Analiza podatkov VoIP klicev

[Članek pri predmetu Digitalna forenzika]

Tomaž Tomažič
Fakulteta za računalništvo in infromatiko
Tržaška 25
Ljubljana, Slovenia
tt3710@student.uni-lj.si

Zupanec Žiga
Fakulteta za računalništvo in infromatiko
Tržaška 25
Ljubljana, Slovenia
zz9698@student.uni-lj.si

ABSTRACT
Popularnost telefonije preko IP (VoIP) je v zadnjih letih narasla, ker je cenovno ugodnejša in enostavnejša za uporabo. Kakorkoli že, ta tehnologija je tudi atraktivna za kriminal, ker je VoIP globalna telefonska storitev, v kateri je težko identificirati uporabnika. Privlačna je tudi zaradi visoke varnosti, saj veliko implementacij uporablja močno enkripcijo za zaščito, tako zvočnih podatkov kot kontrolo samih sporočil v primerjavi z žično telefonijo kjer je prisluškovanje enostavnejše. Zato so za VoIP klice potrebni drugi načini pridobivanja digitalnih dokazov in informacij. V najini raziskavi smo pogledali kateri dokazi ostanejo po opravljenem VoIP klicu na obeh napravah, trdem disku in bralno-pisalnem pomnilniku (RAM).

Keywords
Digitalna forenzika, dokazi, telefonija preko IP, VoIP, forenzika v pomnilniku

1. UVOD
VoIP telefonija je tehnologija preko katere se prenaša večpredstavnostna vsebina po internetnem omrežju. Uporablja močno enkripcijo za zaščito, tako zvočnih podatkov kot kontrolo samih sporočil v primerjavi z žično telefonijo kjer je prisluškovanje enostavnejše. Zato so za VoIP klice potrebni drugi načini pridobivanja digitalnih dokazov in informacij. V najini raziskavi smo pogledali kateri dokazi ostanejo po opravljenem VoIP klicu na obeh napravah, trdem disku in bralno-pisalnem pomnilniku (RAM).

Identifikacijske poverilnice so osnovane v informacijah iz glav paketov vsebovanih v VoIP protokolu. Narejeni so bili različni kontrolni testi v katerih je bila forenzična analiza narejena na virtualnih strojih s katerimi so bili opravljeni različni VoIP klici. Eksperimenti so bili ponovljeni na istem protokolu tako na disku kot v bralno pisalnem pomnilniku (RAM).

2. PALETA VOIP
Telefonija preko IP protokola je zelo spremenila način kako se podatki telefoniranja prenašajo in tako začela pravo telekomunikacijsko industrijo. S samo rastjo popularnosti in široko dostopnostjo do interneta je omogočeno, da se klici prenašajo preko internetne infrastrukture kot pa po tradicionalnem javno komutiranem telefonskem omrežju (PSTN). Ta tehnologija, ki se ji reče VoIP, uporablja internetni protokol (IP) za prenašanje paketov ki vsebujejo majhne koš-čke glasovnega pogovora med klicočima.

Popularnost VoIP je narasla zaradi cenejše in enostavnejše uporabo tako doma kot v podjetjih[1]. Kakorkoli že, ta tehnologija je zelo privlačna za kriminalce, še posebej za VoIP pogovore ki niso spremljani iz strani internetnega ponudnika. To je zaradi tega ker je VoiP globalen telefonski servis v katerem je težko identificirati uporabnikovo identiteto, ker večina implementacij uporablja močno enkripcijo za zavarovanje tako zvočnih podatkov kot kontrolo samih sporočil in nadziranje ali sledenje takšnih VoIP klicev je oteženo zaradi konvencionalnih metod kot so žično prisluškovanje in le teh ni mogoče aplicirati na VoIP klice. Zaradi teh razlogov so za pridobivanje podatkov in informacij iz telefonije preko IP potrebne druge metode. Bistveno za forenzične raziskovalce je, da imajo metodo ki omogoča organom pregona premagati nekatere vidike tega načina telefonije, ki so ugodne za storilce kaznivih dejanj.

Ta uvod podaja pregled transportnih protokolov VoIP in signalne protokole. Ti določajo podatke, iz katerih je mogoče forenzično pridobiti polja iz glave protokola, kot tudi uporabnikovo registracijo za VoIP klic.

VoIP ni samo en protokol ampak kolekcija različnih že obstoječih protokolov, ki so uporabljeni za vzpostavitev, vzdrževanje in končanje klica, protokoli za enkapsulacijo in prenos paketov po internetu. Protokoli IP, UDP in RTP so protokoli ki enkapsulirajo in prenašajo pakete, ki vsebujejo informacije potrebne za identifikacijo izvora in ponora klicateljev in dostavo samih zvočnih podatkov. Session Initiation Protocol (SIP) je signalni protokol uporabjen za vzpostavitev, vzdrževanje in zaključevanje klica.

2.1 Internet Protocol
Protokol IP[3] je odgovoren za hranjenje internetnega naslova v glavi, kar omogoča paketom da so dostavljeni iz svojega izvora do IP naslova. Format glave protokola IP je prikazan na sliki 1.

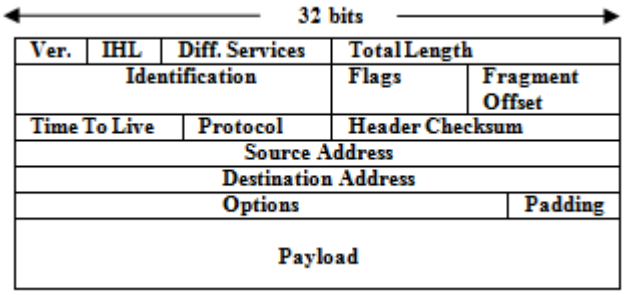

Figure 1: Format glave paketa IP.

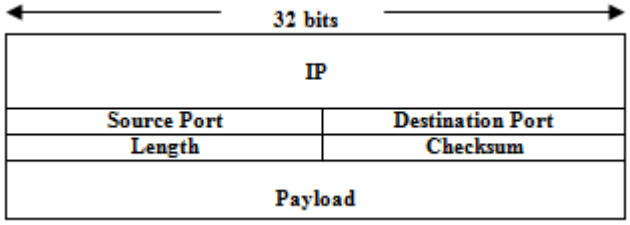

Figure 2: Glava paketa UDP.

2.2 User Datagram Protocol

Zanesljiv protokol za prenos paketov po internetu je protokol TCP[4], ki zagotavlja dostavo tudi za izgubljene in pokvarjene pakete s ponovnim pošiljanjem. Vendar za VoIP klice, ki potekajo v realnem času, ni smisla ponovnega pošiljanja za izgubljene pakete. TCP uporablja nadzor pretoka, ki začasno zaustavi prenos paketov dokler pokvarjeni paket ni uspešno prenešen.

Namesto protokola TCP je za zahteve VoIP bolj primeren, čeprav je manj zanesljiv pri dostavi paketov, protokol UDP (slika 2). Izbran sistem je tako sklad protokola IP/UDP. IP datagram zagotavlja izvorni in ciljni naslov in izvorna in ciljna vrata. Pogoste aplikacije delujejo na specifičnih vratih. Ker TCP zagotavlja prenos izgubljenih paketov, ni zaželjen v realnočasnih aplikacijah in je zato za prenos zvoka uporabljen UDP.

Protokol UDP[2] se uporablja tudi zaradi lažjega prebijanja NAT-a pri uporabi načina prevajanje omrežnega naslova (angl. Network Address Translation, krat. NAT). Poznamo več vrst NAT (slika 3) in sicer:

- Direktna preslikava (angl. Full-cone) pri kateri se notranji lokalni IP naslov in vrata preslikajo v zunanji IP naslov z istimi vrati. Zunanji odjemalci lahko s pošiljanjem na začasni par (zunaj vidni IP naslov in vrata) pošiljajo sporočila notranjemu IP naslovu.
- Omejena direktna presilava (angl. Restricted cone): deluje na istem principu kot direktna preslikava z omejitvijo, da mora prvi paket poslati interni odjemalec.
- Z vrati omejena direktna preslikava: zunanji odjemalec lahko pošlje paket le na vrata, katerim je predhodno pošiljal notranji odjemalec.

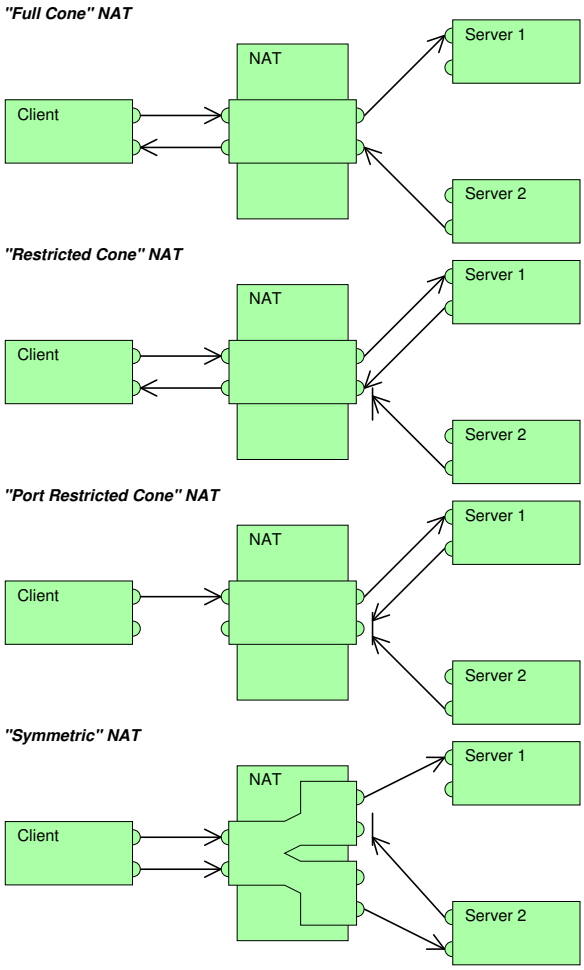

Figure 3: Primerjava med različnimi metodami NAT.

- Simetrična preslikava (angl. Symmetric cone): usmerjevalnik vodi preslikovalno tabelo glede na ponorni IP naslov in vrata. Vrata se dodelijo naključno za čas trajanja seje glede na ponorni IP naslov. Le tisti zunaji odjemalec, ki prejme paket paket notranjega odjemalca lahko pošlje paket nazaj (odgovori) notranjemu odjemalcu.

NAT prebijamo[7] z orodji za sprehajanje po takih omrežjih, ki jih imenujemo "Obhod NAT-a", (angl. Session Traversal Utilities for NAT, krat. STUN[8]). Gre za tehniko, ki vzpostavi in vzdržuje IP povezave skozi NAT usmerjevalnike, ki kršijo povezavo iz enega konca na drugi (end-to-end). Uporablja se za peer-to-peer in VoIP povezave. Obstaja veliko metod za rešitev tega problema, vendar ne obstaja ena univerzalna. Metoda, pri kateri potrebujemo strežnik, se imenuje "relay"oz. posrednik. Pri takem načinu, potujejo paketi enega odjemalca najprej do strežnika, ki jih nato posreduje drugemu odjemalcu in obratno. Streznik mora biti naprava s katero lahko komunicirata oba odjemalca, ki sta v omrezju NAT. Veliko tehnik uporablja pomoč strežnika. Nekatere pa strežnik uporabljajo samo za vzpostavitev povezave. Če strežnik uporabljajo za celotno komunikacijo se s tem zniža kvaliteta povezave in poveča latenca. Druga

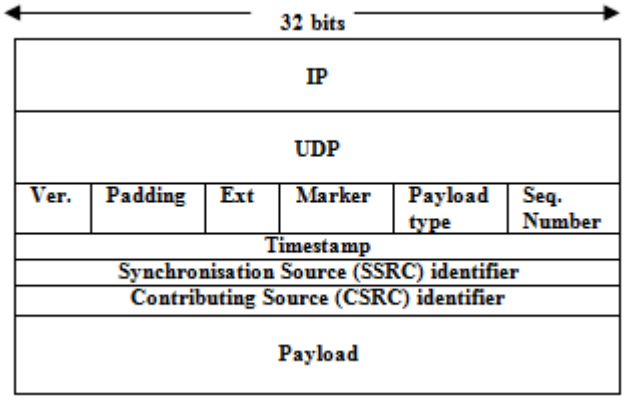

Figure 4: Sklad UDP/RTP in glava paketa RTP.

tehnika je, da se dovoli požarnim zidovom in NAT omrežjem da dopuščajo VoIP, hkrati pa ohranjajo varnost podjetij. To določajo protokoli RSIP (realm-specific IP) in MIDCOM (middlebox communications).

2.3 Real-Time Transport Protocol

Real-Time Transport Protocol (RTP) zagotavlja prometno omrežje za aplikacije v realnem času, kot so prenos zvoka preko paketno komutiranega omrežja. Protokol RTP je izbran za prenos govornih podatkov, saj dodaja dodatne informacije, kot je na primer zaporedna številka za vsak paket, da zagotovijo prejemni aplikaciji zvoka možnost razporeditve paketov v pravilnem vrstnem redu in zagotavlja tudi časovno oznako za vsak posamezen paket, ki omogoča predvajanje zvoka v zaporednih časovnih presledkih. Za klicanje in sprejemanje VoIP klica ni potrebna uporaba protokola RTP, vendar ta lahko preprosto doda dodatne podatke, ki pripomorejo k sprejemanju paketov v vrstnem redu in olajša delo z VoIP konferencami. Sklad IP/UDP/RTP in glava paketa RTP je prikazana na sliki 4.

Za vsak paket sta enolično določena časovna značka in sekvenčna številka. Sekvenčna številka se poveča z vsakim poslanim paketom in omogoča ponovno razvrstitev in detekcijo izgube paketov na prejemnikovi strani.

Polje sinhronizacijski izvorni identifikator (SSRC) označuje izvor sinhronizacije, navadno z računalnikovo uro medtem ko polje doprinašani izvor (CSRC) označuje vir posameznih prispevkov, ki sestavljajo en podatkovni tok paketov. Za sodelovanje v VoIP klicu ni nujno uporabljati protokola RTP. Nekatere aplikacije VoIP kot je na primer Skype ne uporabljajo protokola RTP, medtem ko pa ga X-Lite in Ekiga[9] uporabljajo. Prav zaradi tega smo naš eksperiment naredili na programu Ekiga saj imamo z dodatnim protokolom RTP, potem na voljo dodatna polja iz katerih lahko iščemo informacije o klicu.

Zvočni posnetek je razdeljen v paket ki je potem prenesen po omrežju. Če je paket prevelik in ga je potrebno fregmenitrati ali pa izvira iz različnih virov, potem bo imel vsak fragment enak CSRC za identifikacijo izvora iz istega podatkovnega toka. Različne sekvenčne številke pa omogočajo rekonstrukcijo v pravem zaporedju za vsak CSRC. To je uporabljeno za sinhronizacijo na prejemnikovi strani.

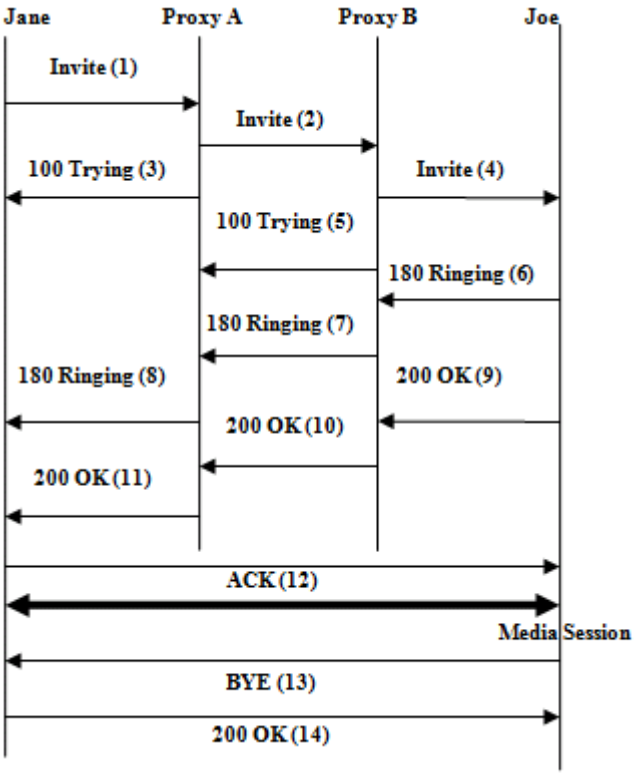

Figure 5: Primer izmenjave sporočil med sejo SIP.

2.4 SIP protocol

Protokol SIP[5] omogoča klicanje uporabniških posrednikov (UA) za lokacijo in registracijo z uporabo proxy strežnikov, ki omogočajo drugim uporabniškim posrednikom priključitev v klicno sejo. Vsaka transakcija je sestavljena iz zahteve, ki sproži določeno metodo na vsaj en odgovor, kot je prikazano na sliki 5. Jane uporablja svojo VoIP aplikacijo za pošiljanje zahteve Invite (vabilo) Joetu. Zahteva Invite je SIP metoda, ki določa akcije, ki jih Jane želi od Joeta, to je sprejetje klica. Zahteva Invite gre skozi dva proxy strežnika, da doseže Joeta (korak od 1 – 5). Na prejemnikovi strani se začne zvonjenje, odgovor pa Joe vrne pošiljatelju ponovno skozi oba proxy strežnika (korak 6 – 8). Joe potrdi prejetje zahtevka Invite z odgovorom OK osebi Jane (9 – 11). Prenos večpredstavnostne vsebine se začne ko Jane potrdi odgovora OK (12). Ta sejo lahko zaključi katerikoli udeleženec v komunikaciji (13 -14).

3. ALTERNATIVNI PROTOKOLI VOIP

Vrata, ki se navadno uporabljajo pri paleti protokolov VoIP so povzeta v tabeli 1.

3.1 Paleta protokolov H.323

Namesto protokola SIP se lahko za vzpostavitev seje, kontrolo nad sejo, prenos multimedijskih podatkov in kontrolo pasovne širine uporabi zbirka tehnologij H.323 (slika 6). H.323 [10] lahko po funkcionalnosti grobo primerjamo s protokolom SSL/TLS, a je precej obsežnejši. Protokol povezuje različne

Table 1: Uporaba vrat pri protokolu VoIP

Protokol	Vrata	Tip	Razlaga
SIP	5000 do 5100	UDP	SIP seja privzeto 5060. Različno pri NAT.
STUN	3478 do 3479	UDP	
RTP	Naključna/razpoložljiva	UDP	Prihajajoč promet na drugi strani. Navadno 5004, 7070, 16382
H.323	1720	TCP	Poslušanje.
H.323	5000 do 5100	UDP	Vratarji.
H.323	30000 do 30010	TCP	Kanal H.245 za Microsoft Netmeeting.

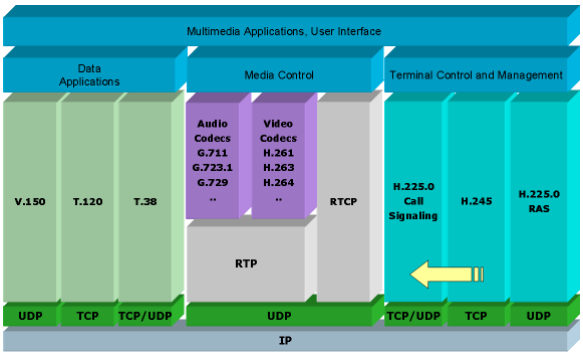

Figure 6: Celoten sklad protokola H.323.

naprave (terminale, usmerjevalnike (angl. MCUs), prehode vratarje, in zaključne elemente).

Terminali so naprave katere tipično uporablja končni uporabnik (telefoni, programski odjemalci, konferenčni sistemi ...). Usmerjevalniki povezujejo oziroma združujejo terminale ali skupino le-teh med seboj. Prehodi skrbijo za združljivost med različnimi tehnologijami, ki se uporabljajo pri povezovanju naprav (PTSN, ISDN). Vratarji niso obvezni za delovanje sistema skrbijo pa za registracijo končnih naprav, avtentikacijo uporabnikov, preslikavo naslovov, dovoljenja uporabnikov in/ali naprav. Vratarji med seboj uporabljajo protokol RAS (angl. Remote Access Service). Zaključni elementi prav tako niso potrebni, uporabljajo pa se za nadzor, upravljanje terminalov in vodenje računov znotraj upravljalske domene. Po analogiji spominjajo na naprave RAS[1] (angl. Remote Access Server) [11].

3.1.1 Primer vzpostavitve klica

Faze pri vzpostavitvi klica pri protokolu H.323 (slika 7).

1. Setup (Namera o vzpostavitvi povezave z napravo.)
2. Setup acknowledge (Klicana naprava želi komunicirati s klicočo.)
3. Call Porceeding (Potrditev klicane naprave, da ima vse potrebne informacije za usmeritev klica.)
4. Progress (Obvestilo prehoda, da klic v izvajanju.)
5. Alerting (Obvestilo klicane naprave, da je pričela z zvonenjem.)

[1]Ni enako kot prej omenjeni RAS (Registration, Admission and Status).

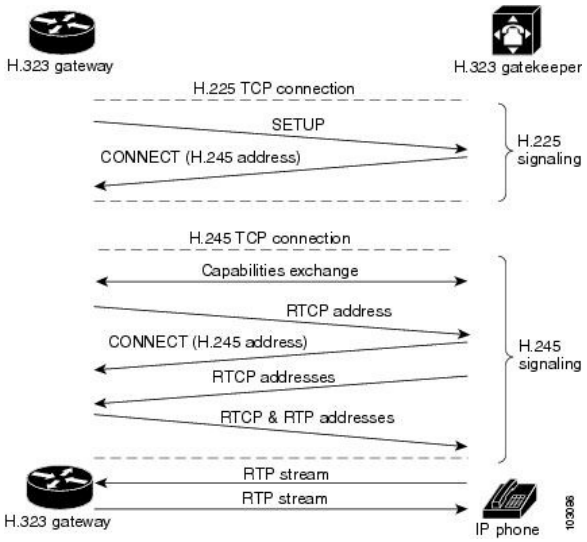

Figure 7: Primer vzpostavitve klica pri protokolu H.323.

6. Connect (Obvestilo klicane naprave, da je klic sprejet - uporabnik je dvignil slušalko.)
7. User Information (Dodatna, (večinoma) nenujna obvestila o trajajočem klicu.)
8. Release Complete (Obvestila o sprostitvi klica.)
9. Status Inquiry (Poizvedovanje o statusu trenutnega klica.)
10. Status (Sporočilo kot odgovor na poizvedovanje o statusu trenutnega klica.)
11. Information (Dodatne informacije o klicu.)
12. Notify (Sporočila o spremembah, ki so nastale med klicem.)

3.2 Skype

VoIP aplikacija Skype je zelo popularna, vendar tudi predmet številnih forenzičnih raziskav, zaradi dobrih sposobnosti prečkanja NAT[12] in zaobitja požarnega zida. Katerikoli Skype klient z nameščeno eno Skype aplikacijo na računalniku z namenom opravljanja VoIP klicev, lahko neželeno postane super vozlišče na Skype komunikacijski poti za vzdrževanje Skype omrežja, kar je še posebej riskantno za korporacije. Z analizo samo Skype prometa v njegovem komunikacijskem omrežju bi bilo mogoče zaznati Skype UDP vtičnike. To bi omogočalo blokiranje Skype prometa.

4. TEŽAVE TEHNOLOGIJE VOIP

Poleg že opisanih težav pri povezovanju naprav, ki so v omrežjih varovanimi s požarnim zidom in/ali povezane v medmrežje preko NAT-a.

4.1 Quality of service

Komunikacija prek IP omrežja je manj zanesljiva v primerjavi s standardnim PSTN telefonskim omrežjem, ker nima omrežnega mehanizma, ki bi zagotavljal da se paketi ne izgubijo in so dostavljeni v pravilnem vrstnem redu. VoIP telefonija se lahko sreča z raznovrstnimi problemi kot so latenca, izguba paketov in fazno trepetanje (jitter) [13]. Usmerjevalniki običajno promet obdelujejo po FIFO vrstnem redu. Lahko se pa zgodi, da v usmerjevalnikih z veliko obremenitvijo, pride do presežka limita latence ki je dovoljena za VoIP. Ni mogoče nadzorovati, da bi se paketi dostavljali s fiksnim zamikom, saj le ti nastajajo z razdaljo, ki jo potrebujejo, da pridejo do cilja. To je še posebej opazno pri satelitskih omrežjih. En od načinov znižanja latence je z označevanjem zvočnih paketov, saj so občutljivi na časovne zamike, z metodo kot je DiffServ. Obstajajo tudi različni protokoli, ki definirajo specifikacije, za dobro kvaliteto VoIP klicev. Ti so RTCP, SIP, H.460.9, H.248.30 in MGCP.

4.2 Klic v sili

Standardno PSTN telefonsko omrežje je klasično telefonsko omrežje, ki ga vzdržuje telefonski ponudnik. S tem je tudi določena fizična lokacija. Ko je iz takega omrežja klicana ena izmed številk za klice v sili, je službi za pomoč takoj prikazana fizična lokacija klicatelja, ki jo imajo shranjeno v podatkovni bazi. Pri IP telefoniji take direktne povezave med fizično lokacijo in komunikacijo ni [14]. Celo ponudnik fizične infrastrukture, kot je na primer ponudnik DSL, lahko ve le približno lokacijo naprave, ki je osnovana glede na IP naslov, saj nekateri ISP ponudniki samodejno ne beležijo, komu so bili dodeljeni avtomatski IP naslovi.

4.3 Napajanje

Druga težava VoIP je, da zanjo potrebujemo električno napajanje [14]. Tradicionalna telefonija je namreč priključena direktno na telefonskega ponudnika, kateri zagotavlja napajanje za analogno telefonijo. IP telefoni in VoIP telefonski adapterji so priključeni na usmerjevalnike ali na modeme. Kot rešitev obstajajo tudi modemi z vgrajeno baterijo ki zagotavljajo napajanje za nekaj ur. Tipično so to naprave ki lahko uporabljajo tudi analogno tehnologijo ali pa se povežejo na naš mobilni telefon. Ta težava je tudi povezana s prejšnjo saj v nujnih primerih, brez elektrike ne moremo poklicati nikogar, torej tudi telefonskih številk za klice v sili.

4.4 Varnost

VoIP je občutljiv na črve, viruse in vdore. Znani so DOS napadi, snemanje pogovora, kraja seje in nato uporaba plačljivih storitev, itd.

4.4.1 Oddaljeni napadi

Kolumbijski raziskovalci so pokazali, kaj lahko naredijo z vdorom v Cisco VoIP telefon [15]. Hekerji torej lahko oddaljeno spremenijo telefon v navaden mikrofon in prisluškujejo iz kjerkoli. Cisco je globalno najbolj znan VoIP ponudnik, saj ima na milijone VoIP telefonov po svetu, tudi v podatkovno občutljivih podjetjih in vladah. Napravo thingp3wn3r so priključili v serijska vrata in nanj naložili zlonamerno kodo. S posebnim ukazom so dosegli da se je sistem zrušil in izpisal celoten pomnilnik. Z analizo pomnilnika so uspeli spremeniti program na telefonu, kateri je lahko okužil druge računalnike in naprave kot so, na primer tiskalniki. Lahko so dosegli, da telefon ves čas snema pogovore v prostoru tako, da uporabnik tega sploh ne zazna. Zanimivo je, da ima tak telefon tudi predsednik Obama [16].

4.5 Procesorska moč

Problem z VoIP je tudi, da so ti klici odvisni od posameznih računalnikov [14]. V primeru da odpremo zahteven program med samim klicem se lahko procesor preobremeni in kvaliteta pogovora se zniža. V najslabšem primeru pa se lahko cel sistem sesuje. VoIP klici so torej v odvisnosti veliko napak, ki jih ima normalen računalnik.

5. VOIP IN FORENZIKA

VoIP predstavlja paketno osnovano internetno tehnologijo za zvočno komunikacijo v primerjavi s tradicionalnim telefonskim omrejžem. To seveda vpliva na kazenski pregon saj prisluškovanje na žici ni več možno. Potrebna je nova arhitektura za zakonito prestrezanje prometa VoIP, vendar ker paketi potujejo po različnih poteh je njena implementacija težka. Možne subjekte prestrezanja lahko razdelimo na dve področji. Tiste ki pripadajo ponudniku internetnih storitev (ISP), in tiste, ki pripadajo LEA (Law Enforcement Agency), kateri se lahko nahajajo znotraj ISP ali zunaj njega. Subjekti povezani z ISP vključujejo signalizacijo, namestitev, vzdrževanje in zaključevanje IP klicev. Zbiranje podatkov IP zvočnega prometa je lahko realizirano na istem pod omre-žju kot je VoIP usmerjevalnik, kateri se poveže do obstoječe telefonske linije. Subjekti v povezavi z LEA lahko obstajajo znotraj ISP arhitekture vendar ostajajo pod nadzorom LEA saj zajeti podatki potrebujejo dovoljenje ISPja za dostop do dekripcijskih ključev.

Bolj kot je omrežje centralizirano, bolj enostavno je zakonito prestrezanje. Na žalost ne obstaja ena sama naprava, ki bi prestrezala ves VoIP promet ampak je celo značilna visoka stopnja decentralizacije, zlasti za mobilne uporabnike, ki se povezujejo na internet za krajša časovna obdobja. To lahko povzroči premik izven dosega vozlišča nadzorovanega pod vodstvom organov pregona kjer je prestrezanje zahtevano od internetnih ponudnikov. Na primer, Skype uporablja dobro enkripcijo glede na objavljene standarde (DES in AES). To od LEA zahteva pridobitev ključev od podjetja Skype v primeru, če potrebujejo dekripcijo zajetih podatkov VoIP.

Trenutno obstaja nekaj modelov za preiskavo v digitalni forenziki. Ogrodje za digitalno forenziko DFRWS nam zagotavlja naslednje zaporedne korake za analizo:

- Identifikacija
- Ohranjanje
- Zbiranje
- Pregled
- Analiza
- Predstavitev

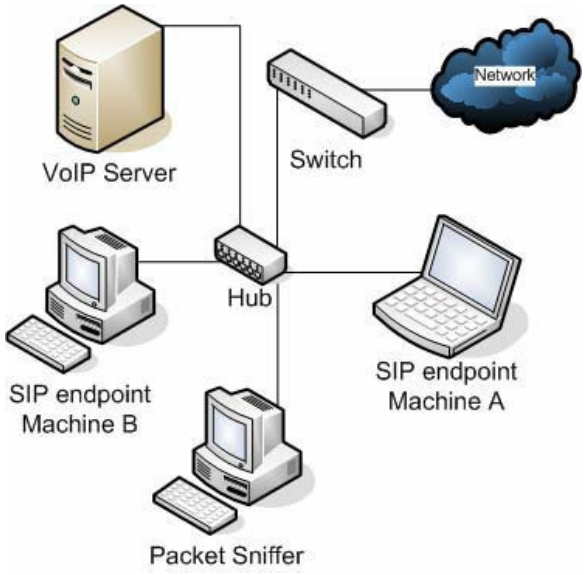

Figure 8: Postavitev in vloge naprav v eksperimentu.

```
tcpdump -nnvvXSs 1514 host \
192.168.1.193 -i eth0 -w voip.cap
```

Figure 9: Zajem prometa za/iz naprave klicoče na usmerjevalniku.

Pregled in analiza zajetega pomnilnika se izvajata v načinu samo za branje, kar pomeni da ostanejo prvotne informacije nespremenjene.

6. EKSPERIMENTI

Cilj eksperimenta je ugotoviti, ali se kakršnakoli informacija o klicu shrani oziroma ohrani na trdem disku in/ali pomnilniku naprave iz katere je bil narejen klic[6]. Pri ponovitvi eksperimentov smo upoštevali strukturo in vlogo naprav, kot je predstavljeno v članku in povzeto v sliki 8. Predhodno smo se registrirali in pridobili naslov SIP pri ponudniku VoIP storitev Ekiga. Naprava s katero kličemo uporablja 32-bitni operacijski sistem Debian, temelji na jedru Linux in osnovnimi programi za upravljanje operacijskega sistema GNU. Na napravi uporabljamo VoIP odjemalec Ekiga. Za testni klic smo poklicali kar "Echo test"odzivnik in počakali 30 sekund, nato pa klic prekinili. Promet zajemamo zunaj govorečih naprav, v usmerjevalniku katerega poganja strojna programska oprema OpenWRT, s programom tcpdump (ukaz 9). Zajet promet analiziramo s programom wireshark. Promet je zaradi poenostavitve in lažje analize nekriptiran.

Prva ugotovitev je, da lahko s prisluškovanjem znotraj lokalnega omrežja brez težav rekonstruiramo celoten klic, vključno z avdio in video komunikacijo (sliki 10 in 11). Vendar se tu postavi vprašanje ali je to dovolj dober dokaz na sodišču? Promet na mreži je enostavno ponarediti z npr. napadom replay attack. Večjo stopnjo objektivnosti in verodostojnosti dokaza bi dosegli, če bi ključne informacije klica dejansko našli na fizični napravi, s katere je bil opravljen klic.

```
dd if=/dev/sda of=/mnt/storage/debian.img
```

Figure 12: Zajem slike diska.

```
dd if=/dev/fmem of=debian_mem.bin bs=1024
```

Figure 13: Zajem pomnilniške slike.

Za potrebe seminarske naloge smo napisali skripto v programskem jeziku python, ki v izpisu diska ali pa v pomnilniškem izpisu poišče ključne elemente seje. Za ključne elemente seje smatramo vse tiste elemente s katerimi je mogoče enolično identificirati določen klic. V konkretnem primeru je ta identifikator:
"Call-ID: 381d54a4-ccd2-e311-90e9-00155d014713@debian32".

6.1 Eksperiment 1

Naša hipoteza je, da bomo na disku odjemalca našli podatke, ki bodo enolično določili klic med vsemi podatki zajetimi na usmerjevalniku. Po opravljenem klicu zajamemo podatke na disku (ukaz 12).

Na disku nismo našli nobenih sledi, tj. delcev paketov, ki bi lahko predstavljali podatke klica.

6.2 Eksperiment 2

V tem eksperimentu pričakujemo, da se bodo podatki, ki enolično določajo klic nahajali v pomnilniškem prostoru odjemalca. Za zajem pomnilnika smo najprej namestili modul fmem, da lahko zajamemo celotno pomnilniško sliko (ukaz 13).

Z našo skripto smo na različnih lokacijah našli niz "Call-ID" (slika 14), kar je dovolj za identifikacijo klica. Našli smo tudi en paket identičen tistemu, ki je bil zajet na usmerjevalniku.

7. ZAKLJUčEK

Za forenziko na področju protokola VoIP velja, da je to še precej nerazvito področje. Da ni (prosto dostopnih) orodji za analizo protokola VoIP in, da se tako stanje ohranja naprej bi deloma pripisali dejstvu, da ta orodja verjetno obstajajo, a so v lasti državnih tajnih služb, ki nimajo interesa, da bi ta orodja postala javna. Deloma tako stanje ustreza tudi ponudnikom ter proizvajalcem strojne in programske opreme, saj smo v članku predstavili kako "ranljiv"je pravzaprav velik del prometa VoIP. Dokler je orodij za analizo prometa VoIP malo, večina proizvajalcev in uporabnikov uživa lažen občutek varnosti, t.i. "Security through obscurity".

8. REFERENCES

[1] I. D. D. A. S. J. S. Malcolm. Extraction of electronic evidence from voip: Forensic analysis of a virtual hard disk vs ram. *The Journal of Digital Forensics, Security and Law*, 2012.
[2] J. Postel. User datagram protocol. *IETF RFC 768*, 1980.
[3] J. Postel. Internet protocol. *IETF RFC 791*, 1981.
[4] J. Postel. Transmission control protocol. *IETF RFC 793*, 1981.

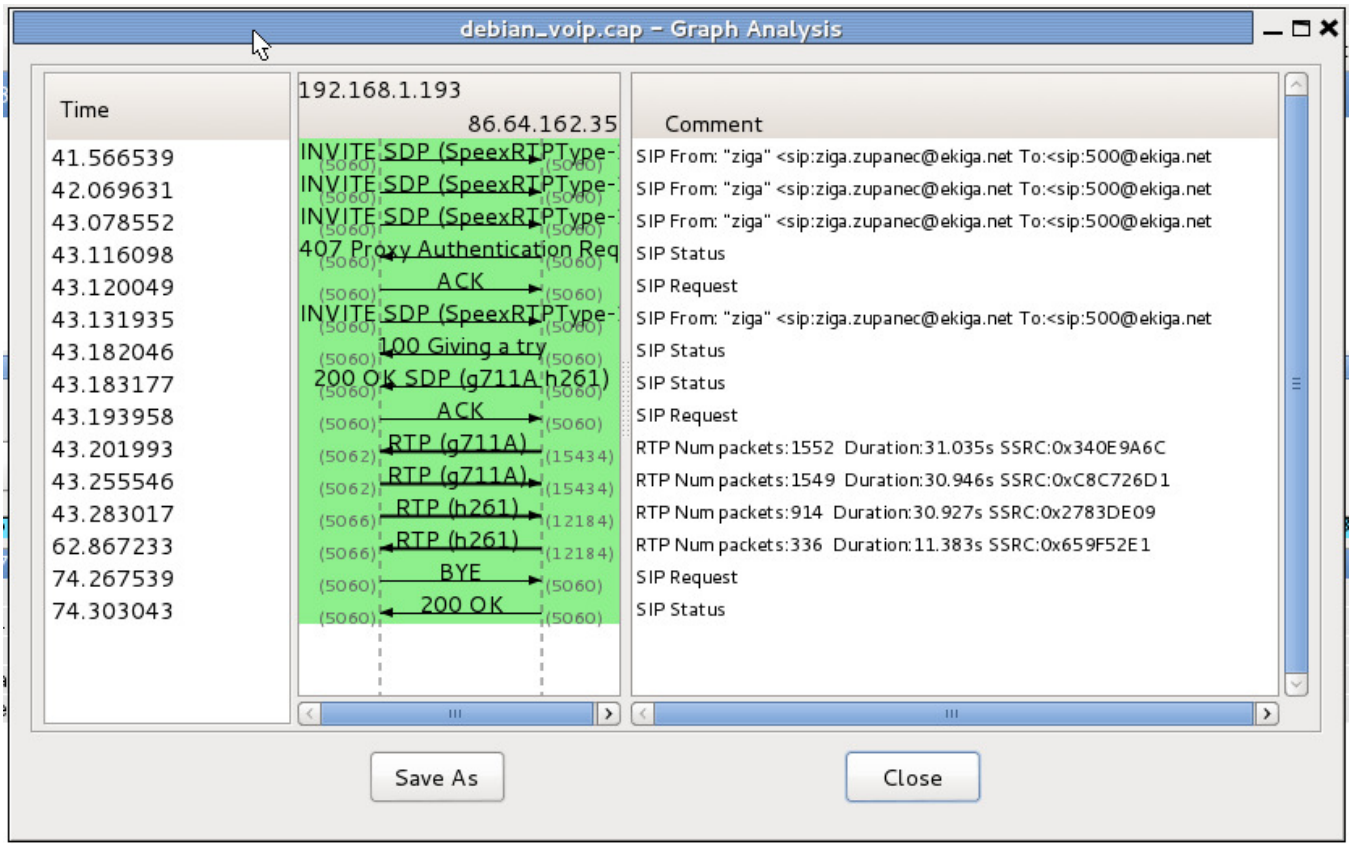

Figure 10: Vzpostavitev in potek klica.

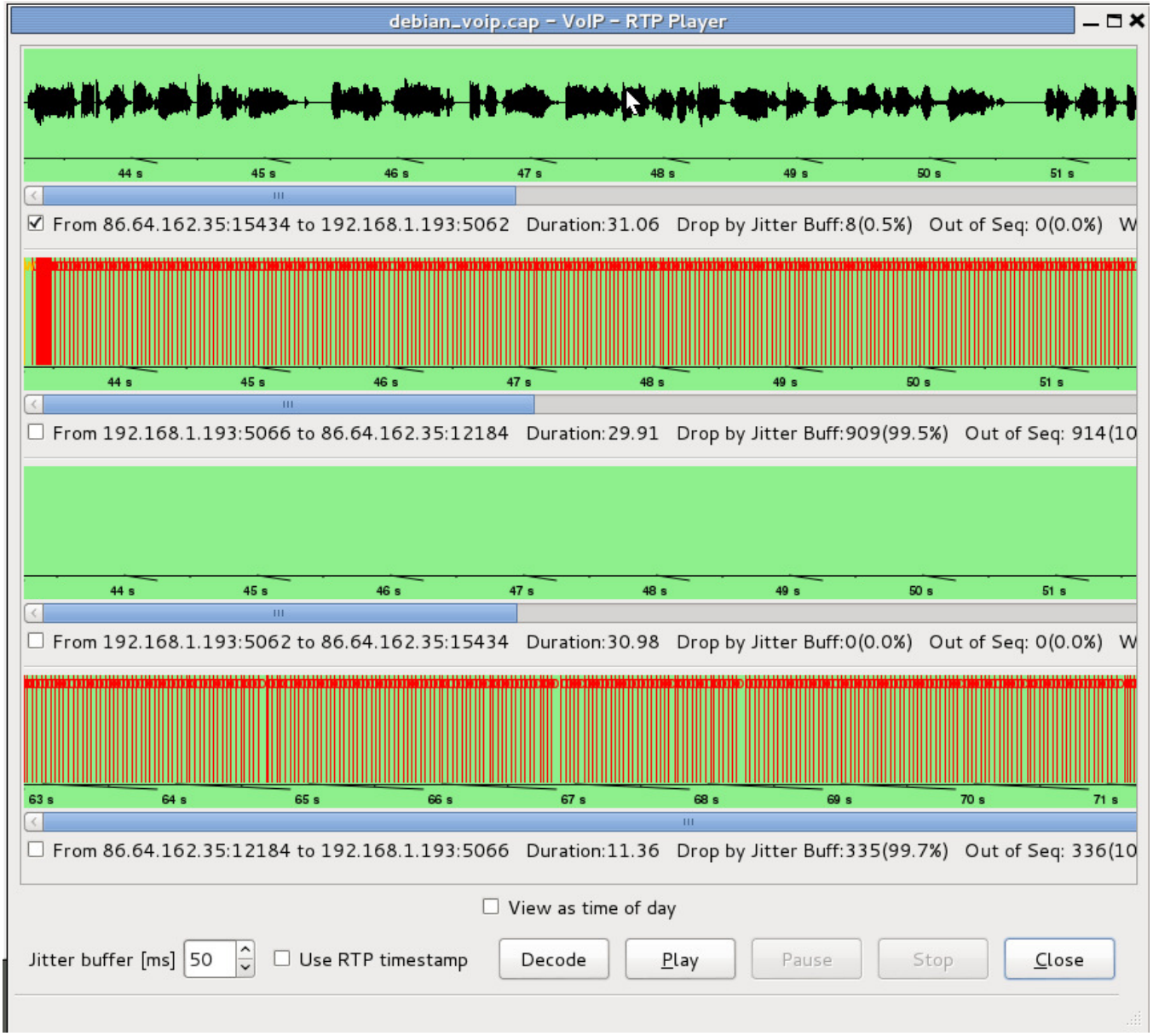

Figure 11: Rekonstrukcija zvočnega zapisa s programom wireshark.

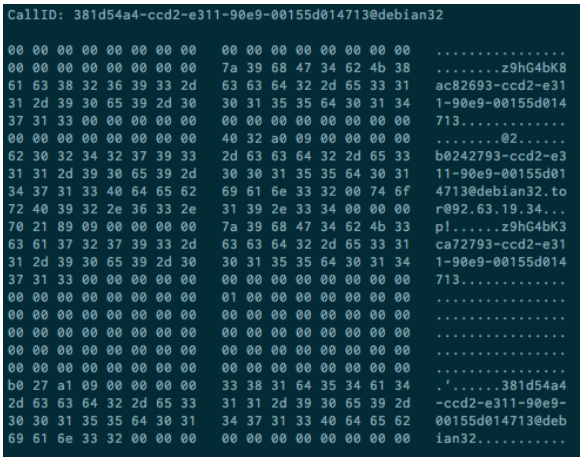

Figure 14: Del pomnilniške slike, kjer smo našli vrednost "Call-ID".

[5] J. E. a. Rosenberg. Sip: Session initiation protocol,. *IETF RFC 3261*, 2002.

[6] M. Simon. Packet reconstruction software: Defence and systems. *Institute (DASI) at the University of South Australia*, 2008.

[7] Wikipedia. `http://wiki.ekiga.org/index.php/Understanding_NAT/firewall_issues_with_SIP_clients_(eg_ekiga)`.

[8] Wikipedia. `https://en.wikipedia.org/wiki/STUN`.

[9] Wikipedia. `http://wiki.ekiga.org/index.php/Manual#H.323_addresses`.

[10] Wikipedia. `https://en.wikipedia.org/wiki/H.323`.

[11] Wikipedia. `https://en.wikipedia.org/wiki/Registration,_Admission_and_Status`.

[12] Wikipedia. `http://en.wikipedia.org/wiki/NAT_traversal`.

[13] Wikipedia. `http://en.wikipedia.org/wiki/Voice_over_IP#Quality_of_service`.

[14] Wikipedia. `http://computer.howstuffworks.com/ip-telephony5.htm`.

[15] Wikipedia. `http://webcache.googleusercontent.com/search?q=cache:ZvS3tmAMEvcJ:docwiki.cisco.com/wiki/Cisco_IOS_Voice_Troubleshooting_and_Monitoring_--_H.323-Related_Standards&client=iceweasel-a&hl=en&strip=1`.

[16] Wikipedia. `http://geeknizer.com/hack-any-cisco-voip-phone/`.