ping from NASA:





# Observations:

Due to limited budgets for compatibility testing and increased emphasis on institutional network security, it became increasingly difficult to implement legacy configurations that required non-tunnel modes, and manual keying. Static Keys are considered risky and major terrestrial vendors and institutions no longer support this configuration. Terrestrial firewall vendors are responding to networking needs of the internet world and flexibility is reduced in favor of security.

If non-tunnel modes, and manual keying, configurations are needed for space flight, then efforts needs to be undertaken to support space operational modes with vendors to keep these functions within their actively supported equipment and software.