SVEUČILIŠTE U SPLITU  
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

SEMINARSKI RAD

EMAIL FORENZIKA

Ante Miljak, Karlo Marić

Split, svibanj 2023.

[1 UVOD 1](#_Toc139278915)

[2 TEHNIČKI ASPEKTI EMAILA 2](#_Toc139278916)

[2.1 Struktura emaila 2](#_Toc139278917)

[2.2 Protokoli za isporuku emaila 2](#_Toc139278918)

[2.3 Analiza i oporavak 2](#_Toc139278919)

[3 FORENZIČKA ANALIZA EMAILA 4](#_Toc139278920)

[3.1 Analiza metapodataka 4](#_Toc139278921)

[3.2 Identifikacija i autentifikacija pošiljatelja, sadržaja emaila i priloga 4](#_Toc139278922)

[3.3 Povezivanje s drugim digitalnim tragovima 5](#_Toc139278923)

[4 ANALIZA EMAIL KOMUNIKACIJE 6](#_Toc139278924)

[4.1 Identifikacija i izolacija relevantnih emailova 6](#_Toc139278925)

[4.2 Analiza sadržaja, privitaka i veza emailova 6](#_Toc139278926)

[4.3 Grafička analiza mreže emaila 6](#_Toc139278927)

[4.4 Rekonstrukcija slijeda događaja 7](#_Toc139278928)

[5 ALATI I TEHNIKE U EMAIL FORENZICI 8](#_Toc139278929)

[5.1 EnCase Forensic 8](#_Toc139278930)

[5.2 Forensic Toolkit (FTK) 8](#_Toc139278931)

[5.3 MailXaminer 8](#_Toc139278932)

[5.4 Exclaimer Mail Archiver 8](#_Toc139278933)

[5.5 Wireshark 9](#_Toc139278934)

[6 PRAKTIČNI PRIMJERI 10](#_Toc139278935)

[6.1 Analiza headera emaila 10](#_Toc139278936)

[7 ZAKLJUČAK 13](#_Toc139278937)

# UVOD

U seminaru fokusirat ćemo se na pružanje razumijevanja email forenzike i njenih implementacijskih aspekata. Cilj nam je pružiti dublje znanje i vještine potrebne za uspješnu implementaciju sigurnih i učinkovitih sustava za analizu emaila.

Email forenzika igra ključnu ulogu u sigurnosnom i forenzičkom istraživanju, a developeri imaju ključnu ulogu u razvoju alata i sustava koji omogućavaju analizu, praćenje i identifikaciju potencijalnih prijetnji putem emaila. Kroz ovaj seminar, istražit ćemo različite tehničke aspekte emaila kao što su njegova struktura, komponente te protokoli kao što su SMTP, POP i IMAP. Posebnu pozornost posvetit ćemo analizi email headera, koji je ključan za forenzičku analizu emaila.

Također, dotaknut ćemo metode identifikacije i autentifikacije pošiljatelja, uključujući analizu IP adresa, provjeru autentičnosti domena te druge tehnike. Proučit ćemo i metode pronalaženja skrivenih tragova u emailu, analizu priloga i enkripcije te tehnike oporavka izbrisanih emailova i oštećenih podataka.

Važan dio seminara bit će analiza email komunikacije iz perspektive developera. Razmotrit ćemo metode utvrđivanja autentičnosti email komunikacije, analizu jezičnih i stilskih obilježja te identifikaciju potencijalnih prijetnji i zlonamjernih sadržaja. Također, istražit ćemo upotrebu metapodataka u analizi komunikacije i kako ih iskoristiti za dobivanje korisnih informacija.

Uz teorijski dio, istražit ćemo alate i tehnike koje se mogu koristiti u implementaciji email forenzike. Proučit ćemo specijalizirane alate za analizu emaila, tehnike za izvlačenje i obradu digitalnih tragova te napredne tehnike analize metapodataka. Kroz praktične primjere i studije slučaja, povezat ćemo teorijske koncepte s njihovom primjenom u stvarnom svijetu.

# TEHNIČKI ASPEKTI EMAILA

## Struktura emaila

Email se sastoji od headera i tijela poruke. U headeru se nalaze metapodaci o emailu kao što su adrese pošiljatelja i primatelja, datum slanja, subjekt itd. Razumijevanje strukture headera ključno je za identifikaciju i analizu emaila. Tijelo poruke sadrži tekstualni ili HTML sadržaj emaila. Ovdje se mogu nalaziti i prilozi kao binarne datoteke. Analiza sadržaja emaila pomaže u otkrivanju potencijalnih prijetnji ili zlonamjernih aktivnosti.

## Protokoli za isporuku emaila

Dva glavna protokola za isporuku emaila su SMTP protokol, POP te IMAP protokoli. Simple Mail Transfer Protocol (SMTP) je osnovni protokol za slanje emaila. Razumijevanje kako SMTP funkcionira omogućava analizu IP adresa, provjeru autentičnosti pošiljatelja i utvrđivanje putanje isporuke. Post Office Protocol (POP) i Internet Message Access Protocol (IMAP) omogućuju korisnicima pristup i preuzimanje emaila s poslužitelja. Poznavanje ovih protokola korisno je za analizu pristupnih logova i tragova preuzimanja emaila.

## Analiza i oporavak

Analiziranjem IP adresa, enkripcije i headera moguće je izvući niz korisnih informacija za rad. Provjera IP adresa pošiljatelja može pomoći u identifikaciji geografske lokacije i autentičnosti emaila. Analiza SPF (Sender Policy Framework) i DKIM (DomainKeys Identified Mail) autentifikacije također pruža informacije o autentičnosti domena. Analizom enkripcije provjerava se je li email enkriptiran i kojim algoritmom može otkriti razinu sigurnosti i privatnosti komunikacije. Proučavanje headera emaila može pružiti korisne informacije o putanji isporuke, rutiranju, oblačnim uslugama i drugim tehničkim detaljima. Razumijevanje različitih polja u headeru može pomoći u identifikaciji potencijalnih nepravilnosti ili manipulacija.

Oporavak izbrisanih emailova i oštećenih podataka bitan je aspekt email forenzike. U slučajevima kada su emailovi izbrisani ili podaci oštećeni, tehnike oporavka mogu biti korisne. To uključuje analizu nepotvrđenih pravila brisanja, praćenje tragova u datotekama i korištenje posebnih alata za obnovu.

# FORENZIČKA ANALIZA EMAILA

Forenzička analiza emaila ima ključnu ulogu u otkrivanju, istraživanju i rješavanju sigurnosnih incidenata, zloupotreba i kriminalnih aktivnosti. Ova analiza omogućuje forenzičarima da identificiraju potencijalne prijetnje, otkriju tragove osumnjičenih i pruže relevantne dokaze u sudskim postupcima. U ovom dijelu seminara, detaljno ćemo istražiti metode, alate i tehnike koje se koriste u forenzičkoj analizi emaila.

## Analiza metapodataka

Metapodaci emaila sadrže ključne informacije o vremenu slanja, adresama pošiljatelja i primatelja, putanji isporuke i drugim tehničkim detaljima. Forenzička analiza metapodataka omogućuje praćenje komunikacijskih tokova, identifikaciju izvora emaila, provjeru autentičnosti i utvrđivanje putanje isporuke. Analiza metapodataka može otkriti informacije o IP adresama, DNS zapisima, protokolima slanja i drugim metapodacima koji su ključni za forenzičku analizu.

## Identifikacija i autentifikacija pošiljatelja, sadržaja emaila i priloga

Jedan od ključnih koraka u forenzičkoj analizi emaila je identifikacija i autentifikacija pošiljatelja. Forenzičari koriste različite tehnike za provjeru autentičnosti emaila i utvrđivanje stvarnog identiteta pošiljatelja. To uključuje analizu IP adresa, provjeru DNS zapisa kao što su SPF (Sender Policy Framework) i DKIM (DomainKeys Identified Mail) autentifikacija te usporedbu digitalnih potpisa.

Forenzička analiza sadržaja emaila pruža uvid u tekstualni ili HTML sadržaj, priloge, URL-ove i druge elemente koji se nalaze unutar emaila. Ova analiza može otkriti potencijalno zlonamjerne ili nezakonite materijale, kao i pružiti informacije o jezičnim karakteristikama, stilu pisanja i skrivenim porukama. Forenzičari koriste tehnike kao što su heuristička analiza, prepoznavanje uzoraka i analiza koda kako bi otkrili potencijalne prijetnje ili dobili dodatne dokaze.

Prilozi u emailu često su nositelji zlonamjernog softvera ili sadrže važne informacije relevantne za istraživanje. Forenzička analiza priloga uključuje provjeru integriteta datoteka, analizu metapodataka priloga, upotrebu antivirusnih alata i sandboxinga kako bi se otkrile potencijalne prijetnje ili dobili dodatni uvidi. Ova analiza može otkriti prisutnost virusa, trojanaca, ransomwarea ili drugih zlonamjernih programa.

## Povezivanje s drugim digitalnim tragovima

Forenzička analiza emaila često uključuje povezivanje s drugim digitalnim tragovima kako bi se dobila cjelovita slika događaja. To može uključivati analizu logova poslužitelja, pregledavanje web stranica, provjeru mobilnih uređaja ili pristup društvenim mrežama. Povezivanje s drugim digitalnim tragovima omogućuje forenzičarima da stvore kontekst komunikacije, identificiraju povezane osobe ili aktivnosti te pruže informacije relevantne za istragu.

# ANALIZA EMAIL KOMUNIKACIJE

## Identifikacija i izolacija relevantnih emailova

Prvi korak u analizi email komunikacije je identifikacija i izolacija relevantnih emailova za istraživanje. To se može postići korištenjem pretraživanja email baza podataka, filtriranja prema određenim kriterijima kao što su datum, pošiljatelj, primatelj, ključne riječi ili korištenjem posebnih alata za analizu. Identificirani emailovi mogu biti ključni za razumijevanje događaja ili otkrivanje relevantnih informacija.

## Analiza sadržaja, privitaka i veza emailova

Analiza sadržaja emailova pruža uvid u poruke, priloge, jezične karakteristike, stil pisanja i druge aspekte komunikacije. Ova analiza može otkriti važne informacije, kao što su planirane aktivnosti, dogovori, prijetnje ili neprimjereno ponašanje. Forenzičari često koriste tehnike poput jezične analize, prepoznavanja uzoraka i klasifikacije kako bi izvukli korisne podatke iz sadržaja emailova. Također je važno analizirati i interpretirati emotivni ton poruka, neizrečene poruke ili skrivene informacije koje se mogu otkriti kroz detaljnu analizu sadržaja. Analiza privitaka i veza unutar emaila može otkriti važne informacije o povezanim dokumentima, datotekama ili web resursima. Analiza veza u emailu može otkriti vanjske resurse ili web stranice koje su povezane s emailom, što može pružiti dodatne uvide u kontekst ili svrhu komunikacije.

## Grafička analiza mreže emaila

Grafička analiza mreže emaila koristi se za vizualizaciju veza i interakcija između različitih pošiljatelja i primatelja. Ova analiza omogućuje identifikaciju ključnih aktera, hijerarhije ili grupiranja te prepoznavanje važnih veza unutar email mreže. Alati za grafičku analizu mogu se koristiti za stvaranje grafova koji prikazuju ove veze i olakšavaju razumijevanje kompleksnosti komunikacije. Ova analiza može otkriti ne samo direktnu komunikaciju između osoba, već i posredne veze i povezanost s drugim subjektima ili organizacijama.

## Rekonstrukcija slijeda događaja

Forenzička analiza emaila može uključivati rekonstrukciju slijeda događaja na temelju vremenskih oznaka i sadržaja emailova. Ovo omogućuje razumijevanje kronologije događaja, redoslijeda komunikacije ili promjena u interakcijama. Korištenje metapodataka emaila, kao što su vremena slanja i isporuke, može pomoći u preciznoj rekonstrukciji slijeda događaja. Rekonstrukcija slijeda događaja može otkriti važne informacije o promjenama u dinamici odnosa, povodu za određene poruke ili dogovore.

# ALATI I TEHNIKE U EMAIL FORENZICI

Alati i tehnike koje se koriste u email forenzici igraju ključnu ulogu u analizi, istraživanju i pružanju relevantnih informacija. U nastavku su navedeni neki od najpopularnijih alata i softvera koji se koriste u praksi email forenzike.

## EnCase Forensic

EnCase Forensic je jedan od vodećih alata u digitalnoj forenzici, koji se također može koristiti za analizu emaila. Ovaj alat omogućuje forenzičarima da izvedu naprednu analizu email poruka, obnove obrisane email komunikacije, provjere metapodatke i analiziraju priloge. EnCase Forensic također podržava opsežne metode pretraživanja i filtriranja kako bi se pronašle ključne informacije.

## Forensic Toolkit (FTK)

Forensic Toolkit (FTK) je još jedan popularan alat u digitalnoj forenzici koji se može koristiti za analizu emaila. FTK omogućuje ekstrakciju, analizu i pretraživanje email poruka s ciljem pronalaženja dokaza ili važnih informacija. Ovaj alat podržava veliki broj formata emaila i pruža napredne mogućnosti analize metapodataka, pretrage ključnih riječi i analize priloga.

## MailXaminer

MailXaminer je specijalizirani softver za analizu email forenzike. Ovaj alat omogućuje forenzičarima da istraže, analiziraju i rekonstruiraju email komunikaciju, uključujući metapodatke, sadržaj poruka, priloge i kontakte. MailXaminer također pruža mogućnost analize heuristike, analize steganografije i obnovljive email servere.

## Exclaimer Mail Archiver

Exclaimer Mail Archiver je alat koji se koristi za arhiviranje i upravljanje email komunikacijom. Ovaj alat omogućuje pohranu i organizaciju email poruka, što može biti ključno za kasniju analizu i potraživanje relevantnih informacija. Exclaimer Mail Archiver čuva metapodatke, poruke i priloge te pruža mogućnost brze pretrage i filtriranja.

## Wireshark

Wireshark je popularan alat za analizu mrežnog prometa koji se također može koristiti u email forenzici. Ovaj alat omogućuje snimanje i analizu mrežnog prometa koji se odnosi na prijenos emaila. Forenzičari mogu koristiti Wireshark za analizu protokola, identifikaciju nepravilnosti ili potencijalnih sigurnosnih prijetnji te za dobivanje uvida u put kojim je email prolazio.

# PRAKTIČNI PRIMJERI

## Analiza headera emaila

U slijedećem primjeru analiziran je header emaila korištenjem email i re biblioteka. U ovom primjeru obrađen je header, IP adrese, putanje i metapodaci maila.

import email

import re

def analyze\_email\_headers(email\_data):

# Parsiranje emaila

msg = email.message\_from\_bytes(email\_data)

# Prikazivanje zaglavlja emaila

print("Zaglavlje emaila:")

print(msg)

# Analiza IP adresa

ip\_pattern = r"\b(?:\d{1,3}\.){3}\d{1,3}\b"

received\_headers = msg.get\_all('Received')

if received\_headers:

for received\_header in received\_headers:

match = re.search(ip\_pattern, received\_header)

if match:

ip\_address = match.group(0)

print("IP adresa u Received zaglavlju:", ip\_address)

# Ovdje možete provesti dodatnu analizu IP adrese, poput geolokacije ili provjere poznatih loših IP adresa

# Provjera autentičnosti

spf\_header = msg.get('SPF')

dkim\_header = msg.get('DKIM-Signature')

if spf\_header:

print("SPF zaglavlje:", spf\_header)

# Ovdje možete provjeriti SPF rezultate i provjeriti autentičnost poruke

if dkim\_header:

print("DKIM zaglavlje:", dkim\_header)

# Ovdje možete provjeriti DKIM potpis i provjeriti autentičnost poruke

# Provjera putanja

path\_headers = msg.get\_all('Received-SPF')

if path\_headers:

for path\_header in path\_headers:

print("Putanja u Received-SPF zaglavlju:", path\_header)

# Ovdje možete provjeriti putanju i identificirati potencijalne manipulacije

# Analiza metapodataka emaila

print("Metapodaci:")

for key, value in msg.items():

print(f"{key}: {value}")

# Primjer korištenja

with open('profesor.eml', 'rb') as file:

email\_data = file.read()

analyze\_email\_headers(email\_data)

Prvo, importiramo biblioteku email koja će nam omogućiti parsiranje emaila. Definiramo funkciju analyze\_email\_headers koja će provesti analizu headera emaila. U funkciji, parsiramo email koristeći email.message\_from\_bytes kako bismo dobili objekt msg koji predstavlja email poruku. Prikazujemo zaglavlje emaila koristeći print(msg).

Slika na kojoj se prikazuje tekst, snimka zaslona, Font

Opis je automatski generiran

Koristimo regularne izraze za analizu IP adresa u Received zaglavljima. Iteriramo kroz sva Received zaglavlja, pronalazimo IP adrese pomoću regularnog izraza i prikazujemo ih.

Slika na kojoj se prikazuje tekst, Font, snimka zaslona, tipografija

Opis je automatski generiran

Provjeravamo autentičnost emaila koristeći zaglavlja SPF i DKIM-Signature. Ako su prisutna, prikazujemo ih. Provjeravamo putanje u zaglavlju Received-SPF. Iteriramo kroz sva zaglavlja te prikazujemo putanje.

Analiziramo metapodatke emaila pomoću petlje for koja iterira kroz sve ključeve i vrijednosti u msg.items(). Prikazujemo metapodatke emaila. U primjeru korištenja otvaramo datoteku emaila, čitamo njene podatke i pozivamo funkciju analyze\_email\_headers s tim podacima.

Slika na kojoj se prikazuje tekst, snimka zaslona, Font

Opis je automatski generiran

Ovaj primjer kodiranja pruža osnovnu strukturu za analizu headera emaila, uključujući IP adrese, provjeru autentičnosti, provjeru putanja i metapodatke.

# ZAKLJUČAK

Email forenzika ima ključnu ulogu u istraživanju i analizi email komunikacije u svrhu dobivanja relevantnih informacija, identifikacije tragova i pružanja dokaza. Razumijevanje tehničkih aspekata emaila, kao što su metapodaci, protokoli, enkripcija i pravila slanja, ključno je za uspješnu forenzičku analizu emaila. Analiza metapodataka, priloga, veza i sadržaja poruka omogućuje stjecanje dubljeg uvida u komunikaciju, identifikaciju relevantnih informacija te otkrivanje manipulacija ili zlonamjernih aktivnosti.

Forenzička analiza emaila zahtijeva upotrebu specijaliziranih alata i tehnika. Alati poput EnCase Forensic, FTK, MailXaminer i drugi pružaju napredne mogućnosti za ekstrakciju, analizu i pretraživanje emaila. Tehnike poput analize heuristike, steganografije, digitalnih potpisa i obnovljivih email servera pružaju dodatne načine za dublju analizu email komunikacije. Analiza email komunikacije omogućuje identifikaciju ključnih informacija, odnosa između sudionika, kronologije događaja i povoda za određene poruke. To može biti od vitalnog značaja u forenzičkim istraživanjima, pravnim procesima ili sigurnosnim incidentima.

Na kraju, email forenzika je kompleksno područje koje zahtijeva stručno znanje, iskustvo i korištenje pravih alata. Ova analiza pruža dublji uvid, otkriva važne informacije i omogućuje donošenje relevantnih zaključaka u različitim forenzičkim i pravnim kontekstima.