5G SECURITY™ TEST BED

Securing 5G:

Test Results Based on CSRIC VII NSA Recommendations

Document Overview

This document is the first 5G Security Test Bed (5G STB) Report, containing results from the 5G STB's first round of testing which evaluated use cases leveraging a commercially deployed 5G network architecture. The 5G STB is a collaborative endeavor between wireless providers, equipment providers, cybersecurity experts, and academia to demonstrate and validate how 5G security will work in an existence-proof, real-world setting, using commercial technology that can be found in any U.S. network. The 5G STB is designed to allow for rigorous, transparent, and replicable security use case testing and evaluation of 5G devices, network configurations, and software that may be used to secure wireless communications across 5G technologies.

The 5G Security Test Bed evaluates use cases leveraging an actual 5G network architecture built from a significant investment and in-kind contributions in state-of-the-art equipment. This report evaluates some of the 5G security recommendations developed by the Federal Communications Commission advisory group, CSRIC (Communications Security, Reliability, and Interoperability Council) made up of experts from government and industry. Additional tests and use cases are planned. For more information, or to participate in the 5G STB, please contact Harish Punjabi hpunjabi@ctia.org; (202) 845-5701), or visit https://5gsecuritytestbed.com/.

This report was created by the 5G Security Test Bed. The results were produced by 5G STB members and the University of Maryland, which serves as the Test Bed Administrator. The results have been reviewed by the 5G STB's Technical Advisory Committee.

5G STB and TAC Members

The 5G Security Test Bed is a membership effort open to federal agencies, private sector member companies, researchers, and academic institutions. The 5G STB's founding members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, the MITRE Group, and SecureG; and academic partner the University of Maryland, which also serves as the Test Bed Administrator.

The 5G STB has a Technical Advisory Committee (TAC) made up of the 5G STB's founding members and the Test Bed Administrator. The TAC advises the Test Bed Administrator on the day-to-day technical and operational activities and decisions related to the Test Bed, including but not limited to: development of use cases to be tested, test plan development and review, raw test data analysis, test result and report generation, and development of recommendations to standards bodies based on results.

Executive Summary

Following its formal launch in early 2022, the 5G Security Test Bed has completed its inaugural round of tests, with successful results. Using its private 5G network and testing facilities, the 5G STB assessed and verified the efficacy of key 5G network security recommendations made by the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) VII.

Specifically, CSRIC's Working Group 2 (WG2, "Managing Security Risk in the Transition to 5G") made several recommendations to improve security for traffic transmitted over non-standalone (NSA) networks, where the 5G network is built over a 4G Long Term Evolution (LTE) core to support both types of traffic. Because 5G NSA networks are built with both 4G and 5G components, CSRIC's recommendations aim to ensure 4G networks' existing vulnerabilities do not carry over to 5G wireless technologies. The 5G STB has executed three test cases to validate these recommendations.

Through the three test cases, the 5G STB tested encryption over an untrusted connection between the two main components of an NSA network—the 4G/5G radio access network (RAN) and the 4G LTE Evolved Packet Core (EPC)—as well as end-to-end encryption between user equipment (UE) and an external web server. It assessed protections for both user plane traffic (or UP traffic, which is the actual data being transmitted by the user) and control plane traffic (or CP traffic, which directs and controls how data is forwarded through the network).

The tests confirmed that when a non-standalone 5G network exchanges traffic over an untrusted backhaul connection—in other words, a connection between the Radio Access Network and the LTE Core that is not controlled by the mobile network operator—implementing CSRIC's NSA encryption recommendations provides strong security protections for the network traffic.

Of the 5G STB's tests:

- Two test cases assessed 5G traffic encryption through an Internet Protocol Security (IPsec) tunnel, and particularly its ability to protect user traffic and control traffic from threats such as eavesdropping, modifying, and injecting traffic on the untrusted connection.
- The third test case demonstrated the benefits of transport-layer security (TLS) encryption between an application on user equipment and an application server on the public internet.[1]

[1] TLS is a standard for securing data that uses cryptography to encrypt and decrypt data exchanged between sender and recipient networks. The sending and receiving networks decrypt the data they exchange by using public and private keys ranging from 128 to 2048 bits long.

The 5G STB determined that all tests were successful. Specifically, the tests verified that by using an IPsec tunnel to encrypt traffic, eavesdroppers could not decipher, modify, or inject traffic transferred through the network. TLS encryption—which uses cryptography that can only be deciphered at the traffic's origin and destination networks with secret keys—further enhanced these protections.

On the other hand, the tests found that without encryption on an untrusted connection, an eavesdropper could read and manipulate all user traffic and control traffic passing between the RAN and the LTE core, resulting in various outcomes for each traffic type. Without the IPsec tunnel, user traffic that was captured, modified, and injected into the untrusted connection was generally accepted as valid and passed through to the RAN or the LTE core. In some cases, the LTE core identified the injected control traffic as problematic and sent ABORT messages to the RAN, which resulted in a terminated connection.

When an IPsec tunnel was used to encrypt traffic between the RAN and the LTE core, the tests confirmed that all packets of information were indecipherable. Control traffic could not be distinguished from user traffic, and the source and destination addresses of the original messages could not be determined—the encryption caused all traffic to appear as if it was originating and terminating at the IPsec tunnel endpoints. The tunnel also dropped any modified and injected traffic, which was not allowed to pass to either the RAN or the LTE core. The final test verified that end-to-end TLS encryption further obscured the contents of messages sent through the network, preventing eavesdropping, modification, and injection anywhere between the UE and the TLS endpoint on the public internet.

Given the 5G Security Test Bed's initial set of successful tests over 5G non-standalone architecture, future test cases will assess 5G standalone (SA) architecture, where a 5G network is built with only 5G components. Anticipated test case topics include CSRIC VII recommendations for the SA architecture, as well as network slicing and roaming security concerns.

Table of Contents

Introduction – How the 5G Security Test Bed Advances 5G Security

The 5G STB Is the Latest Industry Initiative to Advance 5G Security

The wireless industry prioritizes stronger security and reliability with every generation of its mobile networks. With 5G in particular, secure connectivity is the foundation that supports and enhances the many benefits these networks provide. The wireless industry devotes significant resources to 5G security, and it is further expanding its efforts through its new 5G Security Test Bed.

Formally launched in 2022, the 5G Security Test Bed is a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies, created with a sole focus on testing and validating 5G security recommendations and use cases from government groups, wireless operators, and others. It is the only initiative that uses commercial-grade network equipment and facilities to demonstrate and validate how 5G security standards recommendations will work in practical, real-world conditions.

The 5G STB reflects the industry's collaborative approach to 5G security—it was created by the Cybersecurity Working Group (CSWG), an industry initiative that convenes the world's leading telecom and tech companies to assess and address the present and future of cybersecurity. The 5G STB further works with a broad array of government agencies, policymakers, international standards bodies, thought leaders, and partners in the telecommunications and information technology sectors. These groups include the 3rd Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the FCC, among others.

The 5G STB Uses Real-World Equipment, Validating Real-World Applications

One of the 5G STB's core values lies in its ability to validate 5G security use cases in a real-world environment, using an actual 5G network architecture. Leveraging a significant investment and in-kind contributions, the 5G STB's founding members built this state-of-the-art, private 5G network from scratch for the singular purpose of evaluating 5G network security.

The 5G STB's initial focus is to validate the recommendations of the FCC's CSRIC advisory group, for both non-standalone and standalone network configurations. It will continue evaluating additional recommendations and use cases from CSRIC and other entities in future tests. It is not set up to be a platform for identifying vulnerabilities or conducting penetration testing of networks or equipment.

Real-World Testing

The 5G Security Test Bed advances wireless security by:

- Conducting real-world tests in a rigorous, transparent, and replicable manner that can assess and validate theoretical and policy concerns and overcome hypothetical laboratory testing limitations.
- Drawing on the expertise of government, wireless providers, and equipment manufactures to evaluate specific use cases and support new equipment development.
- Testing security functionality in different scenarios, enabling industry and government to identify, mitigate, and respond to evolving threats while protecting consumers, businesses, and government agencies.

Real-World Applications

The 5G STB's tests and outcomes support several applications that can drive new technology and transform cities, government, and industries. Use cases include government and enterprise applications, general network security protections, and smart city applications such as:

- Government and Enterprise Applications
    - Building private 5G networks for enterprises and government.
    - Developing dynamic supply-chain verification technologies for uses such as logistics management.
    - Creating automated, reconfigurable factories and other automated factory processes.
    - Developing immersive extended reality (XR) applications, including augmented reality (AR), virtual reality (VR), and mixed reality (MR), for both consumers and enterprises.
- General Network Security Protections
    - Enhancing protections against international mobile subscriber identity (IMSI) catchers and "rogue" base stations used by cyber criminals.
    - Enabling automatic, rapid threat detection and response.
    - Implementing a unified authentication framework that supports security across multiple network types (e.g., cellular and Wi-Fi).
- Smart City Applications
    - Enabling video for unmanned aerial systems (e.g., drones).
    - Providing support for autonomous vehicles and related technology (e.g. connected cars and C-V2X standards).
    - Enabling high-resolution video surveillance systems using fixed cameras.

Scope of Report

Security Focus

This report addresses three use cases derived from the FCC's Communications Security, Reliability, and Interoperability Council VII December 2020 report, *Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture.*[2] The CSRIC VII report focused on the implementation of security protections in 5G NSA networks, which provide 5G service over a 4G Long Term Evolution (LTE) core. The report drew upon established findings from standards bodies and industry associations such as the Global System for Mobile Communications (GSMA), the European Telecommunications Standards Institute (ETSI), 3GPP, and NIST to develop its security recommendations.

The 5G STB report's scope is to evaluate and verify CSRIC VII's recommendations by investigating the security features associated with 5G network infrastructure, as well as the use of devices capable of accessing a 5G NSA architecture.

Background

Why CSRIC VII

The Communications Security, Reliability, and Interoperability Council is a federal advisory committee that provides the Federal Communications Commission with recommendations to enhance the security, reliability, and interoperability of communications systems. CSRIC provides a forum for industry and government technical experts to assess developing technology and analyze complex issues. It is a leading venue for stakeholders in and outside of government to share ideas and best practices, and to help the FCC stay abreast of cutting-edge technology and security issues affecting the communications sector. CSRIC's work continues to influence government and industry agendas and activities.

The FCC charters CSRIC every two years. CSRIC VII's charter was from March 2019 to March 2021, and it focused on a range of public safety and homeland security-related communications matters, including issues related to 5G network evolution.

[2] CSRIC VII WG2, Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture (Dec. 2020), https://www.fcc.gov/file/20181/download.

The FCC tasked CSRIC VII with evaluating the transition from the fourth generation of mobile networks (4G) to the fifth generation (5G) to ensure continued reliability, interoperability, and security. The evolution to 5G will take time, which means that new technology will coexist with legacy technology. This raises interesting and complicated issues for real-world network operators and equipment providers.

As one report explained, "[N]etwork upgrades do not happen overnight. A mobile network operator does not flash-cut from one generation of network technology to another. Rather, a new generation will coexist with prior generations for years, even decades."[3] This is the reason operators, manufacturers, standards bodies, and regulators differentiate between "standalone" and "non-standalone" deployments of 5G—a non-standalone network architecture provides 5G service over a 4G LTE core, which enables both services to operate over the same network to limit customer disruption.

CSRIC VII's work resulted in several key reports and recommendations for enhancing security for non-standalone deployments. CSRIC recommendations do not often lead to testing, so industry and academia saw value in validating the effectiveness and achievability of CSRIC VII's recommendations.

CSRIC VII Working Group 2's Report and Recommendations for 5G Non-Standalone Architecture

The Need for 5G NSA Architecture

5G is an evolving global wireless standard that enables more types of devices to connect, delivers higher peak mobile data speeds, increases network capacity and availability, reduces latency, and provides a more uniform user experience to a broader customer base. 5G's unique architecture includes built-in security features, such as mutual authentication and end-to-end encryption that are not available in previous wireless network generations. Because 5G must coexist with 4G as network operators make the transition, it is necessary to establish standards that ensure the networks are interoperable and at the same time take advantage of 5G's enhanced security features.

3rd Generation Partnership Project (3GPP), a global partnership of telecommunications standards organizations, develops standards for mobile communications, including 5G networks. In doing so, 3GPP has built in backward and forward compatibility when possible, which ensures that network operators can provide both 4G LTE and 5G equipment and services to their users during the transition. As a result, many new 5G network deployments use both 4G

[3] Jon Metzler, Security Implications of 5G Networks, UC Berkeley Center for Long-Term Cybersecurity at 7 (Sept. 2020), https://cltc.berkeley.edu/wp-content/uploads/2020/09/Security_Implications_5G.pdf.

LTE and 5G equipment. In these non-standalone, or NSA, networks, the radio portions of the system are 5G, but the core network is shared with LTE. Standalone, or SA, architectures are independent 5G networks using components built specifically for only 5G.

CSRIC VII's Recommendations

CSRIC VII worked to identify and evaluate optional features in the 3GPP standards that would potentially cause security gaps in 5G if not implemented. CSRIC's Working Group 2 (WG2, "Managing Security Risk in the Transition to 5G") released a December 2020 report, *Report on Review and Recommendation on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture* in December 2020.[4] The report focused on the implementation of security in NSA networks that provide 5G service over a 4G LTE core. Within the 3GPP standards, TS 33.401 and 33.501 specified a security architecture of features and mechanisms for the 4G and 5G systems, respectively.

Several security features outlined in 3GPP TS 33.401 and 33.501 are mandatory for equipment vendors to implement in UE, but optional to deploy by 4G and 5G network operators. CSRIC VII WG2 looked at the optional security features and conducted a risk assessment and analysis on those measures, including: confidentiality and integrity for Non-Access Stratum (NAS) signaling,[5] user plane confidentiality and integrity, radio resource control signaling, UE-configured radio technology, several identity and authentication elements, and network security (IPsec and TLS).

Based on its assessment, CSRIC VII WG2 made five recommendations:

- Communications sector members and stakeholders should adopt CSRIC-recommended best practices for hardware and software vendors that collaboratively address security by design principles.[6]
- Operators should use higher layer security protections, such as TLS, to mitigate user plane threats in non-standalone deployments.
- Operators should decide whether to add more security for control plane signaling messages based on customer requirements, risk analysis, and use cases.

[4] CSRIC VII WG2, Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture (Dec. 2020), https://www.fcc.gov/file/20181/download.
[5] "NAS signaling" carries the user data from the user equipment to the MME through the S1 pathway.
[6] This recommendation was restated from a CSRIC V report. *See* CSRIC V WG6, Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network (Sept. 2016). https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx.

- When IPsec is used, operators should decide whether to deploy IPsec Tunnel Mode or Transport Mode over the S1-MME, S1-U, and management interfaces based on a risk analysis and use cases.[7]
- When using IPsec, operators should decide whether to deploy a Security Gateway for IPsec termination on the core network side.

Definition of Use Cases, Leading to Definition of Test Cases

CSRIC VII WG2 identified use cases associated with its five recommendations. In these use cases, the working group assessed options for protecting user plane integrity, control plane integrity, Based on these use cases, the 5G STB established and executed three test cases described in this report, as follows:

1. Confidentiality and Integrity on User Plane:
   a. CSRIC Use Case: CSRIC VII WG2 assessed options for protecting user plane integrity on 5G NSA networks when data is transmitted over an untrusted connection. Based on a risk analysis and use case requirements, network operators may decide whether and how to use encryption on untrusted connections to provide confidentiality over the S1-U interface. Options available to network operators include using IPsec Encapsulating Security Payload (ESP) encryption or an equivalent encryption technology such as MACsec, or proceeding with untrusted connections based on a risk analysis and by use case.
   b. 5G STB Test Case: To demonstrate the application of this mitigation for the user plane, the 5G STB defined a test case that assessed IPsec encryption on the S1-U interface.
2. Confidentiality and Integrity on Control Plane:
   a. CSRIC Use Case: CSRIC VII WG2 assessed options for security on the control plane, including message security for the NAS signaling interface that carries the data between the UE and the MME. As with the user plane, network operators may decide whether and how to use encryption on untrusted connections to provide confidentiality over the S1-MME interface. Options available to network operators include using IPsec, MACsec, or other encryption technologies, or allowing untrusted connections based on a risk analysis and by use case.
   b. 5G STB Test Case: To demonstrate the application of this mitigation for the control plane, the 5G STB defined a test case that assessed IPsec encryption over the S1-MME interface.

[7] "S1" refers to the logical pathways that connect various parts of the 5G NSA network's LTE core to the RAN. The S1-MME is the control plane's pathway, while the S1-U is the user plane's pathway. The MME, or mobility management entity, is the part of the LTE core that manages mobile device operations such as subscriber authentication, roaming, and handovers to other networks.

3. TLS Implementation on User Plane:
    a. CSRIC Use Case: As highlighted in its earlier June 2020 report, CSRIC VII WG2 recommended higher layer security protections to mitigate user plane threats. In its December 2020 report, WG2 recommended these protections be based on application layer functionality—which controls how applications communicate with other applications and devices.
    b. 5G STB Test Case: To demonstrate the application of this mitigation for the user plane, the 5G STB developed a test case for end-to-end TLS encryption through an IPsec tunnel at the application layer.

The 5G STB anticipates that further testing will look at CSRIC VII WG3 recommendations for the 5G standalone architecture,[8] network slicing, subscriber privacy, and roaming security.

5G STB NSA Test Overview

Summary of Process and Findings

In order to validate CSRIC VII's 5G NSA network security recommendations, the 5G STB defined specific test cases that could demonstrate the efficacy of those recommendations and related use cases. As a result, each of the 5G STB's three test cases corresponds with a specific CSRIC recommendation and objective, as described in Table 1.

Table 1: 5G STB NSA High-Level Test Cases

Test Case ID	Test Case Title	CSRIC Recommendation	Objective
TC-IPsec-01 (Test Case 1)	CSRIC 7 WG 2 item - IPsec on UP	CSRIC VII WG 2, Report 2: 7.2.2 User Plane Confidentiality and Integrity over the S1-U 7.2.4 IPsec	User Plane Security – Higher layer protection via S1-U interface confidentiality and integrity using IPsec on an untrusted link
TC-IPsec-02 (Test Case 2)	CSRIC 7 WG 2 item - IPsec on CP	CSRIC VII WG 2, Report 2: 7.2.3 NAS Signaling Confidentiality and Integrity over the S1-MME 7.2.4 IPsec	Control Plane Security – Higher layer protection via S1-MME interface confidentiality and integrity using IPsec on an untrusted link

[8] CSRIC VII WG3, Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards (Sept. 16, 2020), https://www.fcc.gov/file/19297/download.

TC-IPsec-03 (Test Case 3)	CSRIC 7 WG 2 item – TLS on UP	CSRIC VII WG 2, Report 2: 7.2.2 User Plane Confidentiality and Integrity over the S1-U	User Plane Security – Higher layer protection at application layer using end-to-end TLS encryption through an IPsec tunnel

The 5G STB then developed detailed test plans with step-by-step procedures for setting up and executing tests, including defining specific test points, means of generating and capturing traffic, and other details. While the test results are provided in detail in a later section, Table 2 previews the high-level findings below.

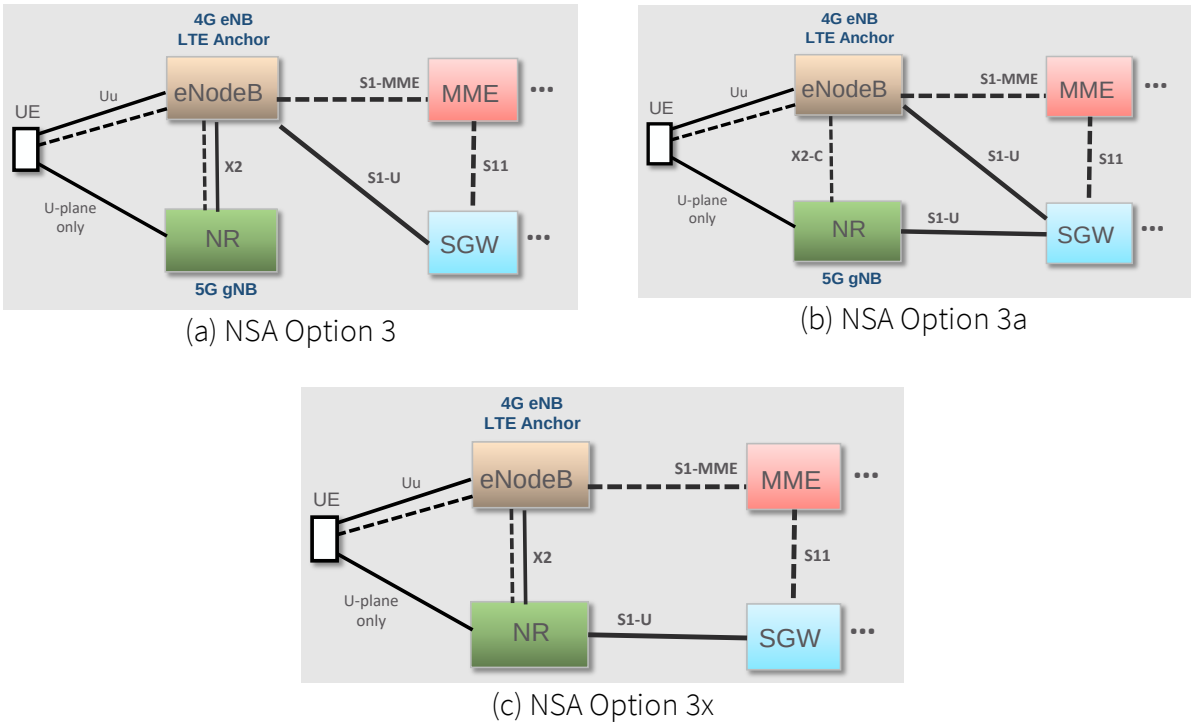
Table 2: 5G STB NSA Test Case Result Summary

Test Case Title	Conclusion	Rationale
CSRIC 7 WG 2 item - IPsec on UP	Success	When the IPsec tunnel is implemented on the untrusted link, an eavesdropper cannot read the user traffic transmitted over the link (it all appears as ESP-encrypted packets with source and destination addresses as the endpoints of the tunnel). The IPsec tunnel does not allow modified and injected packets to exit the tunnel.
CSRIC 7 WG 2 item - IPsec on CP	Success	When the IPsec tunnel is implemented on the untrusted link, an eavesdropper cannot read the CP traffic transmitted over the link (it all appears as ESP-encrypted packets with source and destination addresses as the endpoints of the tunnel). The IPsec tunnel does not allow modified and injected control packets to exit the tunnel.
CSRIC 7 WG 2 item – TLS on UP	Success	When TLS encryption is implemented on the untrusted link, an eavesdropper cannot read the user traffic with or without IPsec encryption. This includes all capture points, not just those on the untrusted link. Adding IPsec to the untrusted link further obscures the traffic, preventing an eavesdropper from reading the source and destination of the TLS messages, as well as knowing which encapsulated packets are TLS. TLS encryption and IPsec encryption do not allow modified and injected packets to reach their intended destinations.

As presented in the table above, all three of the 5G STB's tests successfully validated CSRIC VII's recommendations for implementing IPsec and TLS encryption to protect user plane and/or control plane traffic travelling through 5G NSA networks.

NSA Network Architecture and Test Configuration

3GPP has defined multiple deployment options for 5G NSA networks. Figure 1 below shows 3GPP's NSA Options 3, 3a, and 3x, which all use E-UTRA New Radio – Dual Connectivity (EN-DC) with LTE serving as the Master Radio Access Technology (RAT) and the 5G New Radio (NR) serving as the Secondary RAT.



(a) NSA Option 3

(b) NSA Option 3a

(c) NSA Option 3x

Figure 1: NSA Options

Option 3x is network operators' preferred choice because its direct connection between the 5G system's NR user plane and the LTE system's Evolved Packet Core (EPC) ensure minimal impact on existing networks. The test cases in this document use Option 3x.

Figure 2 shows how the configuration of Option 3x using the Security Gateway (SEG) for IPsec termination.

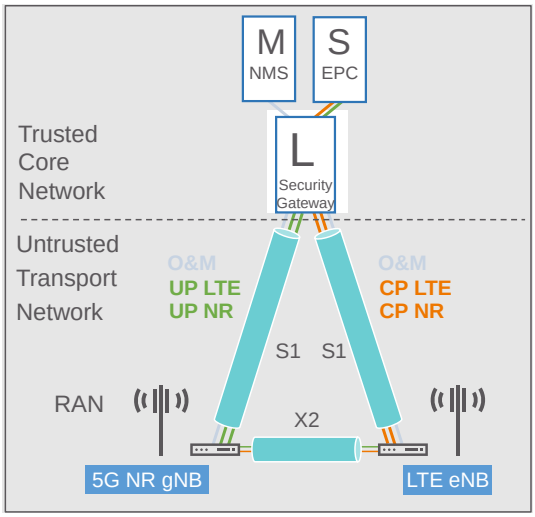


Figure 2: 5G NSA network configuration Option 3x, with SEG for IPsec termination

The physical network configuration used for the 5G STB's initial non-standalone tests consists of a radio access network (RAN) hosted at the University of Maryland and a 4G LTE Evolved Packet Core hosted at the MITRE Corporation in Virginia. Both installations are in secure facilities with safeguards and procedures to ensure the integrity and security of operations.

The connection between the RAN at UMD and the EPC at MITRE is transmitted over the internet and, therefore, for the scenarios considered here, is treated as an untrusted link[9]. Figure 3 shows the configuration for the NSA test cases. The 5G RAN, LTE RAN, and LTE EPC have been provided by Ericsson. The Ericsson EPC product is a combination SGW/PGW/UPF (serving gateway, packet data network gateway, and user plane function). It is configured as SGW/PGW for the purposes of the NSA test cases.

[9] The connection between the two sites is actually protected by two additional security tunnels: both an IPsec tunnel between UMD campus and the MITRE network, protecting traffic over the internet; and a second tunnel between devices in the 5G STB enclaves to further limit access to appropriate personnel.

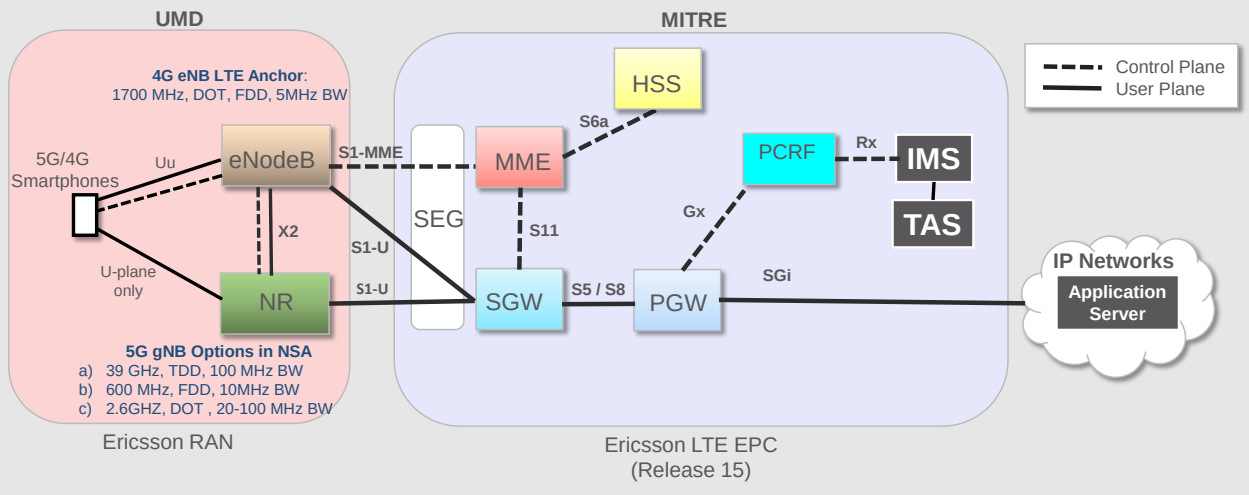


Figure 3: NSA Test Configuration for CSRIC Use Cases

Detailed Test Procedure

Figure 4 shows the test bed's relevant components, including test points (TP) for various tests. The routers shown at each location are Ericsson 6672 routers (referred to as R6672 or R6K for short) and serve as IPsec tunnel endpoints. The switches shown are each Pluribus Freedom 9372-X switches. For the purposes of these tests, the two switches are considered part of the "untrusted" backhaul link.

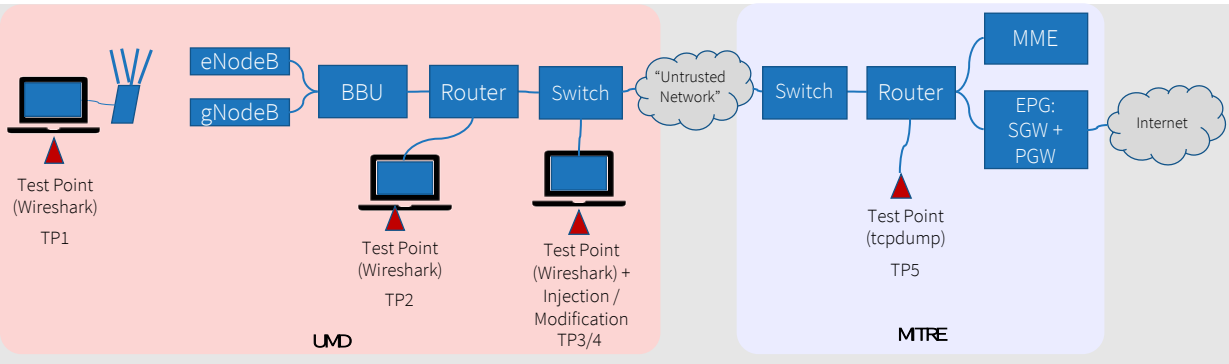


Figure 4: 5G Security Test Bed's Physical Connections and Test Points

The User Equipment (UE) being used in these tests consists of a Sierra Wireless EM9190 card connecting to a laptop by USB. Band 66 is used for LTE and N71 for 5G. For the user plane tests of Test Case 1, traffic is generated at the UE by running the ping command in a Windows Command Prompt, with a desired destination at IP address 8.8.8.8 (the address for Google's domain name server). For the control plane tests of Test Case 2, no user traffic is purposefully generated (although the Windows operating system creates some traffic). For the TLS test of Test Case 3, an HTTPS session is opened from a web browser on the UE laptop.

During the tests, packets are captured on each of the identified test points in Figure 4: at the UE, on the RAN-side R6K router, on the RAN-side Pluribus switch, and on the LTE core-side R6K router. These test points are identified with numbers as shown in the figure and described in more detail in Table 3, below. Packets captured at TP3 on the untrusted link are saved using tcpdump and then modified using Kali Linux and injected into the untrusted link at the same test point. Due to the manual process for starting and stopping packet captures, each set of packet captures starts and stops at a slightly different time. As a result, packets appearing at the beginning or end of the test period may not be present in all captures, and, consequently, counts of specific packets at each test point may differ slightly.

Table 3: Test Point Descriptions

Test Point	Description and Use
TP1	Wireshark running on laptop connected to UE; captures packets originating and terminating at UE laptop
TP2	Wireshark running on laptop connected to RAN-side R6K router; can be configured to capture packets outside the tunnel (i.e., before IPsec encryption or after IPsec decryption) or inside the tunnel (encrypted packets when IPsec tunnel is enabled)
TP3	tcpdump running on laptop connected to the port of RAN-side Pluribus switch used to capture, modify, and inject packets on the untrusted link
TP4	Wireshark running on laptop connected to port of RAN-side Pluribus switch used to monitor packets on the untrusted link
TP5	tcpdump running on computer connected to core-side R6K router; configured to capture packets outside the tunnel (i.e., before IPsec encryption or after IPsec decryption) and inside the tunnel (encrypted packets when IPsec tunnel is enabled)

Wireshark was used to display and filter traffic. It is worth noting that the RAN encapsulates all packets with the GPRS Tunneling Protocol (GTP), so, when observing Wireshark captures, there is an outer Ethernet frame encapsulating a GTP-formatted packet, which itself contains the IP packet. When TLS is used, it encapsulates yet another packet, the encrypted version of the original packet.

While the 5G STB's objective is to verify the efficacy of recommended encryption procedures, we also demonstrate the ability to eavesdrop, modify, and inject packets when the traffic on the untrusted link is left unencrypted. For unencrypted user plane traffic, tcpdump was configured to capture only pings and ping responses (ICMP traffic); for unencrypted control plane traffic, tcpdump captured the naturally occurring control plane traffic, which is the S1 Application Protocol (S1AP) traffic transported over SCTP. When traffic on the untrusted link is encrypted, tcpdump only sees encrypted packets and cannot distinguish between user traffic and control traffic, so all traffic is captured and replayed. Furthermore, for UP test cases, because we can limit the traffic the UE puts on the network, it is straightforward to determine whether injected

traffic is dropped in the IPsec tunnel. However, because we have no control over the CP traffic generated by the RAN and LTE core, in order to make it clear whether or not injected CP packets are dropped, we inject over 1,000 false CP packets during a test and measure the differences in number of packets captured at each test point.

For cases implementing an IPsec tunnel, we used pre-shared keys (PSK) to establish the security association between the two tunnel endpoints. Note that the original use case called for signed certificates. However, the effort to establish the Public Key Infrastructure was deemed excessive for the purposes of these tests, which require encryption, regardless of the security association method.

5G STB NSA Test Results

Table 4 contains the configuration parameters used for the tests.

Table 4: RAN Configuration Parameters

RAT	Band	TDD/FDD	DL EARFCN	UL EARFCN	Bandwidth
LTE Anchor	B66	FDD	66786	132322	20 MHz
NR	N71	FDD	126900	136100	15 MHz

Table 5 shows the connectivity status at the start of the test, including the IP address assigned by the EPC to the laptop connected to the Sierra Wireless card.

Table 5: Modem Connection Details

Parameter	Value
Connection Mode	EN-DC
IP Address	172.18.0.3

Test Case 1, TC-IPsec-01

TC-IPsec-01 has two objectives: (1) to demonstrate that, without encryption on the untrusted link, it is possible to eavesdrop, modify, and inject data packets on the user plane; and (2) to verify that, with an IPsec tunnel between the RAN and LTE core, packets cannot be read, modified, or injected on the user plane.

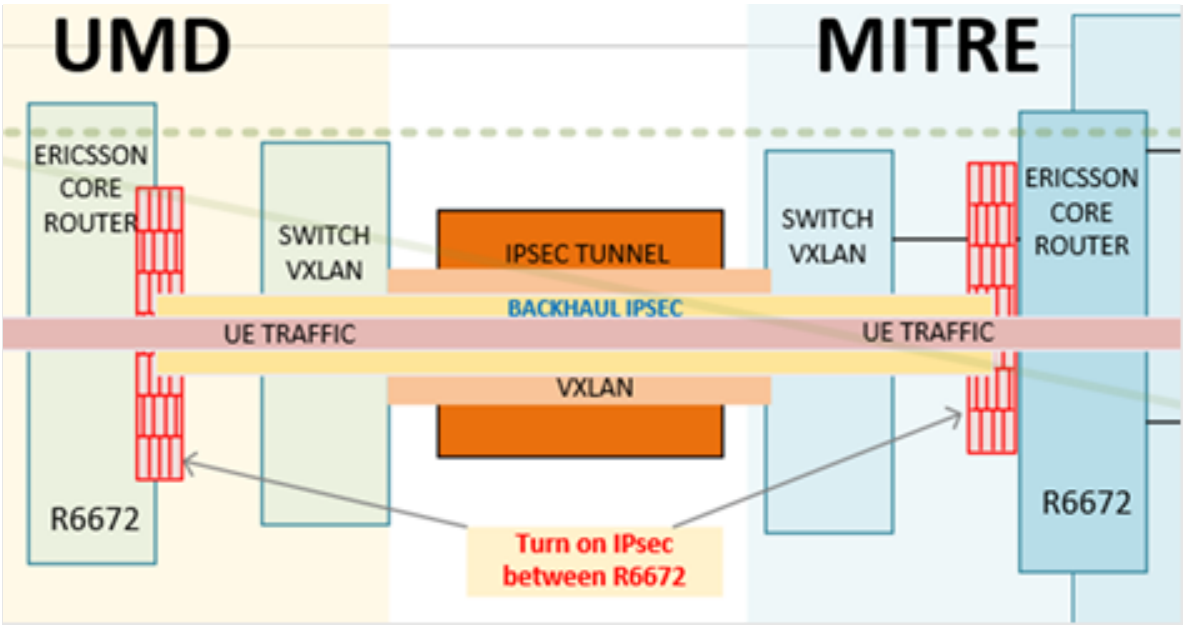


Figure 1: IPsec Tunnel Implementation

Objective 1: Verify ability to eavesdrop, modify, inject payload on UP

Figure 6 shows the traffic captured on the UE where Wireshark is used to display and filter traffic. In this figure, only ICMP (ping requests and replies) messages are shown. For reference on this and subsequent figures, Table 6 lists the files whose data are shown in the figures, along with a description of the contents.

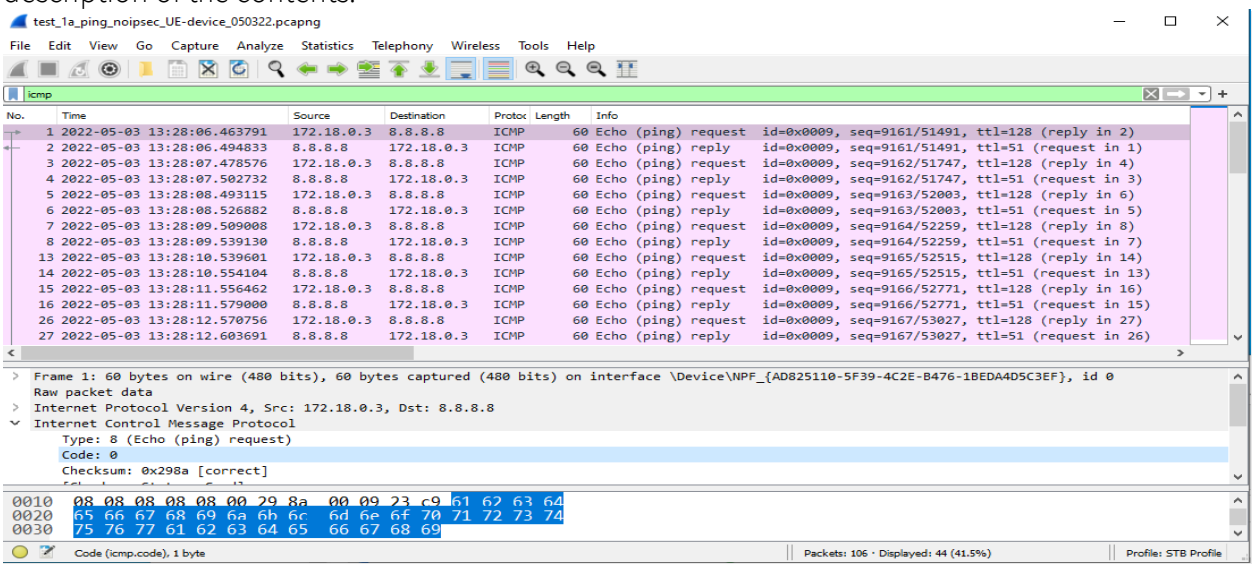


Figure 6: UE Packet Capture

Table 6: Test Case 1 Raw Data Files and Content Descriptions When IPsec Not Implemented

File Name	Contents
test_1a_ping_noipsec_UE-device_050322.pcapng	Ping packets captured at TP1, laptop connected to UE
ping050322.pcap	Captured ping traffic at TP3
mod_ping050322.pcap	Modified ping traffic
final_test_1a_ping_noipsec_testlaptop_050322.pcapng	Injected ping traffic at TP3
final_test_1a_ping_noipsec_pluribus_050322_mod.pcapng	Injected traffic captured at TP4 on outgoing interface to the core
test1A2-MITRE-r6k-noipsec-050322-1640.pcap	Traffic captured at TP5 on core-side ingress R6K interface from RAN
test1A2-MITRE-r6k-clear-050322-1640.pcap	Traffic captured at TP5 on core-side egress R6K interface toward internet

Figure 7 shows three Wireshark windows: one displaying contents of the PCAP file created by tcpdump on the untrusted link that captures transmitted packets to be later modified; one displaying the contents of the PCAP file that results from modifying those captured packets; and one that displays the packets observed on the Pluribus switch after the injection point (TP4). Each window's lower portion breaks down the packet highlighted in its upper portion. The modification that is implemented is changing the source MAC address of the message, which can be seen as Ericsson_8b:a0:50 (98:7a:10:8b:a0:50) in the first window and 66:0e:94:d3:a0:21 in both the modified and injected packet captures displayed in the second and third windows.

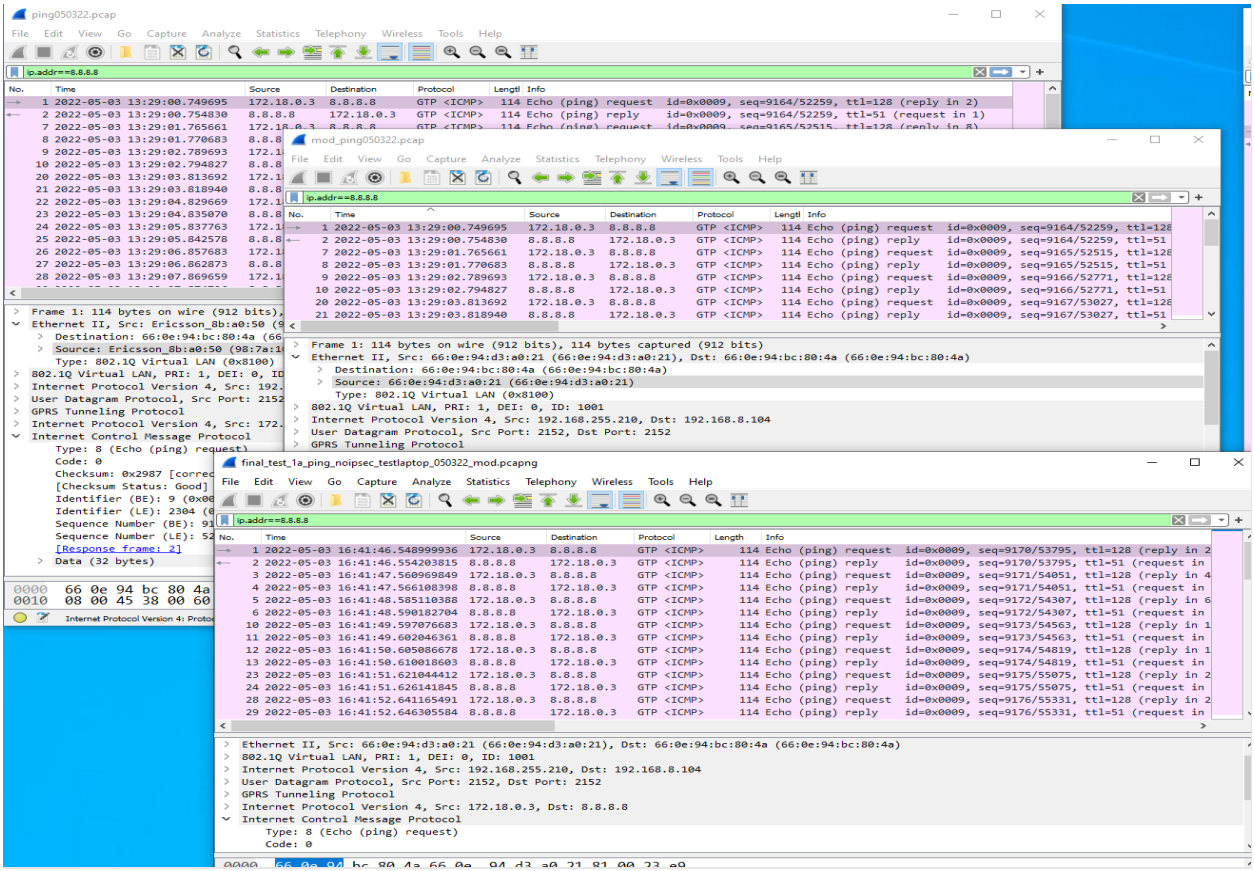


Figure 7: RAN-Side Captures on Untrusted Link: Eavesdropped/Captured Packets; Modified Packets; Injected Packets

Figure 8 and Figure 9 show the relevant packet captures when the ping is stopped on the UE, but the captured packets are modified and injected into the untrusted link. Figure 8 shows the packets captured at the output of the RAN-side switch facing the LTE core (TP4). Figure 9 shows the packet captures at the core-side router (TP5), which includes the traffic captured at the tunnel endpoint (ingress R6K interface) and on the interface toward the SGW/internet (egress/clear R6K interface). Note that, although the UE is not sending any ping packets, the same ICMP traffic is visible at all test points, and, specifically, the ping packets are completely decipherable on the untrusted link. Figure 9 further shows that modified ping packets are received on the ingress R6K interface on the core side, and ping packets (reply and request) are seen on the egress interface of R6K with the correct control codes.

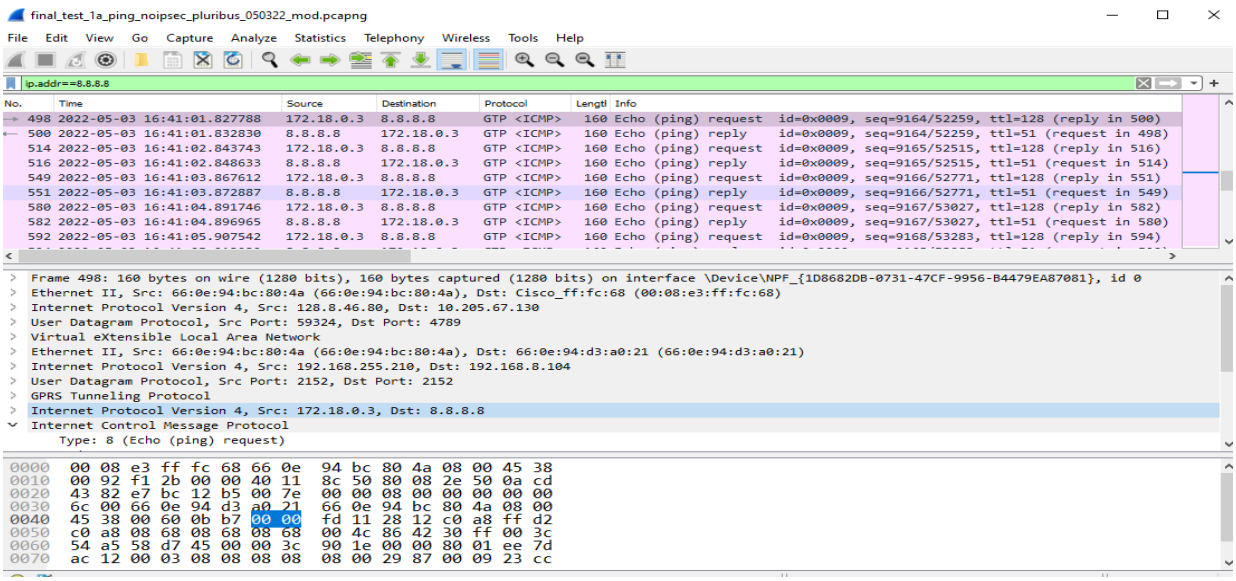


Figure 8: RAN-side Untrusted Link Capture on Outgoing Port Toward Core

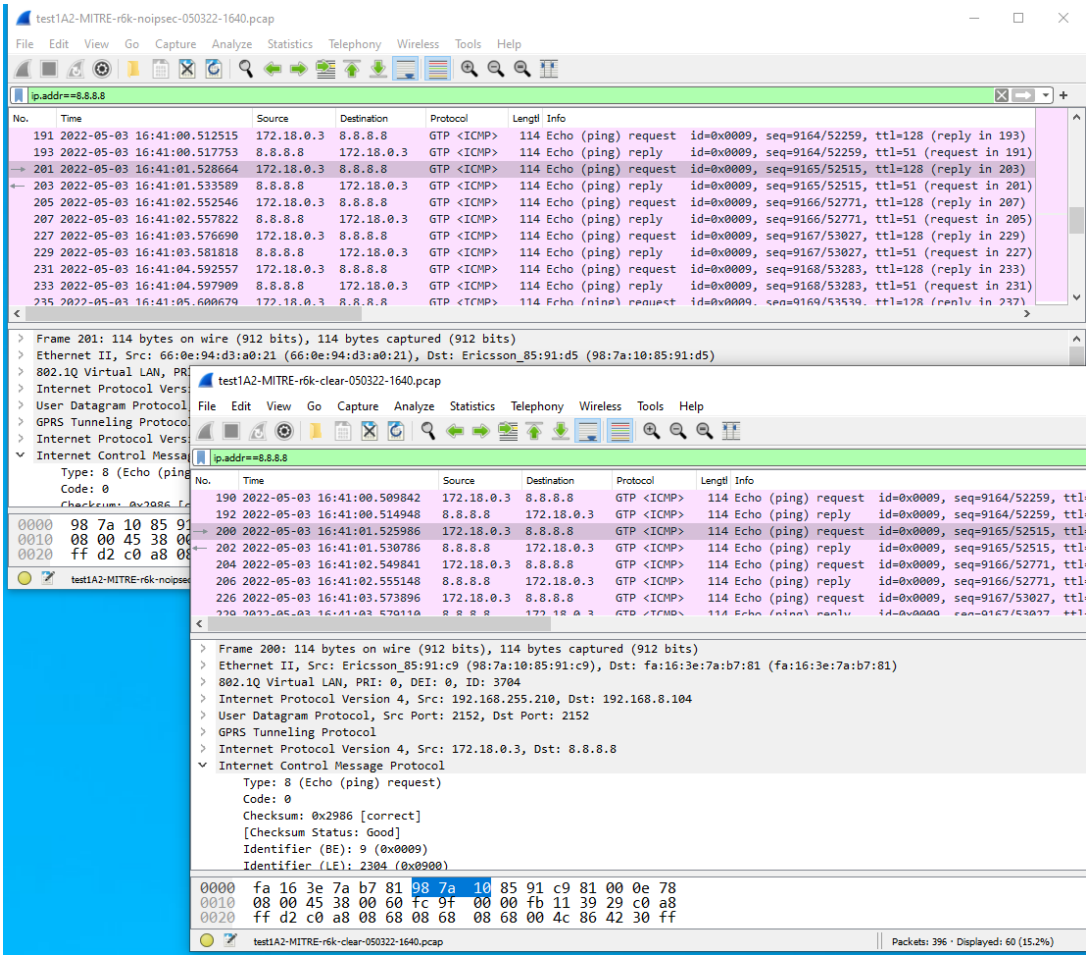


Figure 9: Core-Side Untrusted Link Capture and Core-Side (Trusted) Router Capture

Objective 2: Verify inability to eavesdrop, modify, inject payload on UP

As organized in Figure 7 above, Figure 10 displays three windows: two PCAP files corresponding to the captured packets and modified packets (where, again, the MAC address has been modified), and one PCAP file corresponding to the capture of the injected packets at TP4. As can be seen in the figures, traffic is indistinguishable as it all appears as encrypted (ESP) packets. There are no ICMP packets indicated, nor is there any indication of what traffic is control plane traffic. The source and destination IP addresses shown in the Wireshark windows are those of the endpoints of the IPsec tunnel. For reference on this and subsequent figures, Table 7 lists the files whose data are shown in the figures along with a description of the contents.

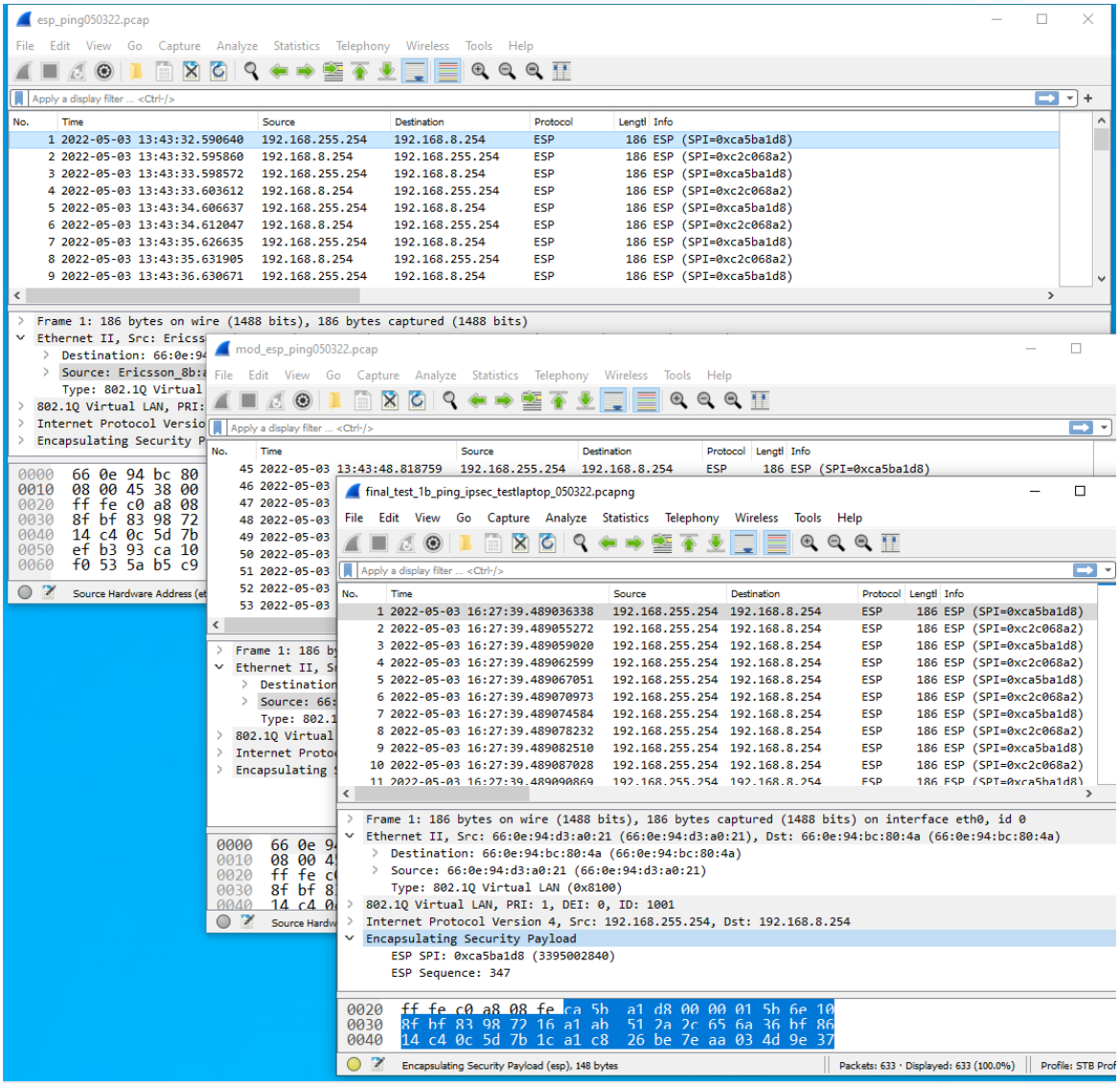


Figure 10: RAN-Side Untrusted Link Capture of Encrypted Traffic, Modification of Packets, and Injected Packets

Table 7: Test Case 1 Raw Data Files and Content Descriptions When IPsec Implemented on Untrusted Link

File Name	Contents
esp_ping_050322.pcap	Captured ESP traffic at TP3
mod_esp_ping050322.pcap	Modified ESP traffic
final_test_1b_ping_ipsec_testlaptop_050322.pcapng	Injected ESP traffic at TP3
final_test_1b_ping_ipsec_pluribus_050322.pcapng	Injected traffic captured at TP4 on outgoing RAN-side switch interface toward LTE core
test1B-MITRE-r6k-ipsec-050322-1626.pcap	Traffic captured at TP5 on core-side ingress R6K interface from RAN
test1B-MITRE-r6k-clear-050322-1626.pcap	Traffic captured at TP5 on core-side egress R6K interface toward internet
final_test_1b_ping_ipsec_R6K_050322.pcapng	Traffic captured at TP2 on RAN-side ingress R6K interface

Figure 11 shows the packet captures at the port of the RAN-side switch that faces the LTE core (TP4) and at the core-side router (TP5). Again, we cannot distinguish between the traffic that exists, for example, due to control plane messages between the RAN and the core and the injected encrypted packets. We do know, though, that the injected packets, which contained ping packets from the UE, do not exit the IPsec tunnel. The third window in Figure 11 demonstrates this, showing that no packets arrive at the ping destination address, 8.8.8.8. That is, modified ESP packets are received on the ingress R6K interface on the core side (TP5), but ping packets are not seen on the egress interface (also TP5), which indicates that the modified and injected UP packets were dropped at the tunnel endpoint. In addition, Figure 12 shows traffic on the RAN-side R6K (TP2), filtered for IP address 8.8.8.8, indicating that no ICMP traffic exists outside the tunnel on the RAN side either. Specifically, 652 ESP packets are received at the core within the IPsec tunnel, but only 44 packets are detected on the egress R6K interface at the core. None of those packets are ICMP packets, which the injected traffic contained. On the RAN side, of the 105 packets captured on the ingress interface, none were ICMP packets.

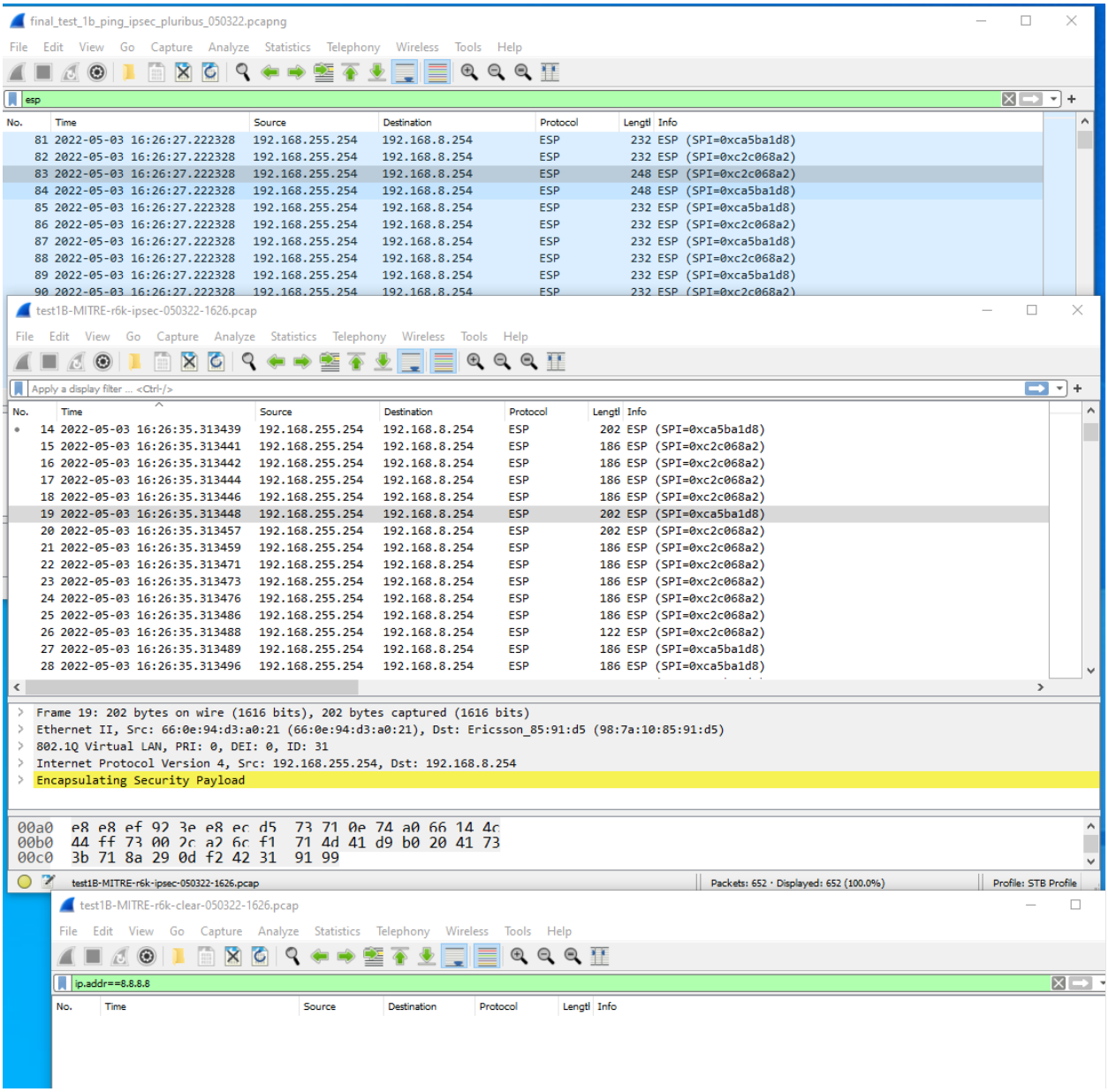


Figure 11: RAN-Side Outgoing Link to Core; Core-Side Untrusted Link Capture of Encrypted Traffic; and Core-Side Capture at Trusted Router after Decryption

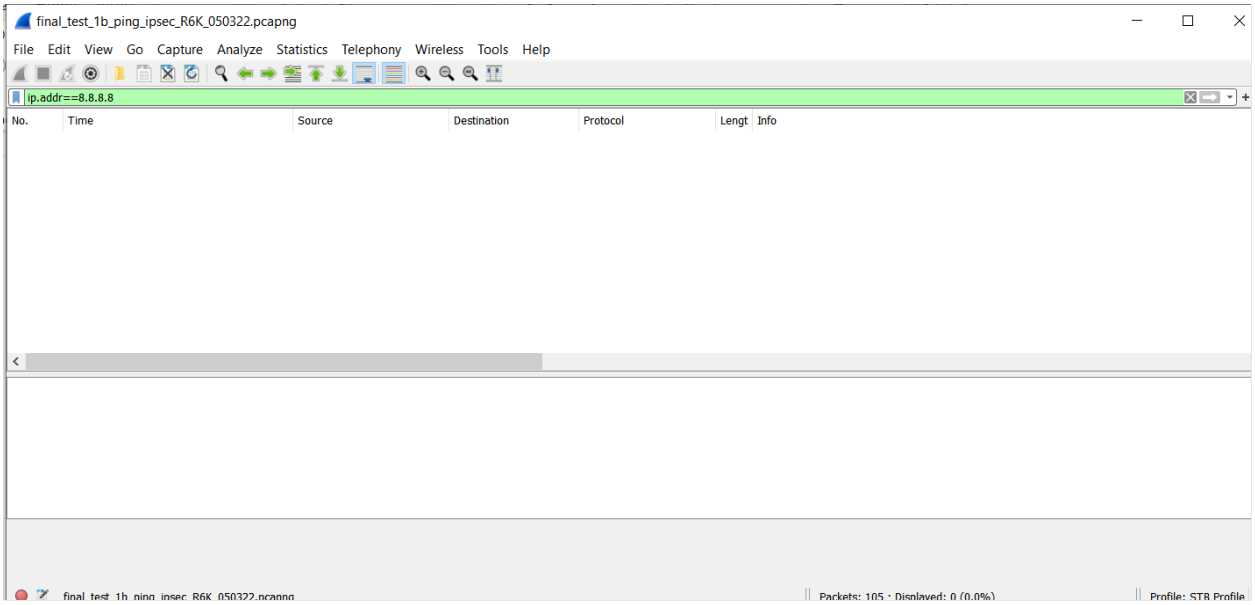


Figure 12: RAN-Side Router Packet Capture Showing No ICMP Packets to or from 8.8.8.8

Test Result

Success: When the IPsec tunnel is implemented on the untrusted link, an eavesdropper cannot read the traffic over the link (it all appears as ESP encrypted packets with source and destination addresses as the endpoints of the tunnel); modification and injection of packets fail to pass out of the tunnel. When IPsec is not implemented, the content of the packets on the untrusted link are decipherable, and injected packets appear to pass through to the internet.

Test Case 2, TC-IPsec-02

The objective of TC-IPsec-02 is to verify that, with an IPsec tunnel between the RAN and the LTE core, packets cannot be read, modified, or injected on the control plane. It also demonstrates that, in the absence of IPsec tunnel, injected control plane traffic gets passed through, although the core appears to reject some replayed packets.

Objective: Verify inability to eavesdrop, modify, or inject payload on CP

As in previous sections, Table 8 lists the files used to store packet captures where those file names are shown in the headers of the Wireshark windows.

Table 8: Test Case 2 Raw Data Files and Content Descriptions for Runs with and without IPsec Encryption on Untrusted Link

File Name	Contents
control050322.pcap	Captured control traffic at TP3
mod_control050322.pcap	Modified control traffic
final_test_2a_control_noipsec_testlaptop_050322.pcapng	Injected control traffic captured at TP4 on outgoing interface to LTE core
test2A-MITRE-r6k-noipsec-041922-1615.pcap	Traffic captured at TP5 on core-side ingress R6K interface from RAN
test2A-MITRE-r6k-clear-041922-1632.pcap	Traffic captured at TP5 on core-side egress R6K interface toward MME
final_test_2a_control_noipsec_R6K_050322.pcapng	Traffic from core captured at TP2 on RAN-side R6K trusted interface
mod_esp_control_050322.pcap	Modified ESP encrypted control traffic
final_test_2b_control_ipsec_testlaptop_050322.pcapng	Injected ESP encrypted control traffic at TP3
final_test_2b_control_ipsec_pluribus_050322.pcapng	Injected ESP encrypted control traffic captured at TP4 on outgoing interface to the core
test2B-MITRE-r6k-ipsec-050322-1628.pcap	ESP encrypted control traffic captured at TP5 on core-side egress R6K interface toward internet
test2B-MITRE-r6k-clear-050322-1628.pcap	Decrypted control traffic captured at TP5 on core-side egress R6K interface toward MME
final_test_2b_control_ipsec_R6K_050322.pcapng	Decrypted control traffic from core captured at TP2 on RAN-side R6K trusted interface

In Figure 13, the first window shows the captured packets from the natural operation of the system (in this case, control messages between the RAN and the LTE core), without the IPsec tunnel; the second window shows modified packets (here restricted to the control packets from the RAN address, 192.168.255.226, to the MME address, 192.168.8.136); and the third window shows the packets as captured on the switch on the untrusted link, which now includes injected packets. Unlike Test Case 1, where we stopped the UE pings, we are unable to stop the flow of control plane messages in the absence of the IPsec tunnel.

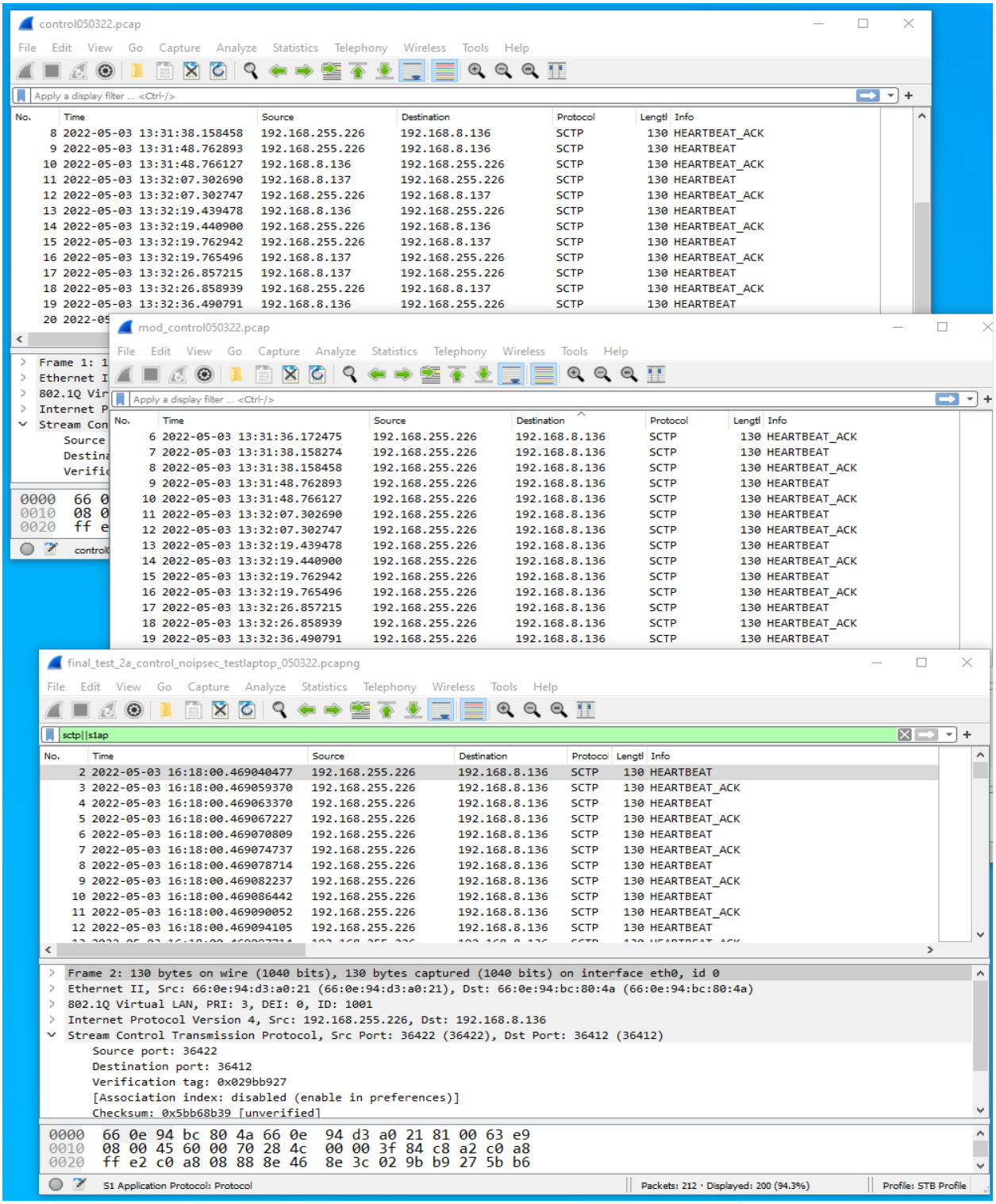


Figure 13: RAN-side Capture of Control Packets, Modified Control Packets and Injected Control Packets on Untrusted Link

Figure 14 and Figure 15 show the captures on the untrusted link (TP4 and TP5), as well as the egress of the core-side router (also TP5). Note that these captures show the presence of control traffic at roughly the same number as were captured on the RAN side. Modified control packets (SCTP and S1AP) are seen on the egress interface of R6K at both core and RAN sides. In addition, ABORT packets from the MME to the RAN are seen. These ABORT packets likely indicate that some of the injected packets did not pass an integrity or duplication check in the MME.

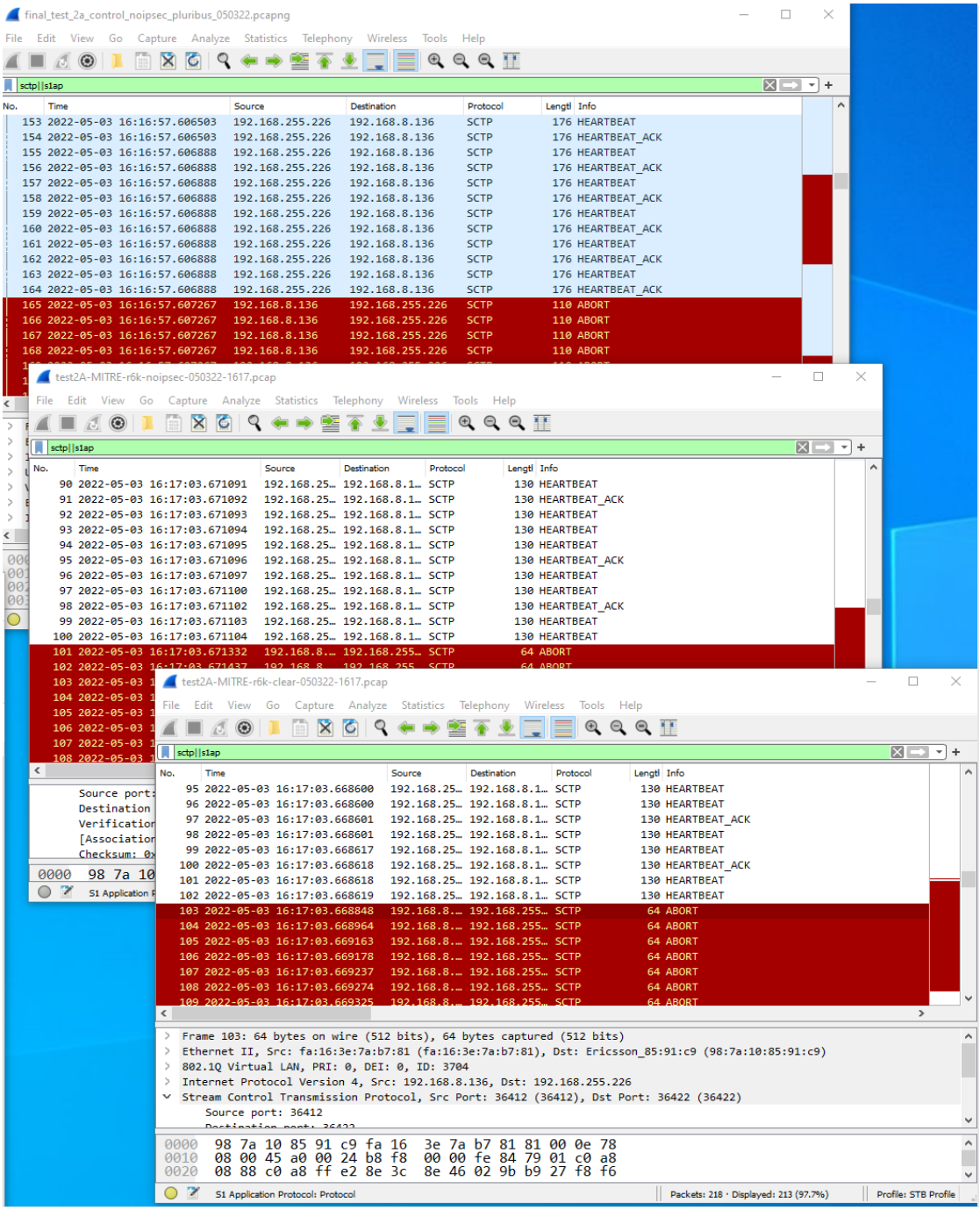


Figure 14: Captured Packets on Core-facing Port of RAN-side Switch; Core-side Untrusted Link; and Core-side Trusted Router without IPsec Encryption on Untrusted Link

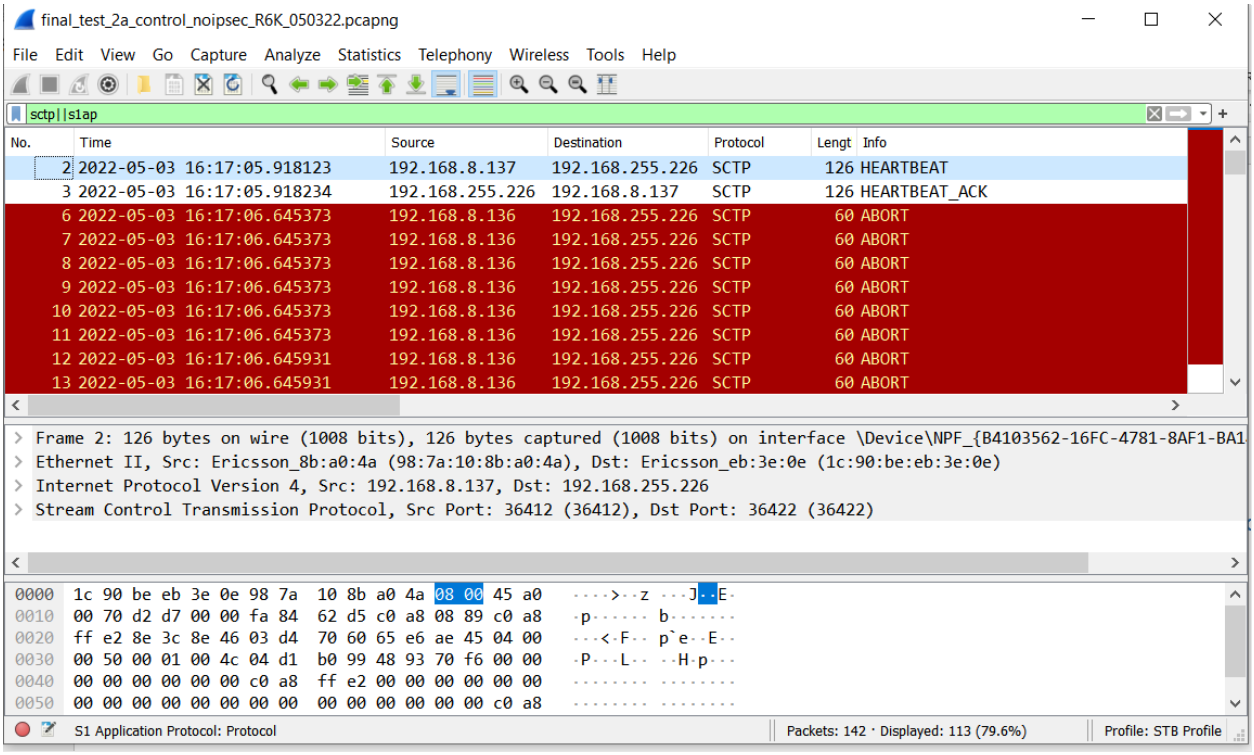


Figure 15: RAN-side Router Capture of Injected Packets

Figure 16 and Figure 17 show the relevant packet captures when the captured packets are modified and injected into the untrusted link when IPsec encrypts traffic in the tunnel. Figure 16 shows the modified packets, the packets injected into the switch (TP3), and the capture from the outgoing port on the switch (TP4). Note that because all of these occur inside the IPsec tunnel, traffic is indistinguishable as it all appears as encrypted packets. There is no indication of what traffic is control plane traffic.

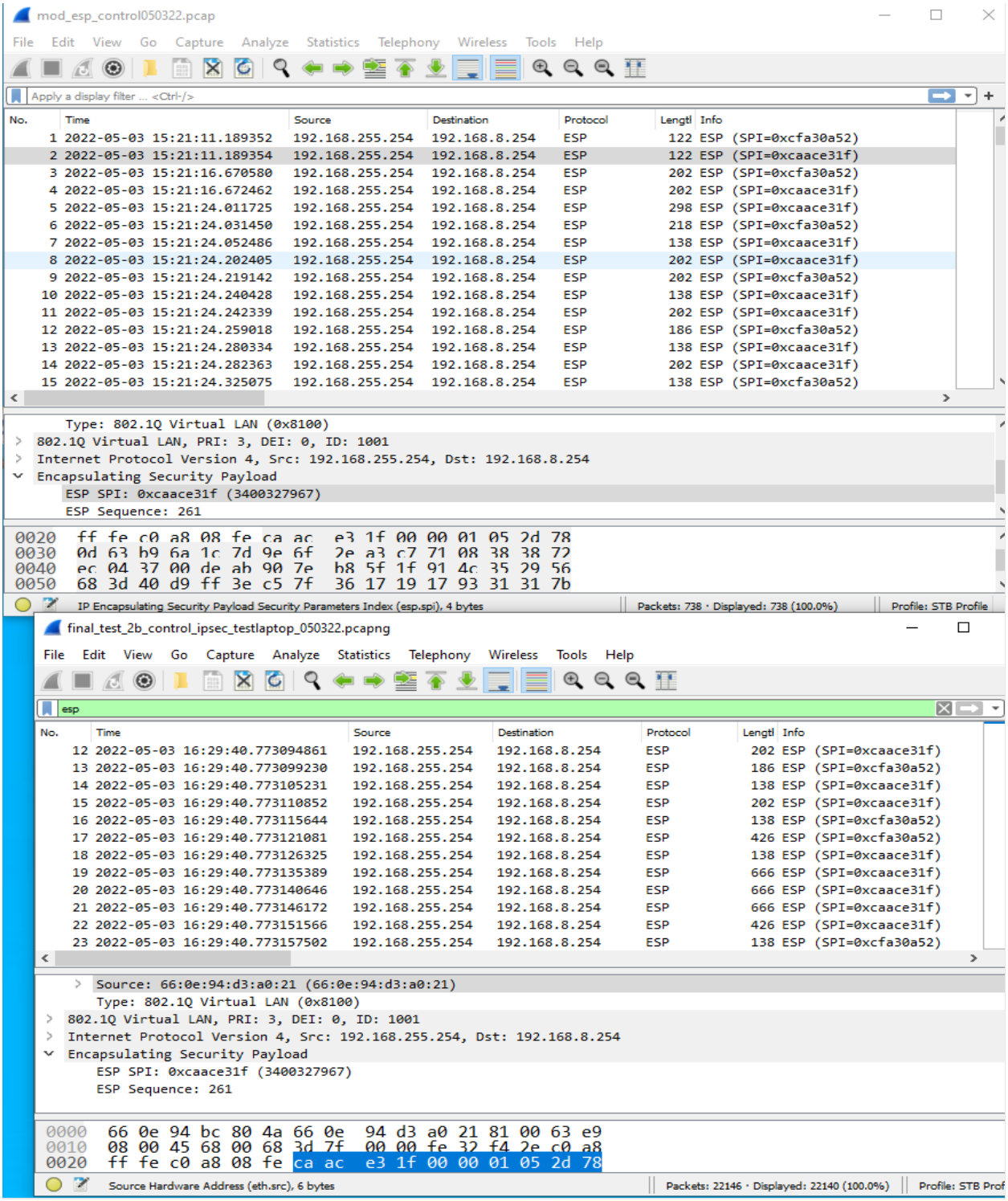


Figure 16: RAN-side Capture of Encrypted Packets, Modified Packets, and Injected Packets on Untrusted Link

Figure 17 shows the packet captures at the core-side router (TP5) as well as on the trusted RAN-side router (TP2). Again, on the untrusted link, we cannot distinguish between the traffic that exists due to control plane messages between the RAN and LTE core and the injected encrypted packets. The decrypted traffic, both at the RAN and at the LTE core show agreement with respect to the control plane traffic. A count of the encrypted packets in the IPsec tunnel, when compared to the unencrypted traffic outside the tunnel indicates the injected packets have been dropped at the tunnel endpoints. Specifically, approximately 20,000 ESP packets (containing control pane traffic) were injected into the transport network, and approximately 14,000 packets were received on the ingress R6K interface at the LTE core. However, only 38 packets were received on the egress R6K interface at the core. Furthermore, of those 38 packets, only 6 were control

packets (as can be seen in Figure 17). Similarly, on the RAN side (TP2), Figure 18 shows that the number of captured control packets when ESP traffic was being injected was 5.

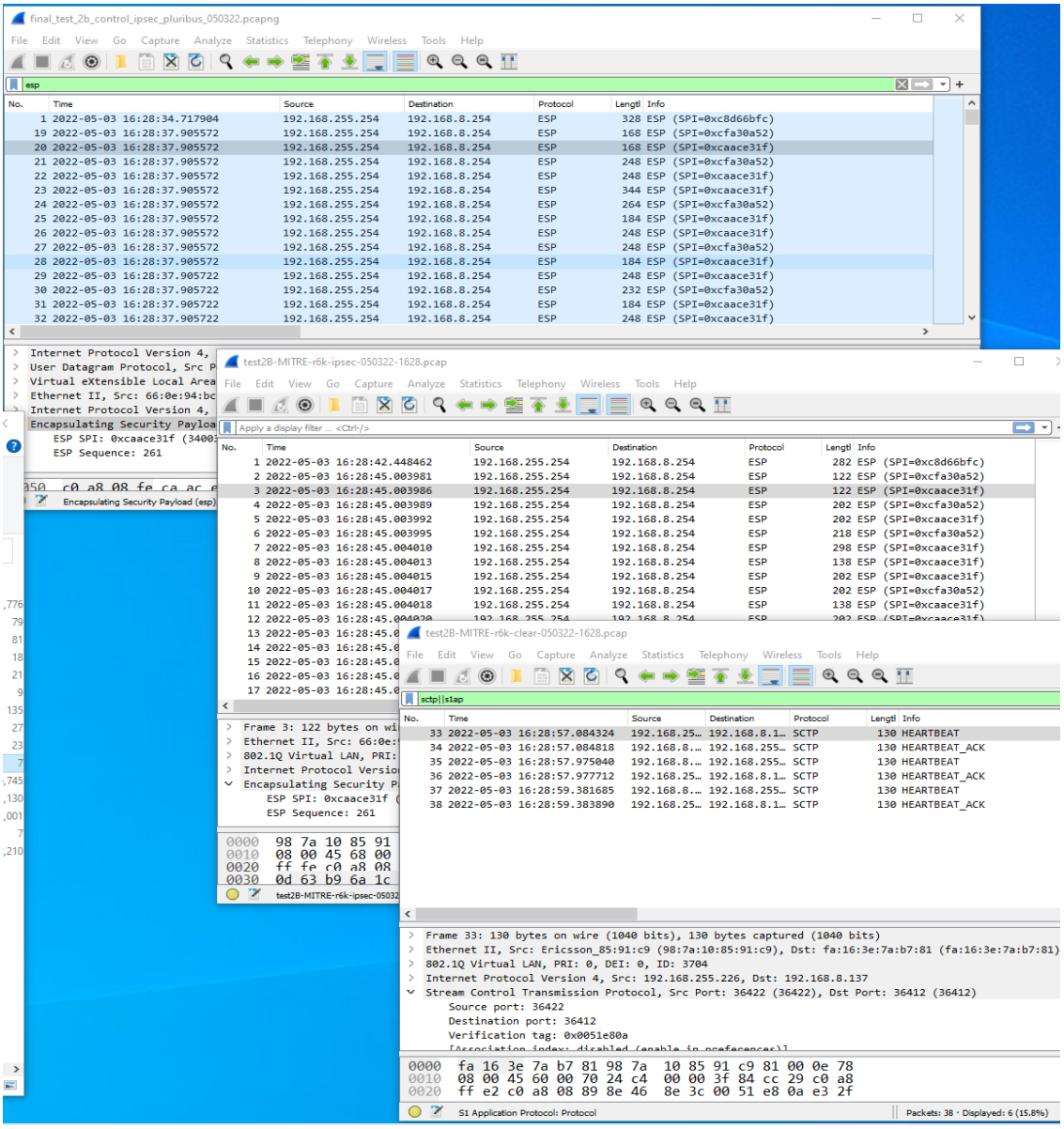


Figure 17: RAN-Side Outgoing Link to Core; Core-Side Untrusted Link Capture of Encrypted Traffic; and Core-Side Capture at Trusted Router after Decryption

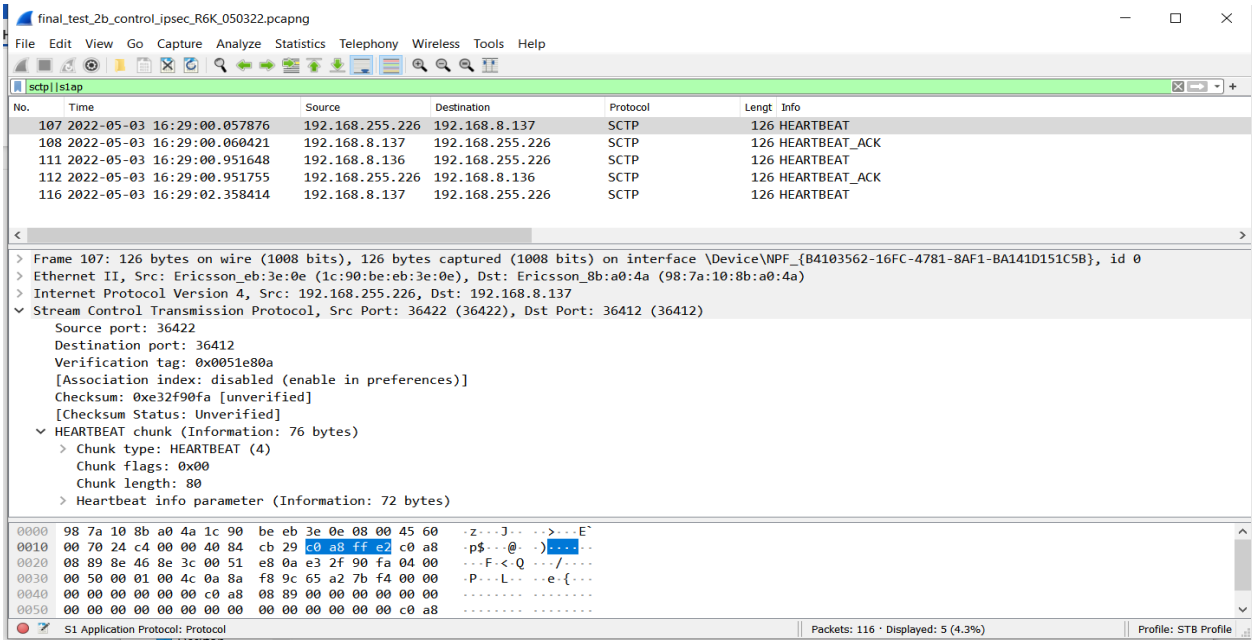


Figure 18: RAN-Side Router Interface Packet Captures of Decrypted Control Traffic

Test Result

Success: When the IPsec tunnel is implemented on the untrusted link, (1) an eavesdropper cannot read the control plane traffic over the link (it all appears as ESP-encrypted packets with source and destination addresses as the endpoints of the tunnel) and (2) modified and injected control packets fail to pass out of the tunnel. When IPsec is not implemented, the contents of the packets on the untrusted link are decipherable. Also, without IPsec encryption, some injected control packets appear to be rejected by the MME as indicated by ABORT messages.

Test Case 3, TC-IPsec-03

The objective of Test Case 3, TC-IPsec-03 is to demonstrate the efficacy of end-to-end TLS encryption over the 5G NSA network.

Objective: Verify inability to eavesdrop, modify, or inject payload on UP

As in previous sections, Table 9 lists the files used to store packet captures where those file names are shown in the headers of the Wireshark windows.

Table 9: Test Case 3 Raw Data Files and Content Descriptions for Runs with and without IPsec Encryption on Untrusted Link

Filename	Contents
test_1a_tls_noipsec_UE-device_050323.pcapng	TLS traffic generated at UE device, captured at TP1
final_test_3a_tls_noipsec_testlaptop_050322.pcapng	Injected traffic without IPsec encryption on the untrusted link, injected at TP3
final_test_3a_tls_noipsec_pluribus_050322.pcapng	Captured injected traffic at TP4 on outgoing interface toward LTE core when traffic is not encrypted on the untrusted link
final_test_3a_tls_noipsec_R6K_050322.pcapng	Traffic captured on ingress interface RAN-side R6K – only TLS traffic generated or received by the UE during this test
test3A-MITRE-r6k-noipsec-050322-1622.pcap	Traffic captured on core-side ingress R6K interface from RAN when traffic is not encrypted on the untrusted link
test3A-MITRE-r6k-clear-050322-1622.pcap	Traffic captured on core-side egress R6K interface toward internet when traffic is not encrypted on the untrusted link
mod_esp_tls050322.pcapng	Modified IPsec-encrypted TLS traffic
final_test_3b_tls_ipsec_testlaptop_050322.pcapng	Injected TLS traffic with IPsec encryption on the untrusted link
final_test_3b_tls_ipsec_pluribus_050322.pcapng	Captured injected TLS traffic on outgoing interface toward LTE core with IPsec encryption on the untrusted link
test3B-MITRE-r6k-ipsec-050322-1630.pcap	IPsec encrypted TLS traffic captured on core-side ingress R6K interface from RAN
test3B-MITRE-r6k-clear-050322-1630.pcap	IPsec decrypted TLS traffic captured on core-side egress R6K interface toward internet
final_test_3b_tls_ipsec_R6K_050322.pcapng	Actual TLS traffic sent/recevied by UE captured at trusted interface of RAN-side R6K

Figure 19 shows the Wireshark windows with the traffic generated at the UE (TP1), injected traffic on the untrusted link (TP3), and traffic captured on the untrusted link as it heads toward the LTE core (TP4). TLS messages appear as TLS in the three packet captures with no ability to look inside to determine the contents. Figure 20 shows the same information captured on the core-side router (TP5). Specifically, 311 injected TLS packets were captured on the ingress R6K router interface at the core, and 376 TLS packets were seen on the egress interface of that router. In contrast, Figure 21 shows that only three TLS packets were generated by the UE and one TLS packet was received by the UE (identified by IP address 172.18.0.3), suggesting that the many

other packets observed in Figure 19 and Figure 20 were dropped due to being malformed encrypted packets injected as part of the test.

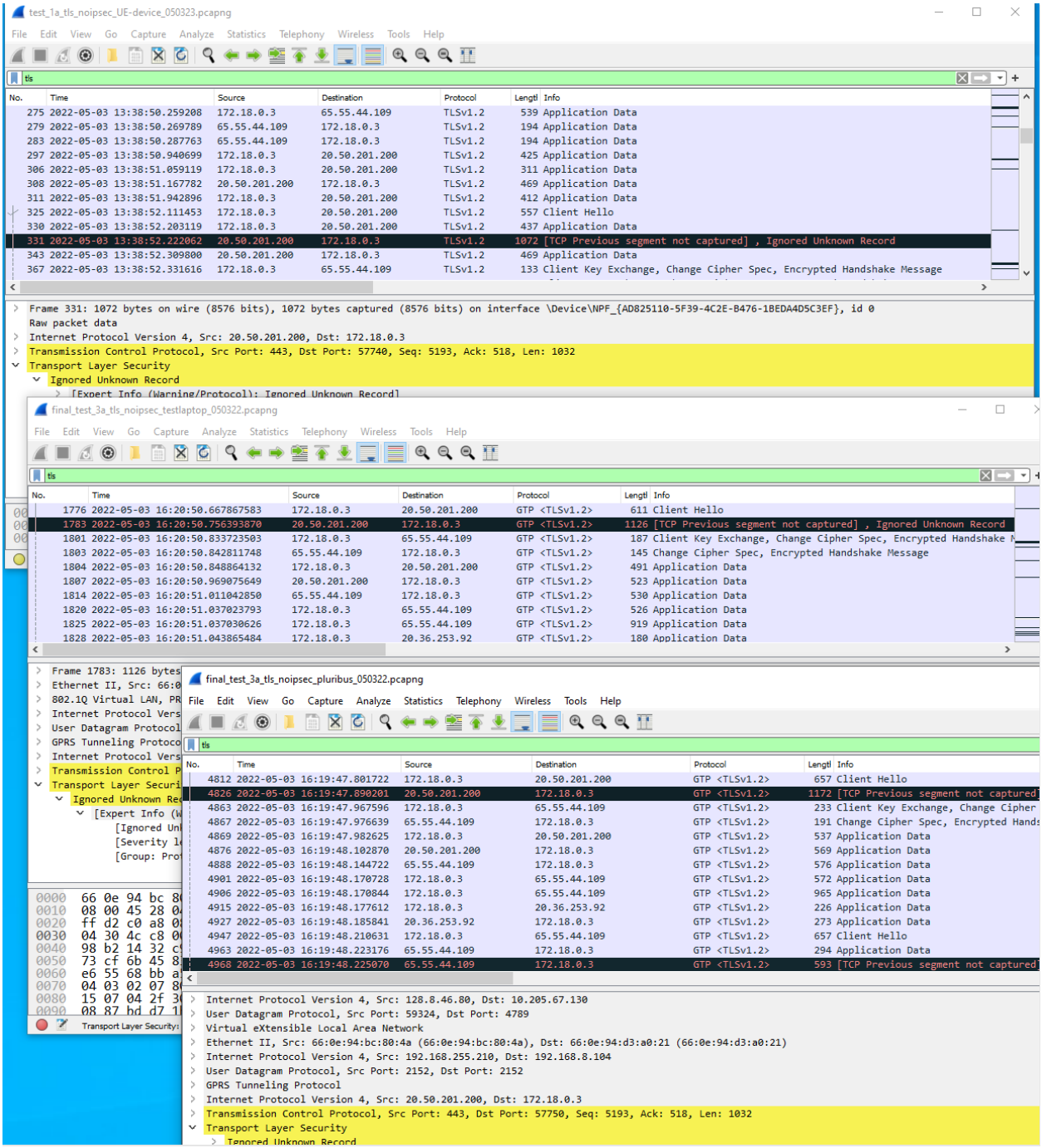


Figure 19: Capture of TLS-Encrypted Packets at UE, Injected/Modified Packets on Untrusted Link, and Capture of Packets on Outgoing Link to Core without IPsec Tunnel on Untrusted Link

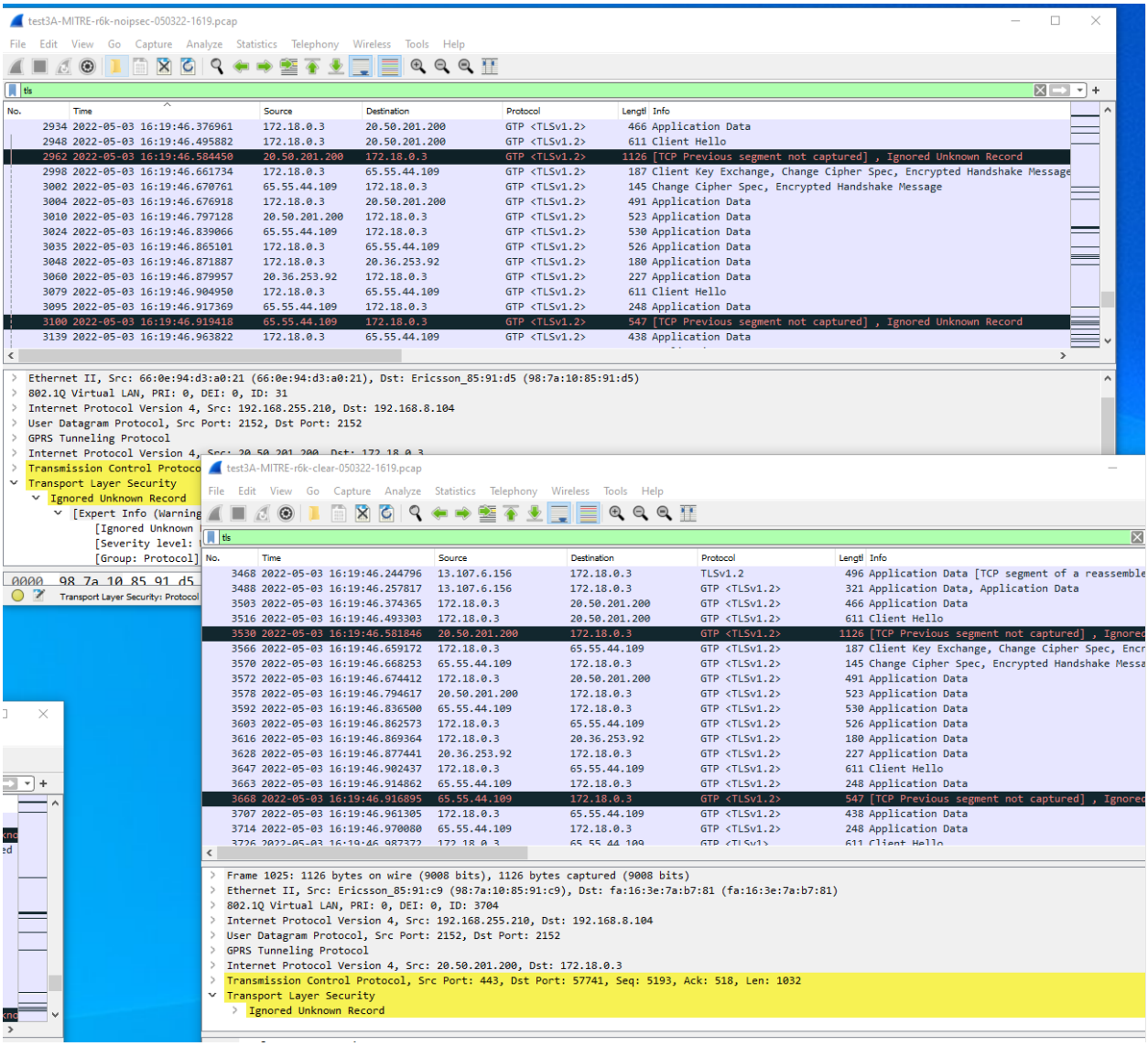


Figure 20: Capture of TLS-Encrypted Packets at Core-Side Router Interfaces without IPsec Tunnel on Untrusted Link

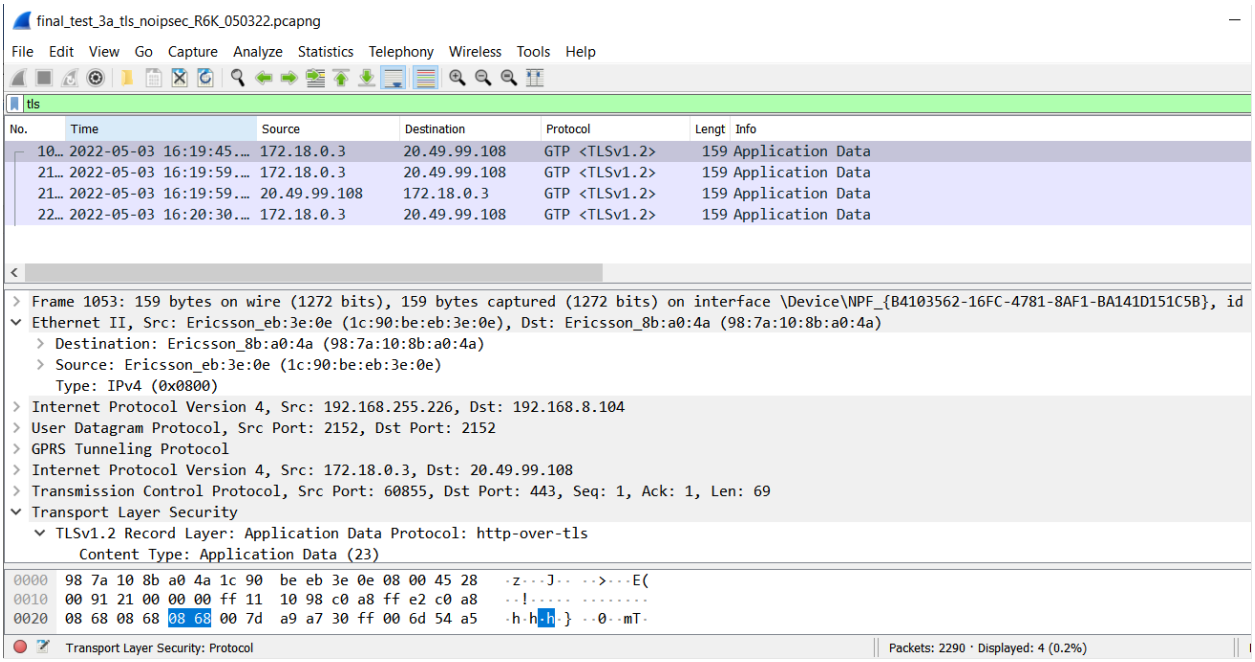


Figure 21: Capture of TLS-encrypted Packets on RAN-side Router Ingress Showing the Only Traffic Generated/Received by the UE for this Test

As described above, for the tests with IPsec encryption of TLS packets, over 1,000 packets were generated in order to clearly distinguish that injected packets are dropped inside the tunnel. Figure 22 shows the modified and injected IPsec-encrypted packets as well as the corresponding capture of those packets on the outgoing link toward the LTE core. As with the prior tests with IPsec encryption, we only see that the packets are ESP packets with sources and destinations the endpoints of the IPsec tunnel. These captured packets include user traffic and control traffic, where some of the UP packets are TLS packets, although it is impossible to distinguish which are which. Further, the payloads of all packets are not decipherable. Approximately 4,500 modified ESP packets were injected into the transport network.

Figure 23 shows a capture of these packets, both on the RAN-facing interface of the core-side router (where traffic is IPsec encrypted) and on the egress interface of the core-side router, after decryption (both TP5). There is a notable difference in traffic volume. Specifically, approximately 4,600 ESP packets were received on the RAN-facing interface, whereas only 33 packets successfully exit (or enter) the tunnel. Only three of those packets are TLS packets. Figure 24 shows the same three TLS packets on the clear (unencrypted) interface of the RAN-side router (TP2).

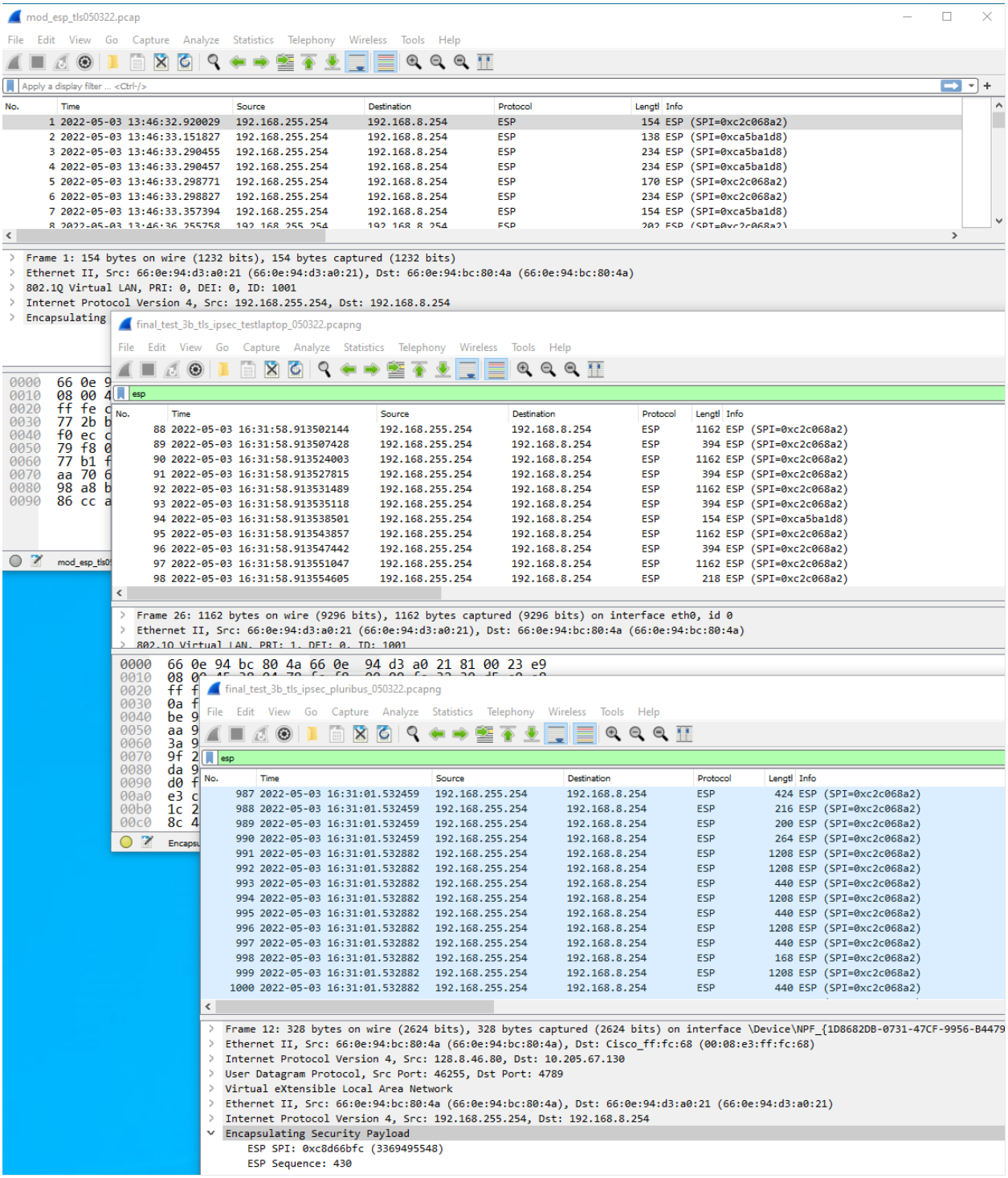


Figure 22: Capture of Modified and Injected TLS-Encrypted Packets on Untrusted Link and Capture of Packets on Outgoing Link to Core with IPsec Tunnel on Untrusted Link

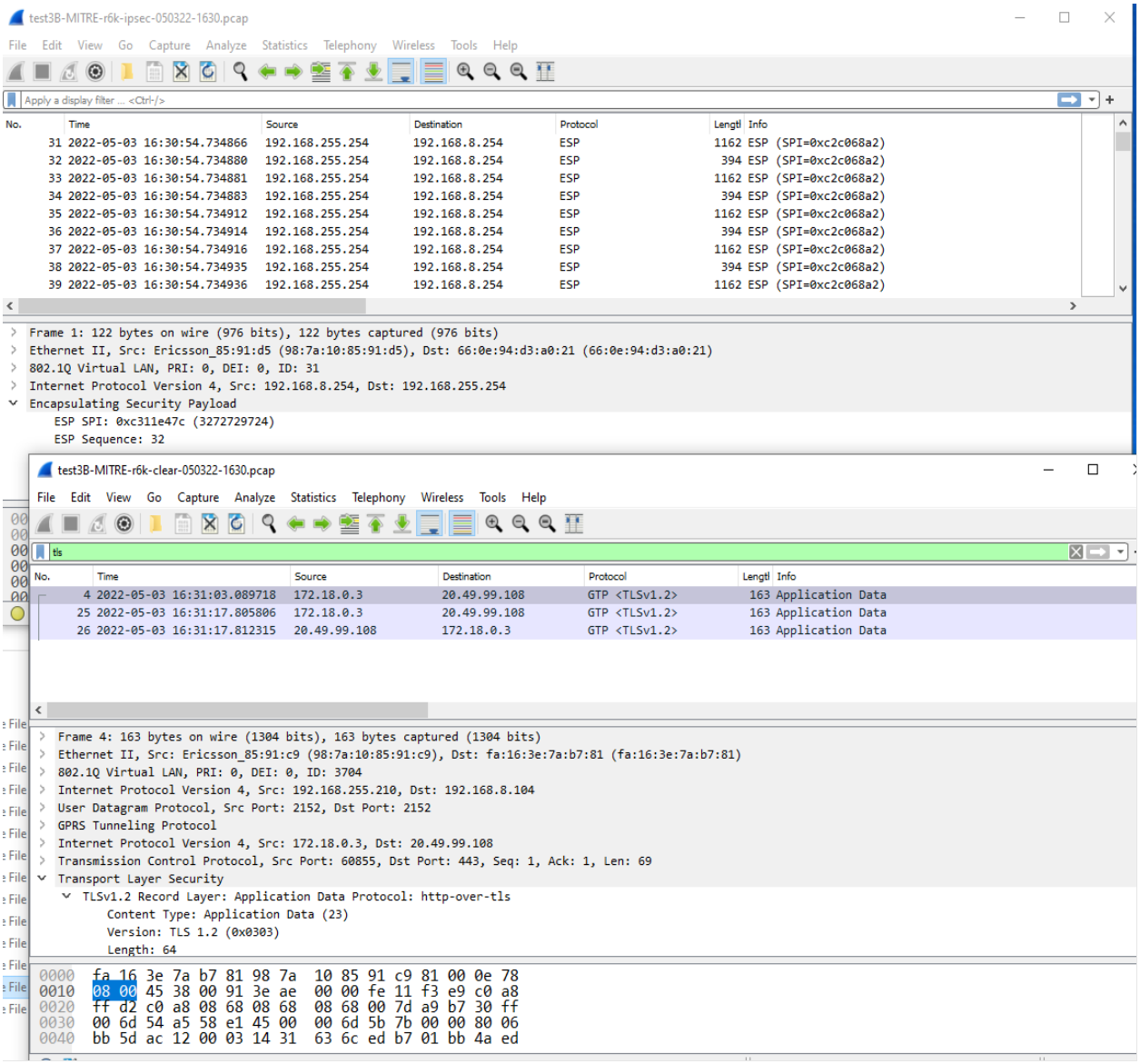


Figure 23: Captures of TLS-Encrypted Packets on Core-Side Untrusted Link and On Trusted Router After Decryption of IPsec

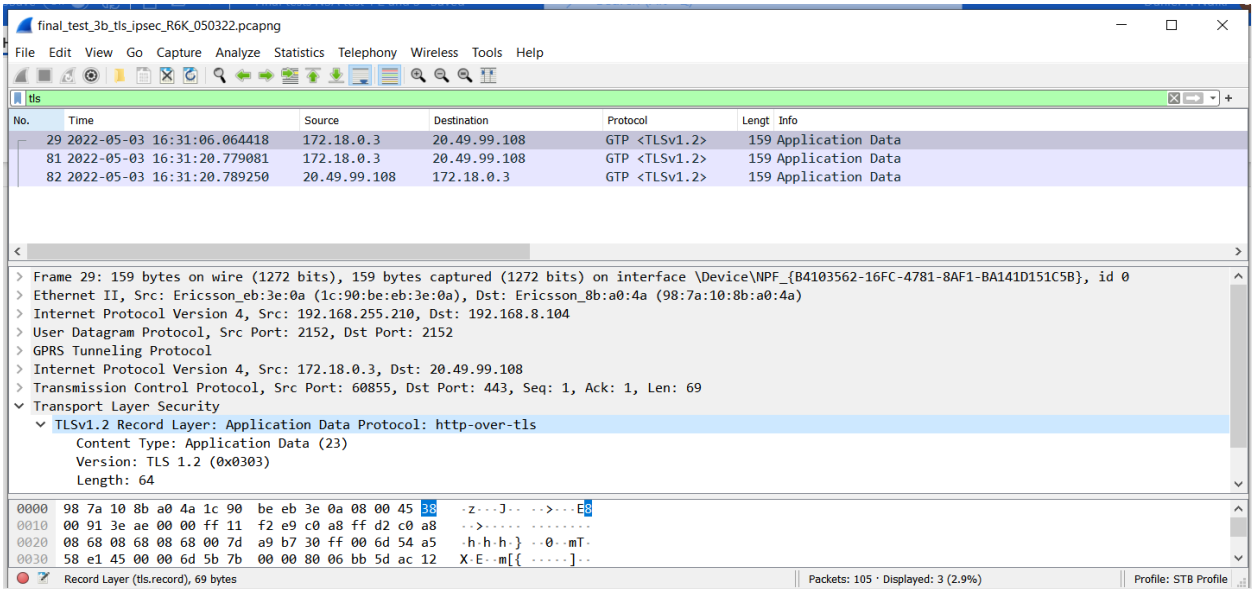


Figure 24: Capture of TLS-Encrypted Packets on RAN-Side Router Ingress Showing the Only Traffic Generated/Received by the UE for This Test with IPsec Tunnel

Test Result

Success: TLS-encrypted traffic is unreadable with or without IPsec encryption; this includes all capture points, not just those on the untrusted link. Adding IPsec to the untrusted link further obscures the traffic, preventing an eavesdropper from reading the source and destination of the TLS messages, as well as knowing that the encapsulated packets are TLS encrypted. In addition, TLS encryption and IPsec encryption prevent injection or modification of packets. Whereas, without the IPsec tunnel, injected TLS packets pass out of the cellular network to be dropped by either the UE or the HTTPS server, when the IPsec tunnel is enabled, that injected traffic is dropped at the tunnel endpoints and not allowed to flow to other parts of the larger network.

Conclusions and Next Steps

For each of the three test cases described here, the tests successfully verified the efficacy of employing security procedures recommended by the CSRIC VII WG2 report, implementing commercial hardware in a commercially-relevant NSA configuration. This verification of the CSRIC NSA recommendations in a commercially-deployed environment is the first of its kind. Test Cases 1 and 2 focused on confidentiality and integrity on an untrusted backhaul link for user traffic and control traffic, respectively. Test Case 3 added end-to-end TLS encryption between an application on the UE and a server on the internet.

Test Case 1 demonstrated that implementation of an IPsec tunnel over the untrusted link prevents eavesdropping on user traffic as well as modification and injection of false traffic designed to appear as originating from or destined to a valid UE. All traffic on the untrusted link

appeared as encrypted ESP packets with no ability to read the contents. Modified and injected packets were observed at test points on the untrusted link, but were dropped inside the tunnel and did not reach either the UE or the internet. Furthermore, in absence of that IPsec tunnel, packet contents and headers were fully decipherable, and modified and injected UP packets were able to reach destinations outside the untrusted link, including the UE and the internet.

Test Case 2 demonstrated that implementation of an IPsec tunnel over the untrusted link prevents eavesdropping on control traffic as well as modification and injection of false traffic designed to appear as originating from the UE, RAN, or MME. As with Test Case 1, all traffic on the untrusted link appeared as encrypted ESP packets with no ability to read the contents. Modified and injected packets were observed at test points on the untrusted link, but were dropped inside the tunnel and did not reach either the UE, RAN, or the MME. Furthermore, in absence of that IPsec tunnel, packet contents and headers were fully decipherable. While modified and injected CP packets were able to reach destinations outside the untrusted link, including the RAN and the MME, that traffic also generated ABORT messages, suggesting that other protocols within the system identified the injected packets as problematic. The exact cause of those ABORT messages was not investigated.

Test Case 3 demonstrated that end-to-end TLS encryption further occludes user traffic between the UE and a server, or other endpoint. The TLS encryption prevented eavesdropping and modification and injection of packets, regardless of the implementation of an IPsec tunnel on the untrusted link, although that protection only exists for the user traffic that is sent between the addresses that set up the encrypted connection. The TLS encryption also protects the associated traffic at points outside the untrusted link, including what is transmitted over the air between the UE and the RAN.

The three successful test cases outlined above conclude the inaugural tests of the 5G Security Test Bed, an industry effort to improve 5G network security through collaboration with government agencies, policymakers, international standards bodies, thought leaders, and partners. While these tests focused on a 5G non-standalone network architecture, with the 5G network built over a 4G LTE core, future steps include implementation and testing of CSRIC VII WG2 recommendations for a 5G standalone configuration, utilizing an Ericsson Release 16 Dual Mode Core. The 5G STB is also in the process of developing test cases for network slicing and roaming security use cases. In addition, the method the 5G STB uses for IPsec tunneling will be modified to utilize PKI certificates.

The 5G STB members and administrator welcome engagement from stakeholders with an interest in the mission of the 5G Security, and we expect new participants and the diversity of test cases to grow in tandem.

Appendix: Acronyms

3GPP	3rd Generation Partnership Project
5G STB	5G Security Test Bed
BBU	Baseband Unit
CP	Control Plane
CPE	Customer Premise Equipment
CSRIC	Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
eNB/eNodeB	Evolved Node B
EN-DC	E-UTRA New Radio – Dual Connectivity
EPG	Evolved Packet Gateway
ESP	Encapsulating Security Payload
E-UTRA	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
gNB/gNodeB	Next Generation Node B
HSS	Home Subscriber Server
IKEv2	Internet Key Exchange Protocol Version 2
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
LTE	Long Term Evolution
MACsec	Media Access Control Security
MME	Mobility Management Entity
NIST	National Institute of Standards and Technology
NMS	Network Management System
NR	New Radio
PGW	Packet Data Network Gateway
RAN	Radio Access Network
RAT	Radio Access Technology
SEG	Security Gateway
SGW	Serving Gateway
STB	Security Test Bed
TAS	Telecom Application Server
TDD	Time Division Duplex
TLS	Transport Layer Security
TP	Test Point

UE	User Equipment
UMD	University of Maryland
UP	User Plane
UPF	User Plane Function
VPN	Virtual Private Network
WG	Working Group

References

Communications Security, Reliability, and Interoperability Council (CSRIC) VII Working Group 2 (WG2), Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture (Dec. 2020), https://www.fcc.gov/file/20181/download.

CSRIC VII WG3, Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards (Sept. 16, 2020), https://www.fcc.gov/file/19297/download.

CSRIC V WG6, Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network, (Sept. 2016). https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx .

Jon Metzler, Security Implications of 5G Networks, UC Berkeley Center for Long-Term Cybersecurity at 7 (Sept. 2020), https://cltc.berkeley.edu/wp-content/uploads/2020/09/Security_Implications_5G.pdf.

IETF Datatracker, Request for Comment (RFC) 4303 (Dec. 2005), https://datatracker.ietf.org/doc/html/rfc4303.

3GPP Portal, Technical Specification (TS) 33.210 (last updated Dec. 23, 2021), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279.

3GPP Portal, TS 33.310 (last updated Mar. 24, 2022), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2293.

3GPP Portal, TS 33.401 (last updated Mar. 24, 2022), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296.

3GPP Portal, TS 33.501 (last updated Mar. 24, 2022), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.