Cryptool2

1. zadatak

(na fakultetu)

Text input - unos poruke koja se sifruje

Text input - 32bitni heksadecimalni key

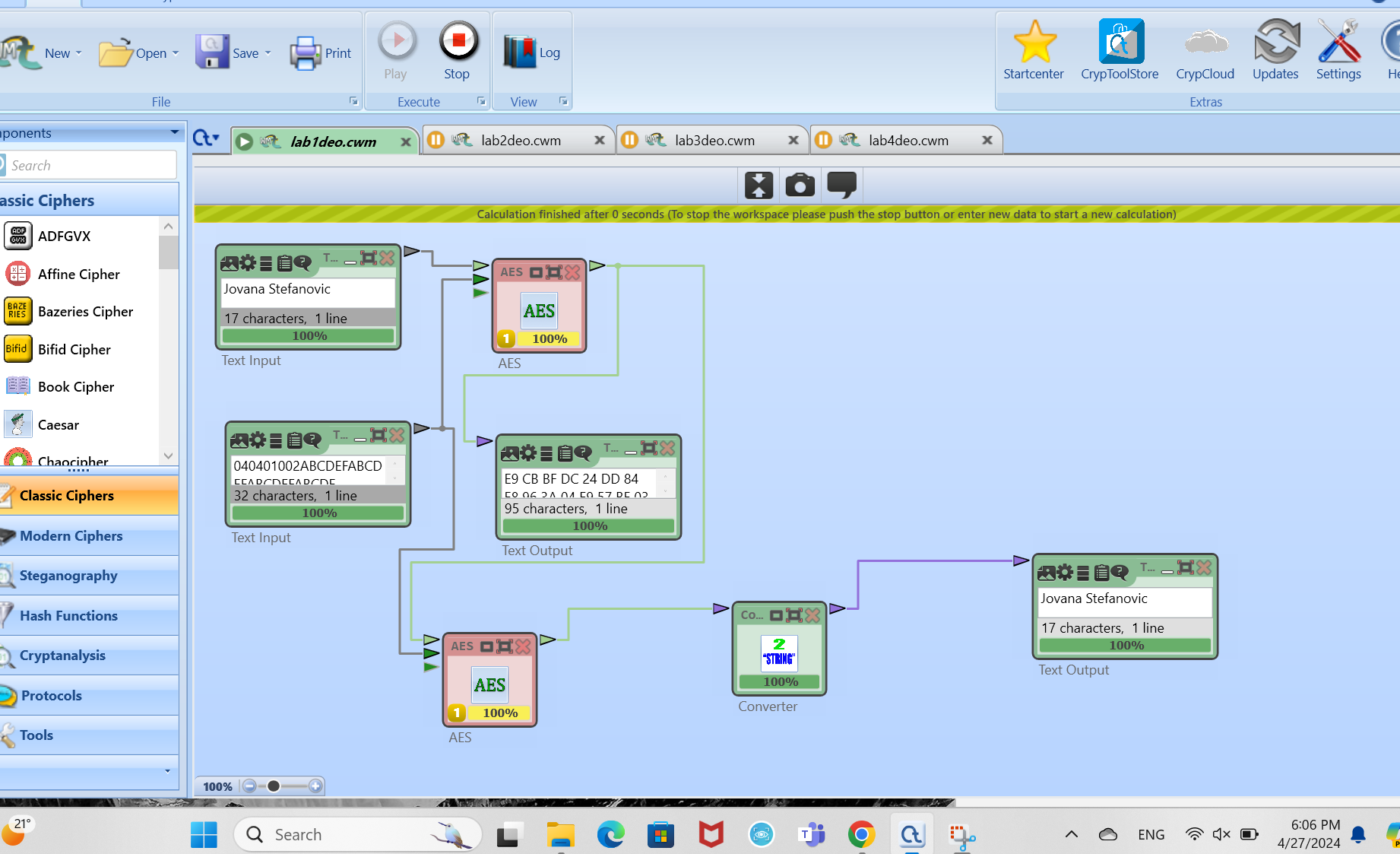
AES - key size 128, enkriptuje, ECB

AES - key size 128, dekriptuje, ECB

Text output - sifrovana poruka

Converter - konvertuje iz heksadecimalnog broja u tekst

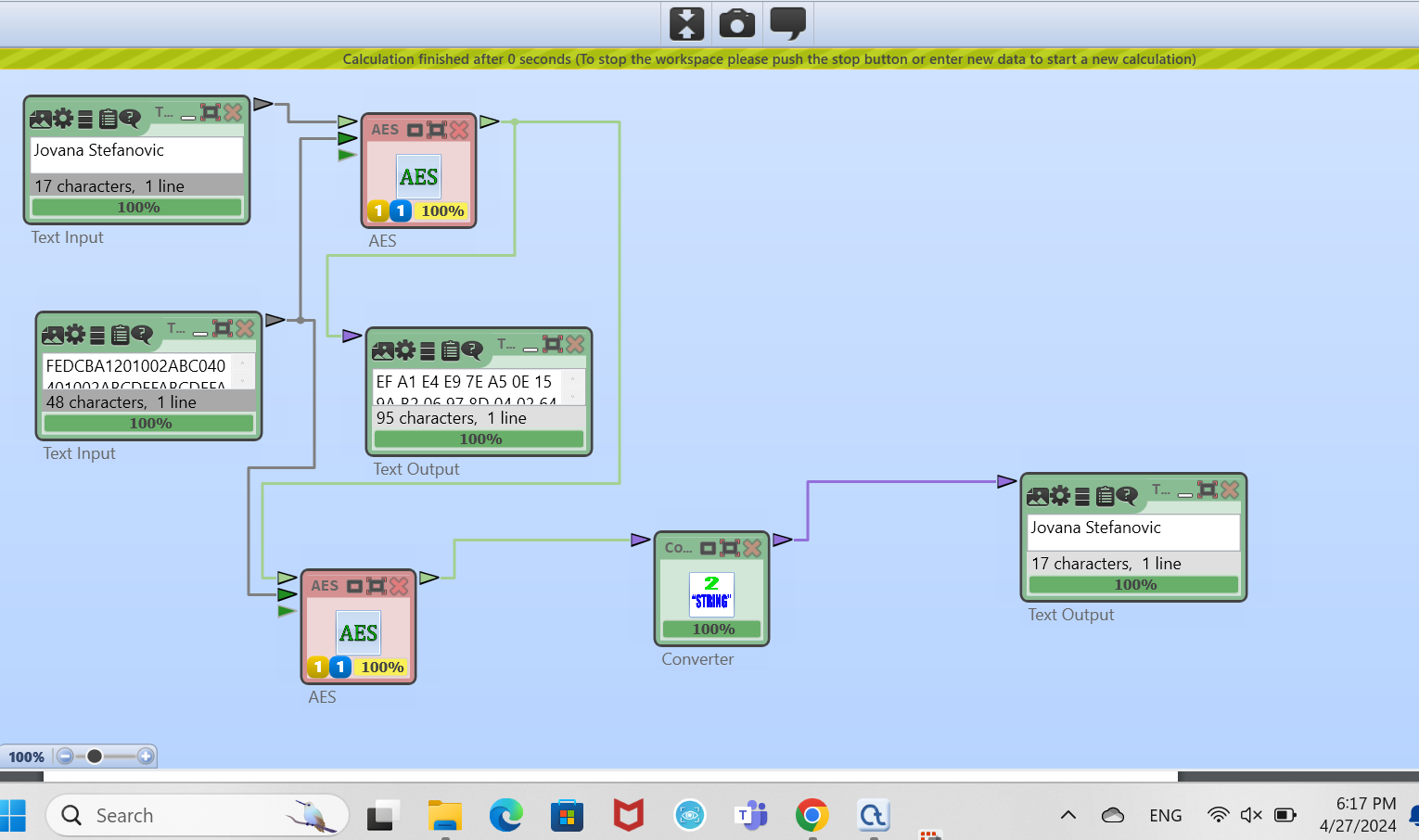
Text output - poruka



Prvo trebate generisati ključ koji će se koristiti za šifrovanje i dešifrovanje poruka. Ključ treba da bude dovoljno dug i nasumičan kako bi bio siguran. Za AES, dužina ključa može biti 128, 192 ili 256 bita, u zavisnosti od željene sigurnosti.

Režim rada ECB (Electronic Codebook) je jedan od osnovnih režima rada simetričnih blok šifri, uključujući AES. U ovom režimu, svaki blok otvorenog teksta se šifruje nezavisno od drugih blokova, što znači da isti blok otvorenog teksta uvek će se mapirati na isti šifrovani blok. Ovo može dovesti do određenih sigurnosnih problema, jer ne dopušta šifrovanje istog otvorenog teksta na različite načine, što može olakšati napade.

(domaci)



U AES je promenjena duzina kljuca na 192, pa nam je bio potreban 48 heksadecimalni broj. Izabrala sam CBC rezim rada.

Režim rada CBC (Cipher Block Chaining) je popularan režim rada simetričnog blok šifrovanja, koji pruža veću sigurnost od ECB režima rada. U ovom režimu, svaki blok šifrovanih podataka XOR-uje se sa prethodno šifrovanim blokom pre nego što se šifruje. Ovo osigurava da isti blok otvorenog teksta šifruje na različite načine, što smanjuje rizik od određenih napada.

1. zadatak

(na fakultetu)

Text input - poruka koja se sifruje

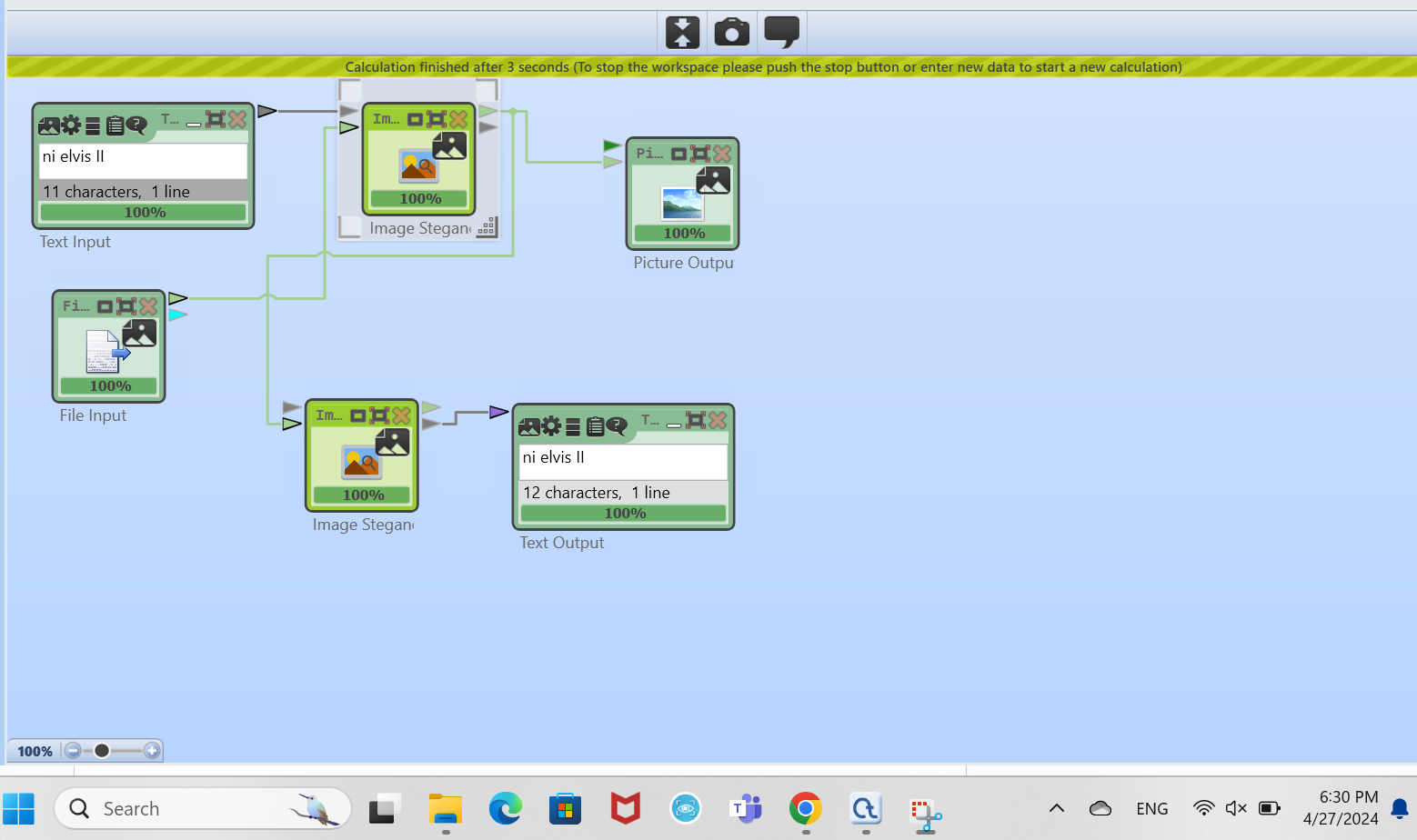
File input - fajl u koji se umece poruka, jpg slika

Image steganography - LSB steganography, hide

Picture output - slika u koju je umetnuta poruka

Image steganography - extract

Text output - ekstraktovana poruka



LSB (Least Significant Bit) steganografija je tehnika koja se koristi za skrivanje informacija unutar digitalnih medija, poput slika, zvukova ili video zapisa, tako što se informacije inkorporiraju u najmanje značajne bitove (obično poslednje bitove) piksela ili uzoraka. Ova tehnika je popularna zbog svoje jednostavnosti i efikasnosti, ali ima ograničenja. Glavno ograničenje je što se sakrivene informacije mogu relativno lako otkriti uz pomoć analize statističkih karakteristika slike. Takođe, ako se slika kompresuje ili se vrši neka druga obrada, informacije mogu biti oštećene ili izgubljene.

(domaci)

BPCS (Bit-Plane Complexity Segmentation) steganografija je tehnika koja se koristi za skrivanje informacija unutar digitalnih slika. Za razliku od LSB steganografije koja koristi najmanje značajne bitove piksela, BPCS steganografija se fokusira na segmentaciju slike na osnovu složenosti bitova na različitim nivoima bitova.

BPCS steganografija može pružiti veću sigurnost od LSB steganografije jer koristi složenost bitova za odabir segmenata za sakrivanje informacija. Međutim, implementacija ove tehnike može biti složenija i zahtevnija u poređenju sa LSB steganografijom.



1. Zadatak

(na fakultetu)

Text input - poruka koja se sifruje

RSA key generator

RSA - enkriptuje

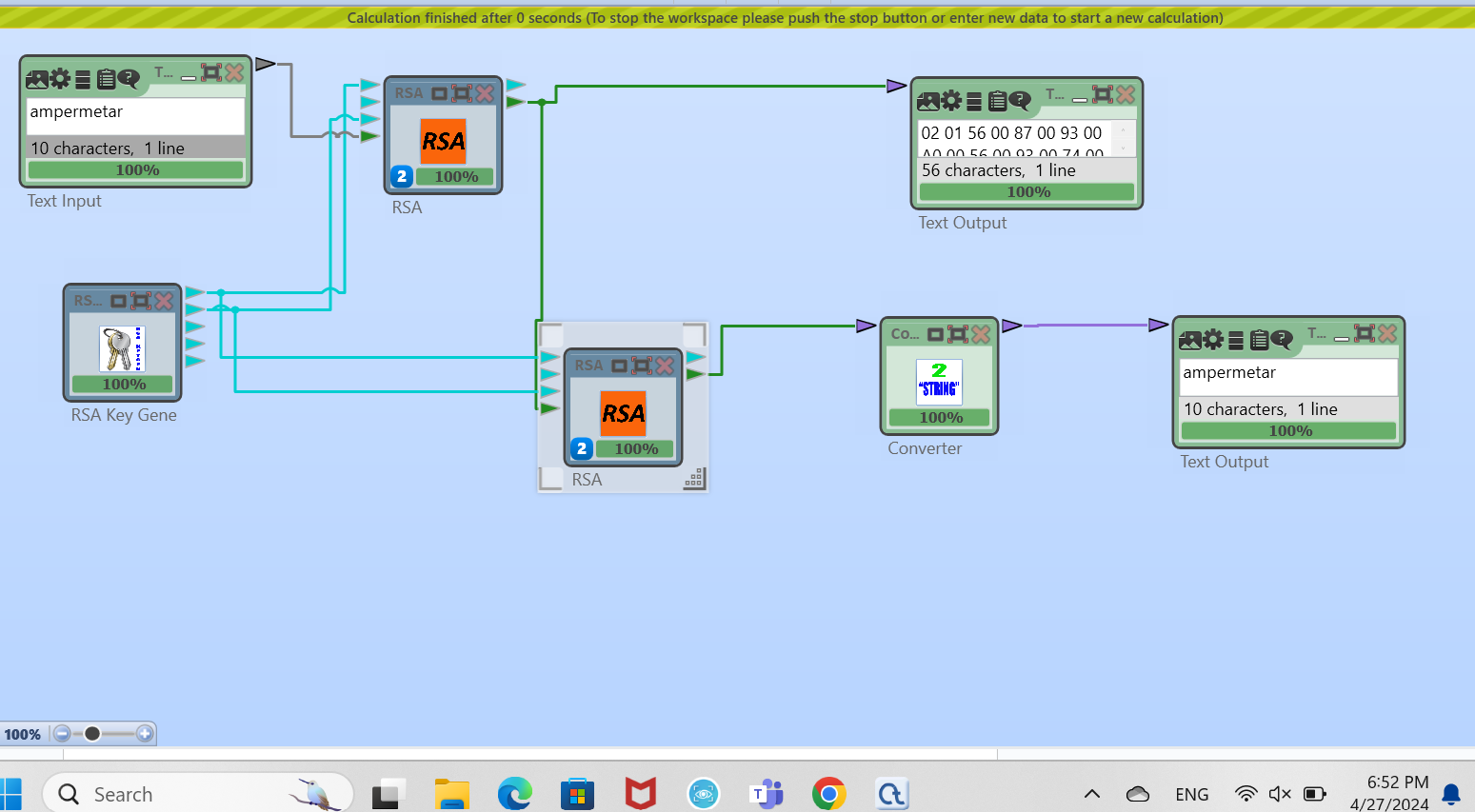
Text output -

RSA - dekriptuje

Converter - konvertuje iz heksadecimalno

Text output - poruka

RSA (Rivest-Shamir-Adleman) je jedan od najpoznatijih algoritama kriptografije sa javnim ključem. On se koristi za enkripciju, digitalno potpisivanje i razmenu ključeva. RSA se zasniva na težini faktorizacije velikih brojeva, što znači da je sigurnost algoritma zasnovana na teškoći faktorizacije proizvoda dva velika prostog broja.



(domaci)

According to the author of CrypTool2 , the purpose of the tool is to introduce the concept of cryptography through E-Learning, and not to provide a full fledged crypto library for application development.

U dokumentaciji <https://www.cryptool.org/en/functions/> DSA I ECDSA NISU DOSTUPNI U CRYPTOOL2

DSA je algoritam digitalnog potpisa koji se zasniva na aritmetici sa velikim brojevima. Koristi se za generisanje i verifikaciju potpisa koji su vezani za određeni skup podataka, omogućavajući identifikaciju autentičnosti i integriteta podataka. ECDSA, s druge strane, koristi eliptičke krive za generisanje ključeva i potpisa, što ga čini efikasnijim u poređenju sa DSA kada su u pitanju dužine ključeva.

1. zadatak

(na fakultetu)

Text input - poruka koja se sifruje

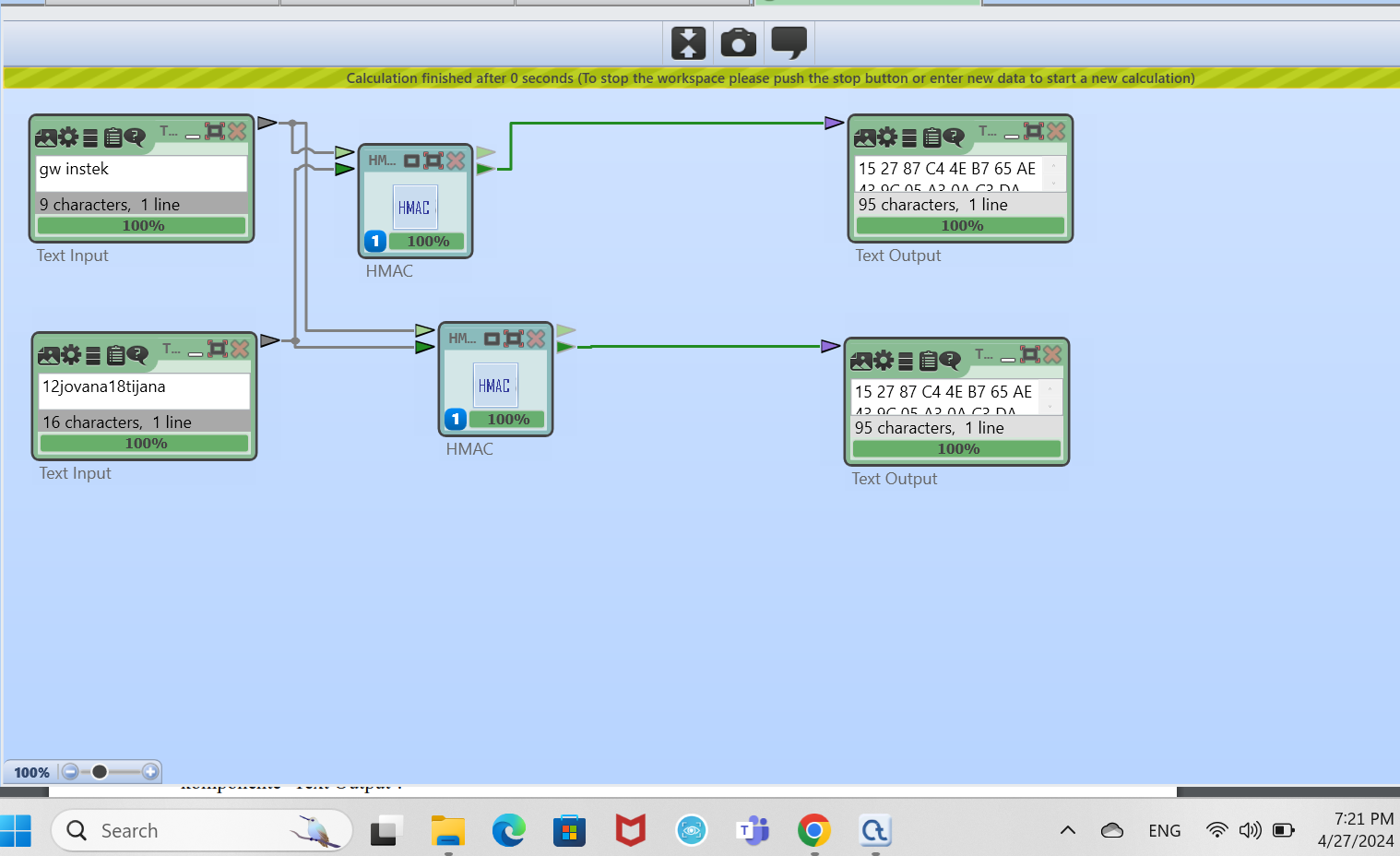
HMAC - sha 256

Text output- hash poruke

Text input - kljuc

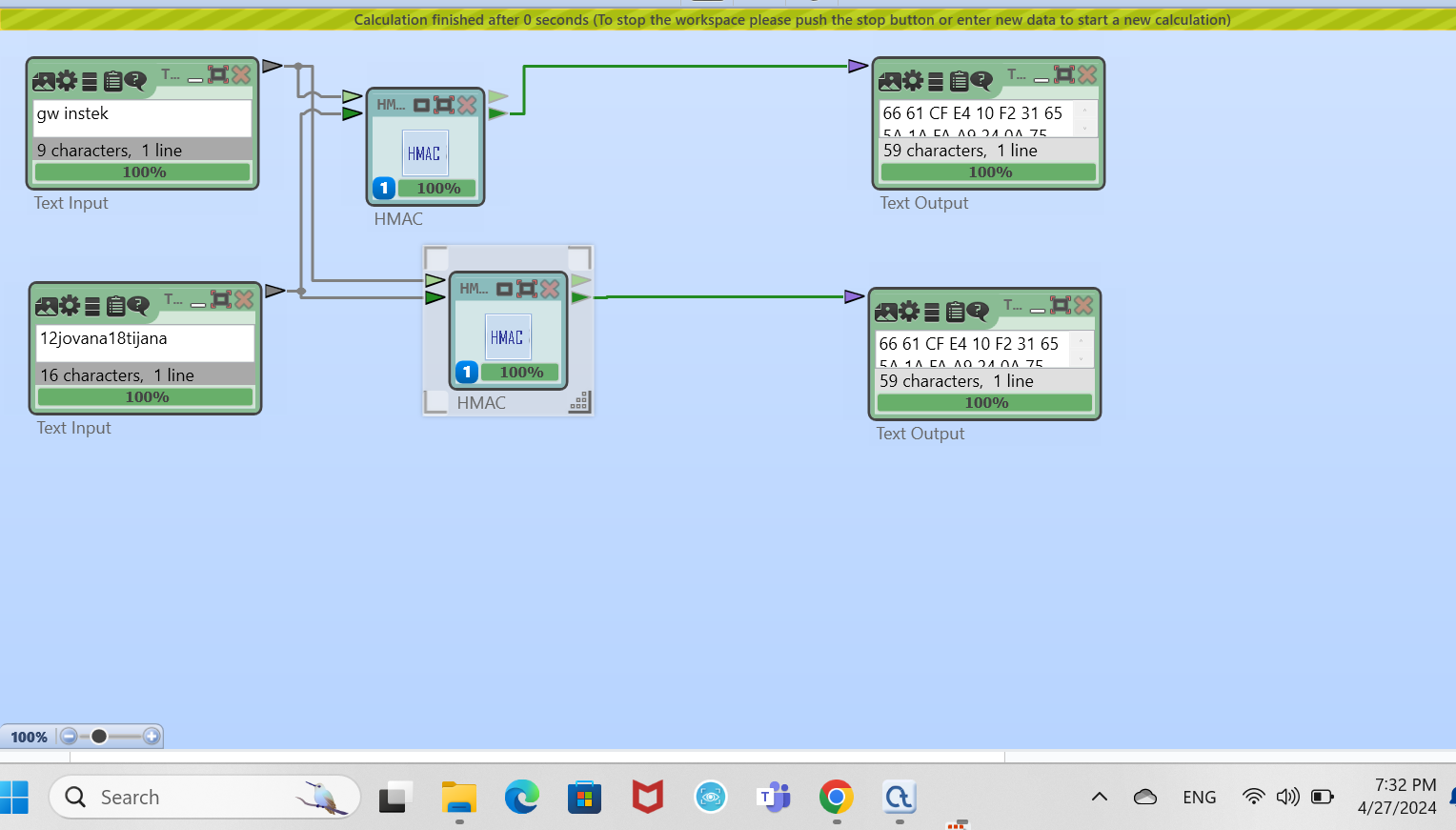
HMAC - sha 256

Text output - hash, koji je isti kao 1. Sto znaci da je dobro



HMAC (Hash-based Message Authentication Code) je algoritam za autentikaciju poruka koji se koristi za proveru autentičnosti i integriteta podataka. On se zasniva na kombinaciji kriptografske heš funkcije i tajnog ključa. HMAC omogućava generisanje kratke, fiksne veličine koda koji se može koristiti za verifikaciju autentičnosti i integriteta poruke.

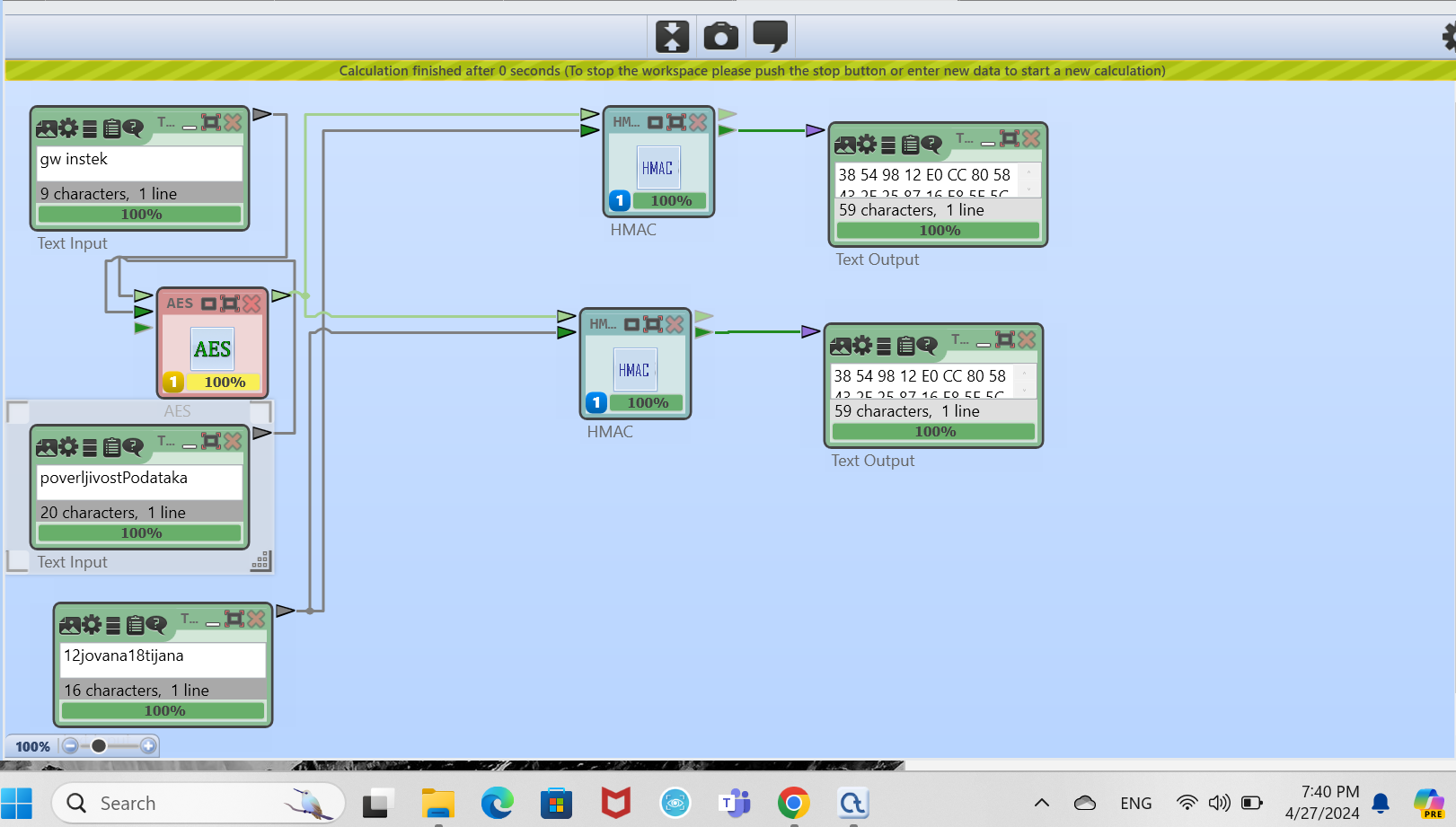
(domaci)



Ovde je koriscen SHA-1

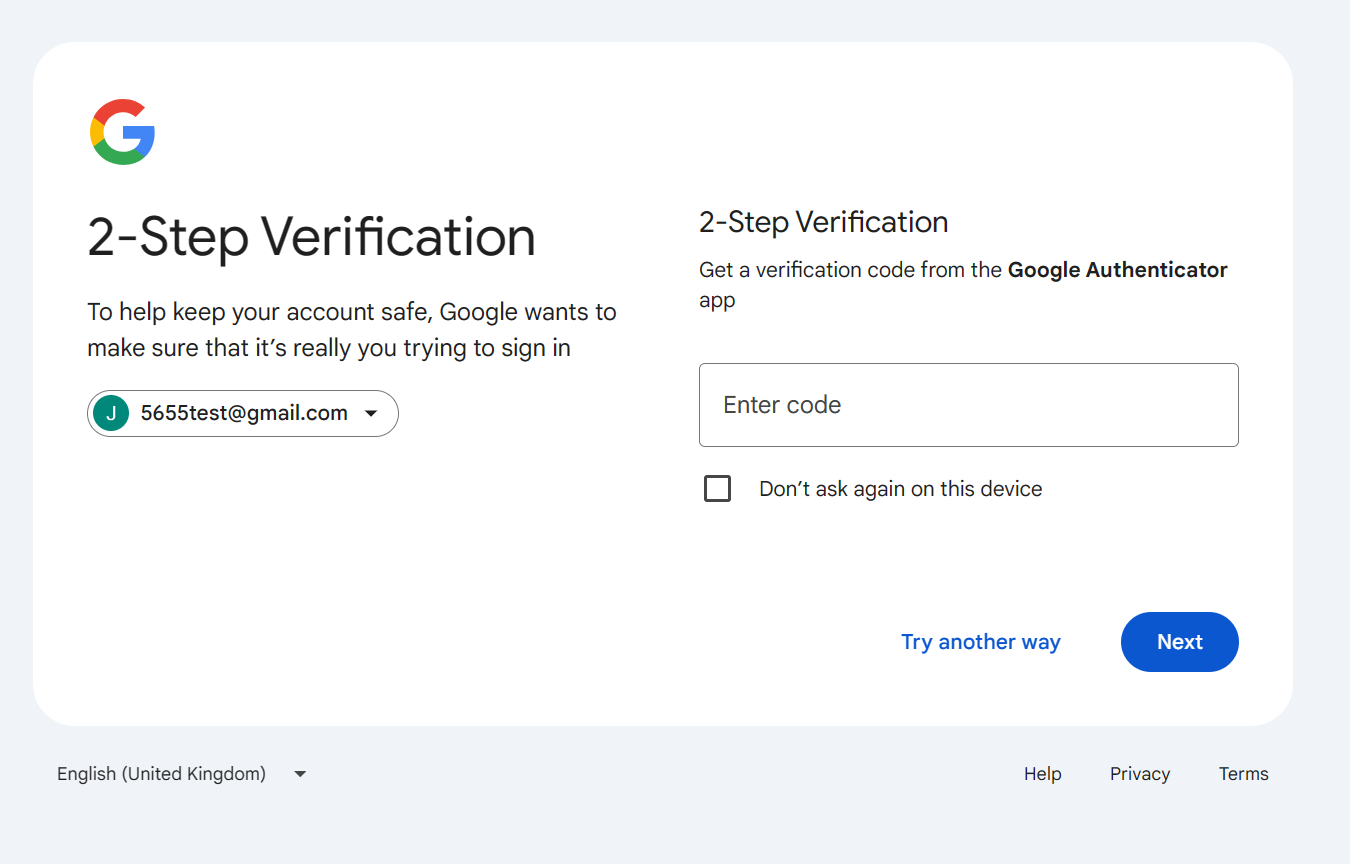
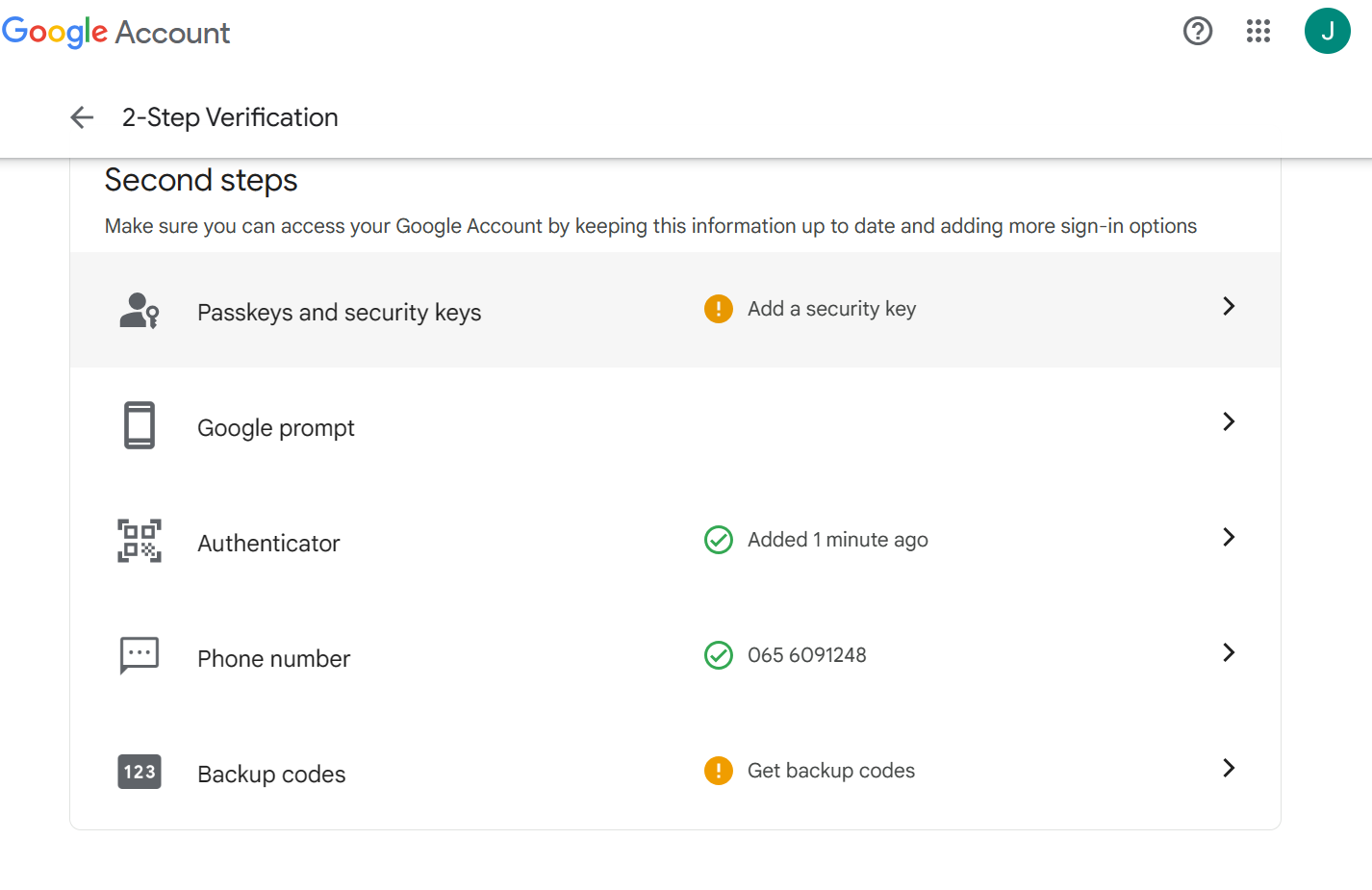
SHA-1 (Secure Hash Algorithm 1) i SHA-256 (Secure Hash Algorithm 256) su dve različite verzije kriptografske heš funkcije iz SHA porodice. Obe funkcije koriste algoritam za generisanje heševa od ulaznih podataka, ali se razlikuju u dužini heševa i nivou sigurnosti koji pružaju.

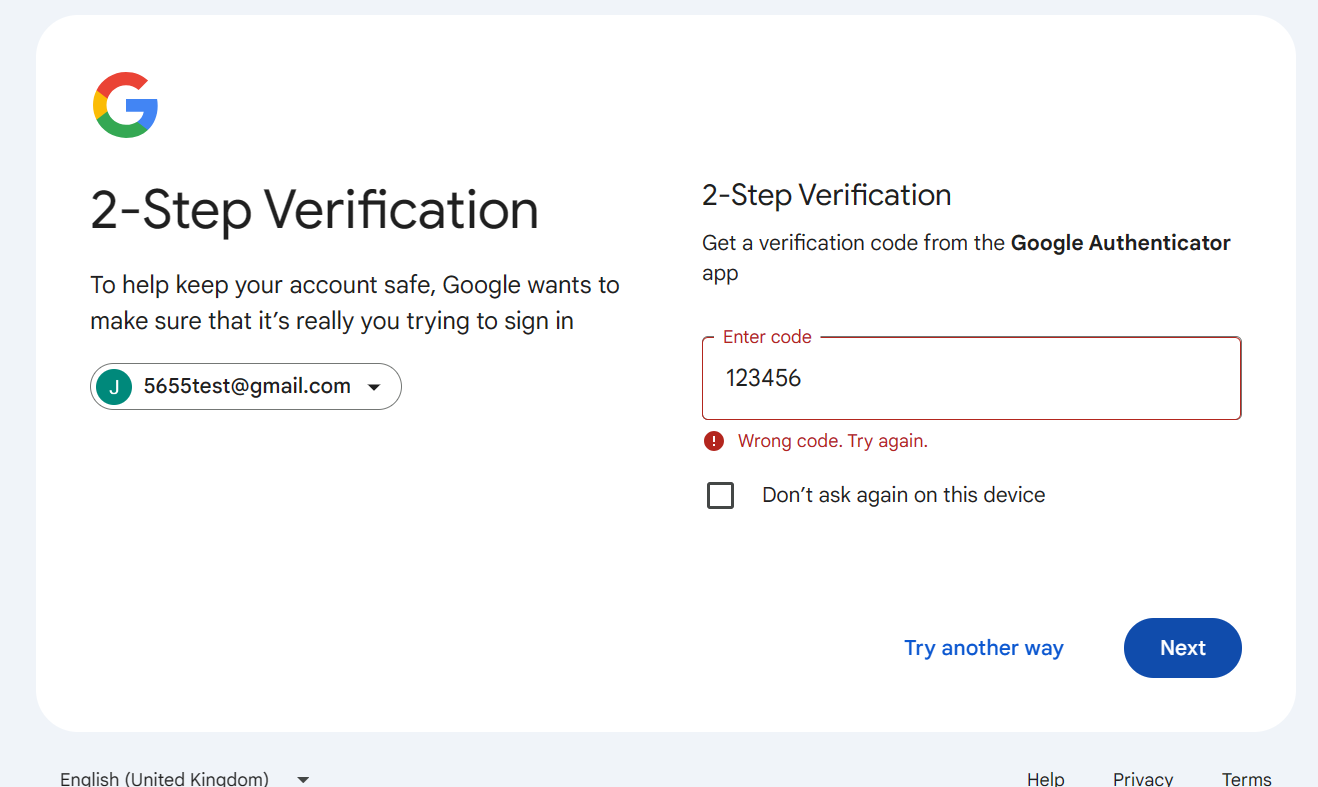
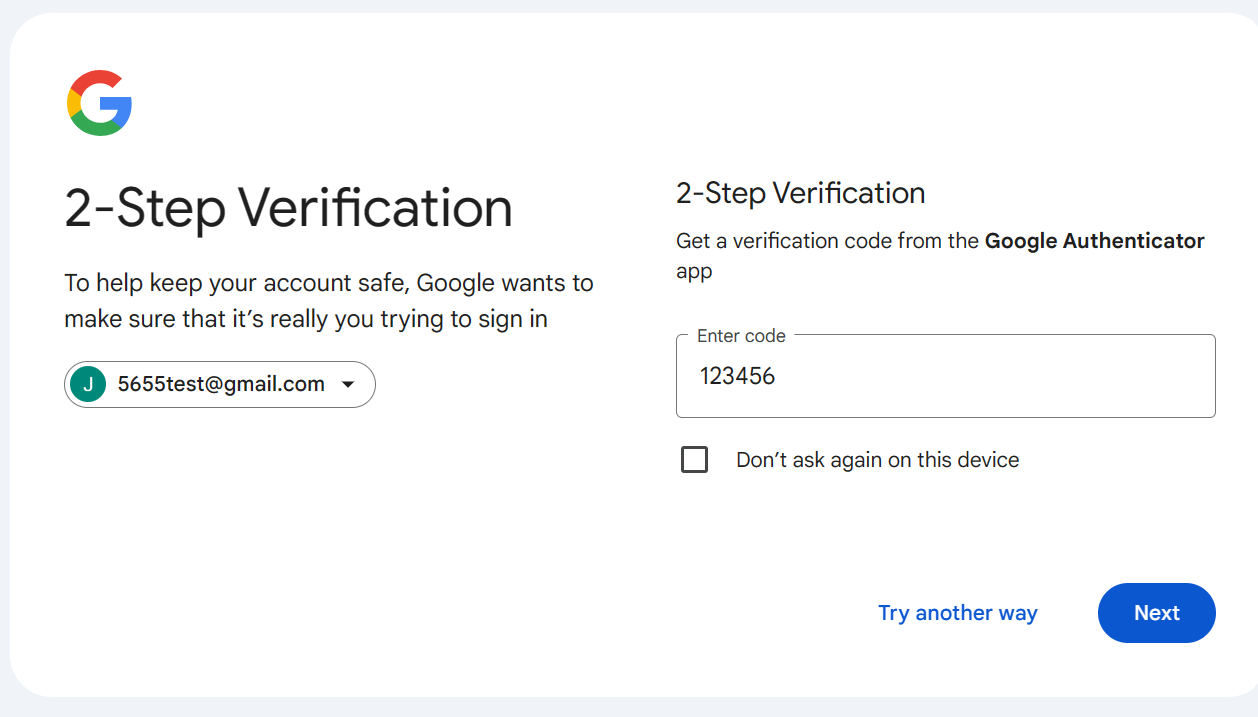
Glavna razlika između SHA-1 i SHA-256 je u dužini heševa koje generišu. SHA-1 generiše heš dužine 160 bita, dok SHA-256 generiše heš dužine 256 bita. Ovo znači da SHA-256 pruža mnogo veći broj mogućih kombinacija i veći nivo sigurnosti u poređenju sa SHA-1.



Da bih obezbedila poverljivost podataka pre generisanja HMAC autentifikacionog koda, primenila sam AES enkripciju na poruku (ili tajni ključ) pre nego što ih prosledim HMAC algoritmu.

1. zadatak





Kada se unese netačan jednokratni PIN u procesu dvofaktorske autentifikacije, korisniku se prikazuje poruka o grešci koja ga obaveštava da je unet neispravan PIN. Nakon toga, korisnik ima nekoliko pokušaja za unos ispravnog jednokratnog koda pre nego što se pristup odbije ili se primeni određena sigurnosna mera (npr. privremeno blokiranje naloga radi sprečavanja brzog uzastopnog pokušavanja).

Kada korisnik izgubi pristup aplikaciji za dvofaktorsku autentifikaciju, uobičajena procedura je korišćenje rezervnih jednokratnih kodova koji su unapred generisani i datih korisniku prilikom prvog podešavanja dvofaktorske autentifikacije. Korisnik može uneti jedan od rezervnih kodova umesto jednokratnog koda koji bi inače dobio putem SMS-a ili aplikacije za autentifikaciju.

Prednosti dvofaktorske autentifikacije uključuju povećanu sigurnost, smanjenje rizika od neovlašćenog pristupa(Čak i ako se lozinka kompromituje, neovlašćeni pristup neće biti moguć bez drugog faktora autentifikacije.). Međutim, postoje i neke slabosti i potencijalni napadi na dvofaktorsku autentifikaciju:

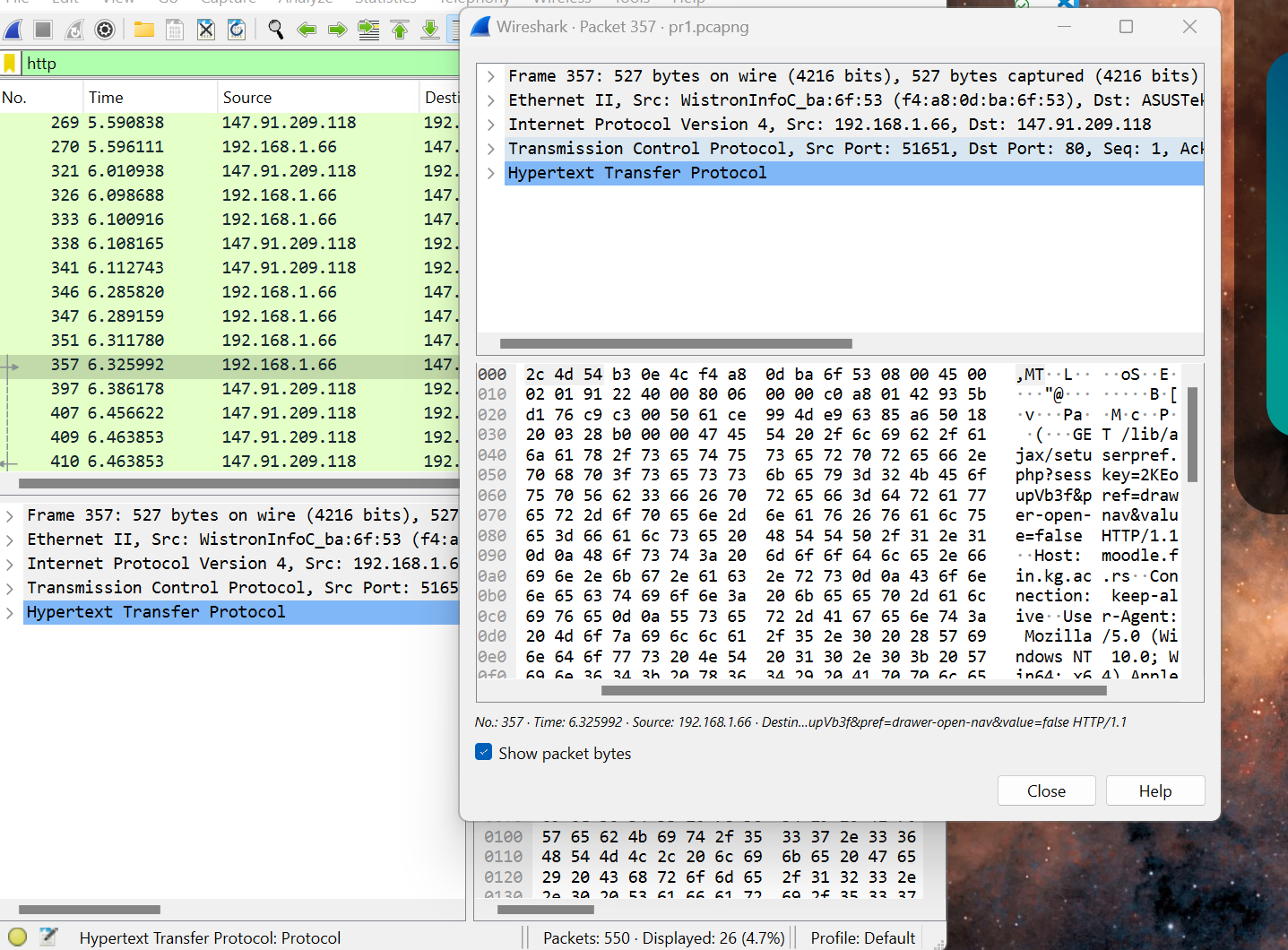
Phishing napadi: Napadači mogu pokušati da prevare korisnike da otkriju svoje informacije za autentifikaciju putem phishing e-pošte ili web stranica.

Krađa mobilnog uređaja: Ako je drugi faktor autentifikacije mobilni uređaj ili aplikacija za autentifikaciju, krađa ili gubitak uređaja može dovesti do kompromitovanja autentifikacije.

Uprkos tim potencijalnim nedostacima, dvofaktorska autentifikacija i dalje ostaje veoma efikasna sigurnosna mera koja značajno povećava sigurnost online naloga.

Wireshark

1.Analiza HTTP saobraćaja koristeći Wireshark



Wireshark omogućava analizu HTTP zahteva i odgovora. Ovo je korisno za razumevanje kako web stranice i aplikacije komuniciraju preko HTTP protokola.

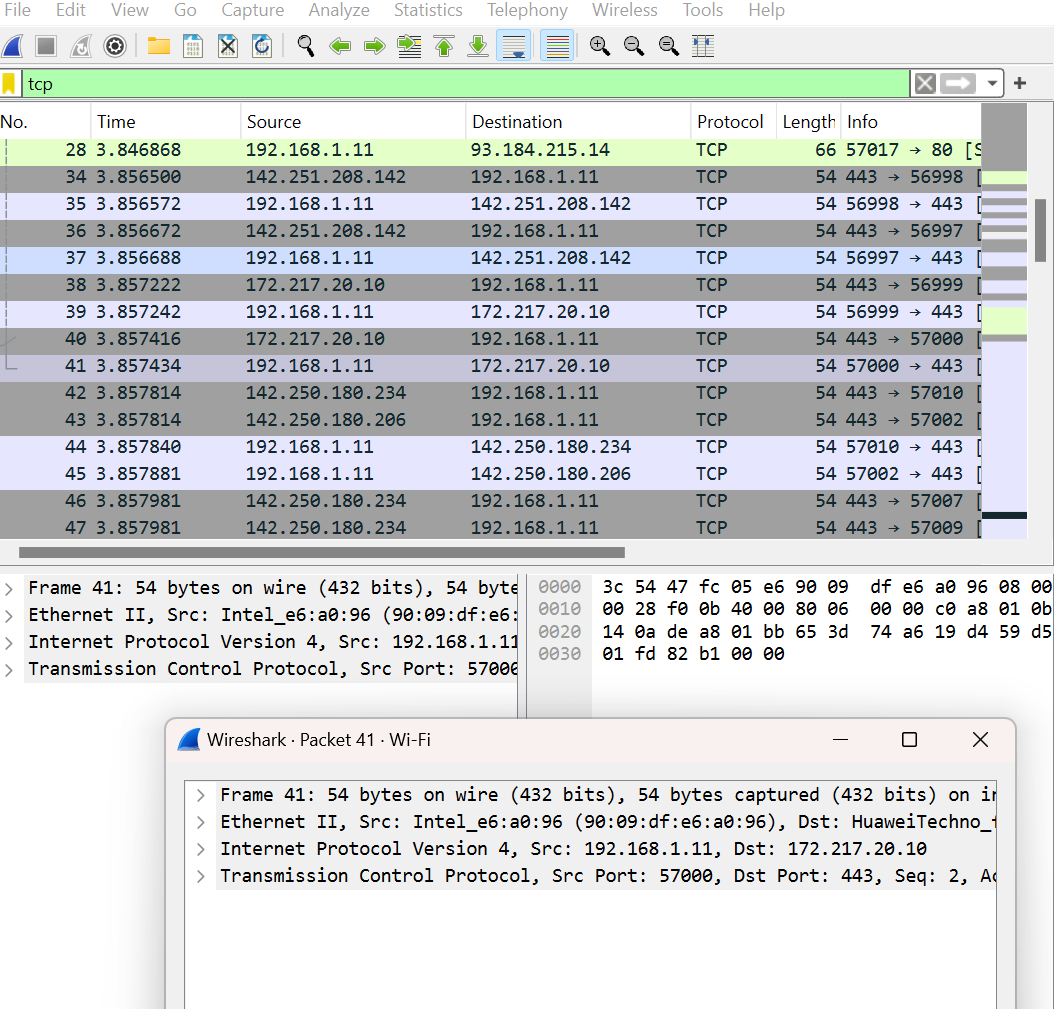
TCP/IP model opisuje kako se podaci prenose preko interneta. Sastoji se od slojeva poput fizičkog sloja (koji se bavi fizičkim prenosom podataka), sloja za vezu podataka (koji upravlja povezivanjem na mrežu), IP sloja (koji omogućava rutiranje podataka) i sloja transporta (kao što je TCP ili UDP, koji upravljaju transportom podataka).

HTTP (Hypertext Transfer Protocol) se koristi za prenos hipertekstualnih dokumenata preko interneta. To je osnova za komunikaciju između klijenta i servera.

HTTP zahtevi i odgovori - kada korisnik pristupa web stranici, web pregledac šalje HTTP zahtev serveru, a zatim server odgovara sa HTTP odgovorom. Wireshark omogućava praćenje i analizu ovih zahteva i odgovora, uključujući zaglavlja, telo poruke i druge metapodatke.

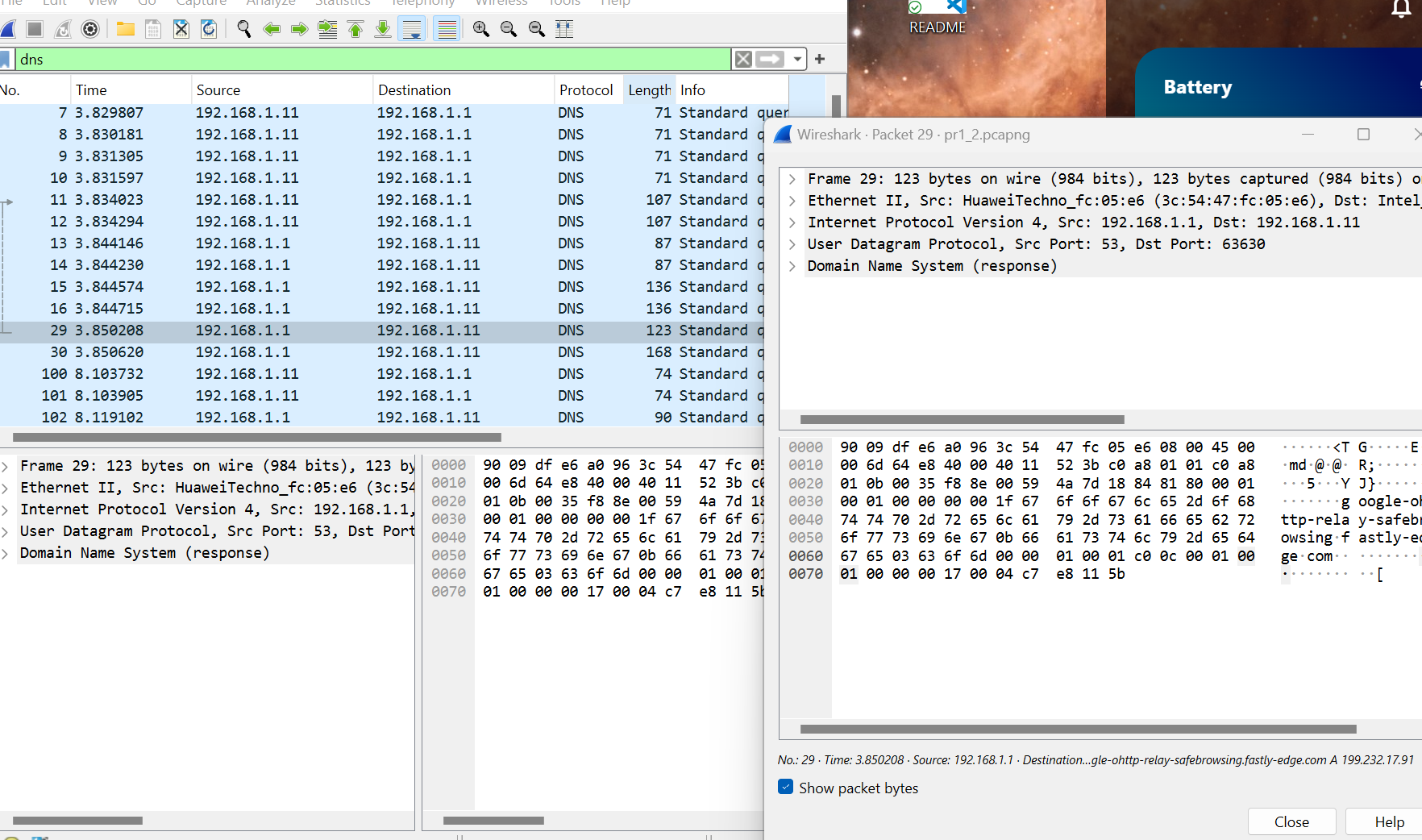
Zaglavlja - HTTP zahtevi i odgovori sadrže zaglavlja koja sadrže metapodatke o zahtevu ili odgovoru, kao što su informacije o klijentu i serveru, vrsta sadržaja koji se prenosi, veličina podataka i drugi relevantni podaci.

Telо poruke su sami podaci koji se prenose preko HTTP-a. To može biti HTML sadržaj web stranice, slike, video zapisi, JavaScript kod ili bilo koji drugi tip podataka koji se prenosi putem HTTP protokola.



Wireshark omogućava prikazivanje svih TCP sesija koje su zabeležene tokom snimanja. Možete pregledati informacije kao što su izvori i odredišta, portovi, veličina paketa, vreme trajanja sesije i druge relevantne informacije. omogućava da analizirate svaki TCP paket zasebno. Možete pregledati zaglavlja TCP paketa, uključujući informacije kao što su TCP kontrolni bitovi, redni brojevi, potvrdni brojevi, prozori za prozorski protokol, opcije TCP-a i druge relevantne informacije. pruža detaljne statistike o TCP sesijama, uključujući informacije o brzini prenosa podataka, veličini paketa, kašnjenjima. Wireshark je koristan alat za otkrivanje problema u TCP komunikaciji, kao što su gubljenje paketa, ponovno slanje, zagušenje mreže.

2.Analiza DNS saobraćaja koristeći Wireshark



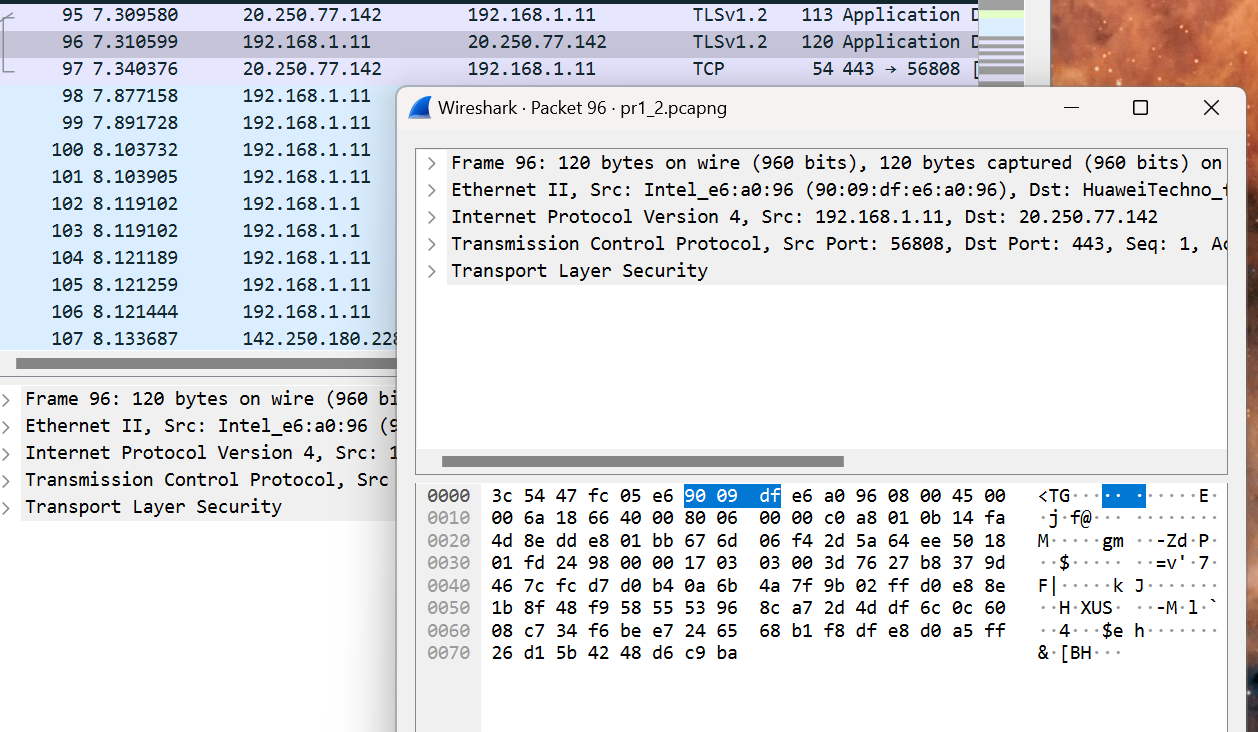
DNS je protokol koji se koristi za prevod imena domena u IP adrese i obrnuto.

Wireshark omogućava praćenje DNS zahteva koje uređaj šalje DNS serverima kako bi pronašao IP adresu povezanu s određenim imenom domena, takođe može pratiti odgovore DNS servera koji sadrže tražene IP adrese.

omogućava detaljnu analizu DNS paketa, možemo pregledati zaglavlja DNS paketa, uključujući tipove poruka, kodove odgovora, informacije o imenima domena i IP adresama, TTL (Time To Live) vrednosti i druge relevantne informacije.

omogućava da identifikujemo koji uređaji ili aplikacije šalju DNS zahteve i na koje DNS servere se ti zahtevi upućuju. To je korisno za dijagnostikovanje problema s povezivanjem na internet, kao i za praćenje aktivnosti različitih aplikacija.

Wireshark omogućava praćenje odgovora DNS servera na DNS zahteve.



TLS (Transport Layer Security) je kriptografski protokol koji omogućava sigurnu komunikaciju između klijenta i servera preko nesigurne mreže, poput interneta. TLSv1.2 je jedna od verzija TLS protokola koja pruža sigurnost i privatnost u komunikaciji.Wireshark omogućava analizu TLSv1.2 saobraćaja, što uključuje praćenje kriptografskih operacija, pregled šifrovanih podataka i analizu rukovanja ključevima.

Možemo videti detalje rukovanja TLS protokolom, uključujući verziju protokola, kriptografske algoritme koji se koriste, kao i druge relevantne informacije.

3.

Wireshark omogućava da detaljno pratimo komunikaciju izmeđuračunara i drugih uređaja ili servera na mreži, što vam daje uvid u to kako različite aplikacije koriste mrežu na različite načine.

Omogućava nam da pratimo komunikaciju na određenim mrežnim portovima. Svaka aplikacija koristi određene portove za komunikaciju preko mreže, pa možemo filtrirati Wireshark da pratimo samo saobraćaj koji prolazi kroz određene portove kako bismo analizirali komunikaciju određene aplikacije.

Wireshark može automatski identifikovati različite protokole koji se koriste u mrežnom saobraćaju, što omogućava da prepoznamo koje aplikacije generišu određene vrste saobraćaja(npr. HTTP zahteve koji dolaze od web pregledaca, DNS zahteve koji dolaze od sistema za razmenu poruka).

Mozemo da vidimo kako aplikacije komuniciraju preko mreže i koji protokoli se koriste,

pregled podataka koji se prenose unutar mrežnih paketa(možemo videti HTTP zahteve i odgovore ili bilo koji drugi tip podataka koji se prenosi preko mreže), da identifikujemo probleme u mrežnom saobraćaju različitih aplikacija, kao što su zagušenja mreže, gubljenje paketa, sporost u odgovorima… za optimizaciju performansi aplikacija, identifikujući resurse koji uzimaju najviše mrežnog saobraćaja i analizirajući kako se mreža koristi.