Kauno technologijos universitetas Informatikos fakultetas Kompiuterių katedra

Laboratorinis darbas

VoIP saugos analizė

Paruošė: Tomas Adomkus

Atliko : Eligijus Kiudys, IFM 1-3

Kaunas, 2022

# Darbo tikslas:

naudojant „Wireshark“ ir „Omnipeek“ paketų analizatorius atlikti VoIP balso sesijos

analizę.

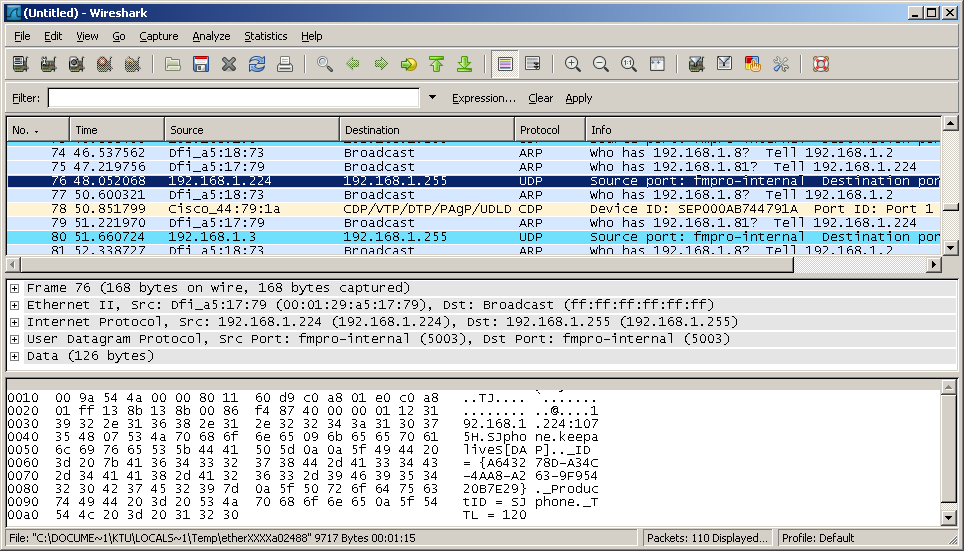
# Darbo uždaviniai:

* išsiaiškinti laboratorinio darbo metu naudojamą tinklo struktūrą;
* išsiaiškinti į tinklą sujungtų įrenginių IP adresus;
* susipažinti su „Wireshark“ ir „Omnipeek“ paketų analizatoriais;
* naudojantis „Wireshark“ ir „Omnipeek“ paketų analizatoriais atlikti VoIP balso sesijų analizę.

# Darbo eiga.

1. Atlikti paketų analizę naudojant „Wireshark“ paketų analizatorių, gautus rezultatus pateikti 1 lentelėje.
   1. Paleisti programą „Wireshark“.
   2. Aktyvuoti paketų „gaudymą“: Capture -> Interfaces -> Parinkti tinklo plokštę, turinčią jūsų kompiuterio IP adresą -> Start.
   3. Paleisti „Ekiga“ programinį telefoną ir užmegzti balso ryšį **su kaimyniniu kompiuteriu**: Paleisti programą „Ekiga“ -> Adresų lauke įvesti signalizacijos protokolą ir kaimyninio kompiuterio IP adresą (pvz.: sip:192.168.0.2 arba h323:192.168.0.2) -> paspausti  mygtuką -> Kaimyniniame kompiuteryje pradėjus skambėti telefonui paspausti  -> Balso sesija užmegzta, trumpai VoIP telefonu pasikalbėti su kaimynu (5 – 10 s.) -> Nutraukti balso sesiją, tam paspausti  mygtuką.
   4. „Wireshark“ programoje sustabdyti paketų „gaudymą“: Capture -> Stop.
   5. Patyrinėti balso paketų struktūrą ir dydžius. 1 paveikslėlyje pateiktas „Wireshark“ programa

„pagautų“ paketų pavyzdys, čia: 1 lange pateikti „pagautų“ skirtingų protokolų paketai, 2 lange pateikta atitinkamą protokolą naudojančio paketo struktūra. Šiuo atveju galima pastebėti, kad paketo nešama informacija yra pasiskirsčiusi keturiuose OSI lygmenyse. 3 lange pateikta paketo nešama informacija. Kokie pagrindiniai skirtumai tarp įeinančių ir išeinančių balso paketų?



**1**

**2**

**3**

**1 pav.** Darbinis „Wireshark“ programos langas

* 1. Išnagrinėti pateiktą „pagautų“ paketų statistiką:
     1. Statistics -> Paeiliui pasirinkti ir išnagrinėti šias statistikas: **Summary** -> peržiūrėti pateiktą statistiką -> Close, **Protocol Hierarchy Statistics** -> peržiūrėti pateiktą statistiką -> Close, **Packet Lengths...** -> Create Stat -> peržiūrėti pateiktą statistiką -> Close -> Cancel, **Flow Graph...** -> OK -

> peržiūrėti pateiktą statistiką -> Close -> Cancel.

* + 1. Telephony -> RTP -> Show All Sreams -> Atkreipti dėmesį į kokybines charakteristikas: Lost, Max Delta (ms), Max Jitter (ms) -> Norint atlikti detalesnę balso sesijos paketų kokybinių

charakteristikų analizę, pasirinkti norimą nagrinėti balso paketų srautą -> Analyze -> Panagrinėti anksčiau išvardintas kokybines charakteristikas -> Close -> Close.

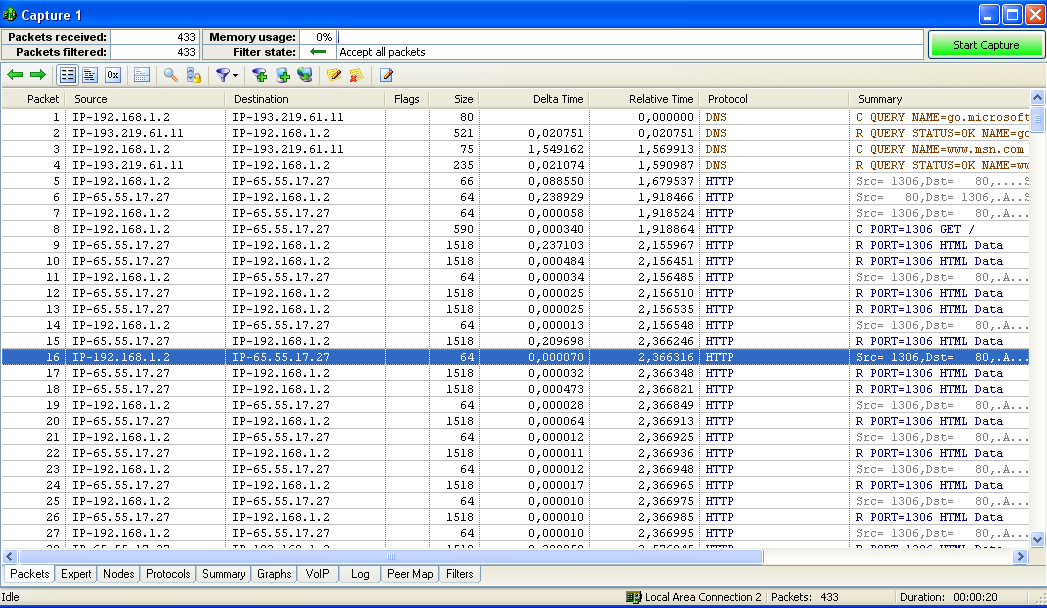
* + 1. Telephony -> VoIP Calls ->Pasirinkti nagrinėjamą balso paketų srautą -> Graph -> Panagrinėti pateiktą balso sesijos sudarymo grafą -> Close. Player -> Decode -> Varnelėmis pažymėti norimus pasiklausyti balso paketų srautus -> Play -> Close.
  1. Uždaryti „Wireshark“ programą.

1. Atlikti paketų analizę naudojant „Omnipeek“ paketų analizatorių, gautus rezultatus pateikti 1 lentelėje.
   1. Paleisti programą „Omnipeek“.
   2. Aktyvuoti paketų „gaudymą“: New Capture -> „Local Area Connection x“ tinklo plokštę -> OK

-> Start Capture.

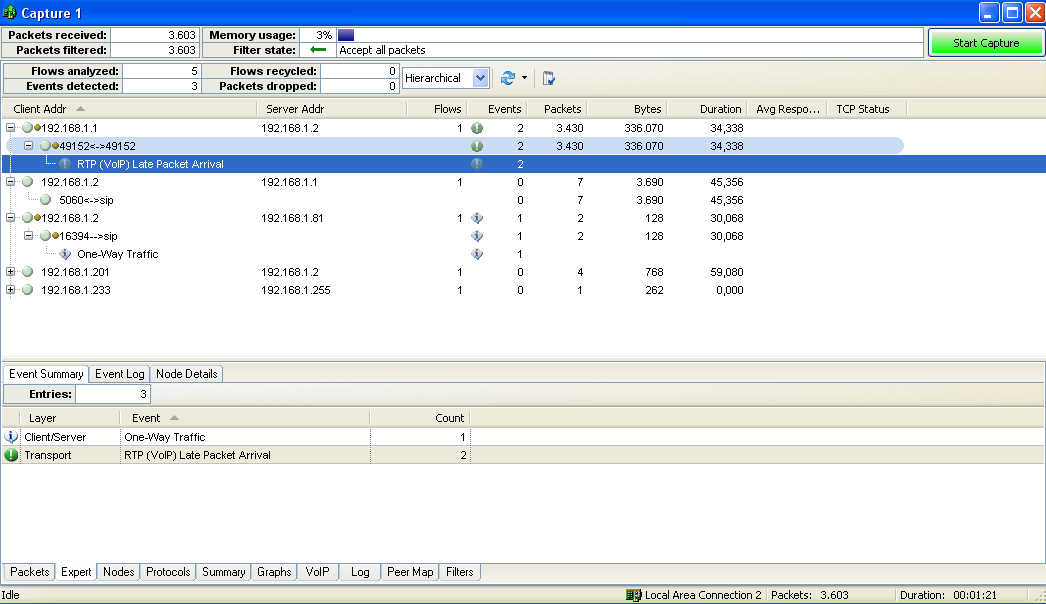
* 1. Paleisti „Ekiga“ programinį telefoną ir užmegzti balso ryšį **su kitu, nei pirmuoju atveju, kaimyniniu kompiuteriu**: Paleisti programą „Ekiga“ -> Adresų lauke įvesti signalizacijos protokolą ir kaimyninio kompiuterio IP adresą (pvz.: sip:192.168.0.2 arba h323:192.168.0.2) -> paspausti  mygtuką -> Kaimyniniame kompiuteryje pradėjus skambėti telefonui paspausti  -> Balso sesija užmegzta, trumpai VoIP telefonu pasikalbėti su kaimynu (5 – 10 s.) -> Nutraukti balso sesiją, tam paspausti  mygtuką.
  2. „Omnipeek“ programoje sustabdyti paketų „gaudymą“, tam paspausti „Stop Capture“.
  3. Patyrinėti balso paketų struktūrą ir dydžius, tam ant pasirinkto paketo du kartus spragtelti kairiu pelės klavišu. Kokie pagrindiniai skirtumai tarp įeinančių ir išeinančių balso paketų?
  4. Išnagrinėti pateiktą „pagautų“ paketų statistiką. Paketų analizės pavyzdžiai pateikti 2 – 11 pav.

**Ypatingą dėmesį atkreipkite į 9 – 11 pav.**, čia pateikta detali balso sesijos analizė.

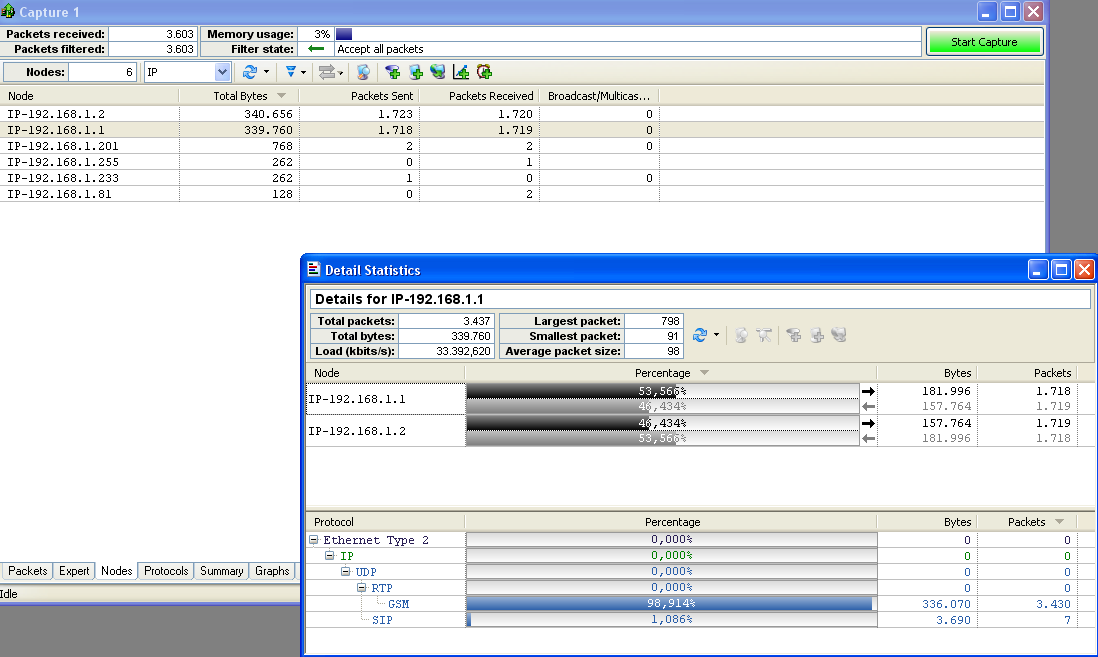


Paketo vėlavimo laikas

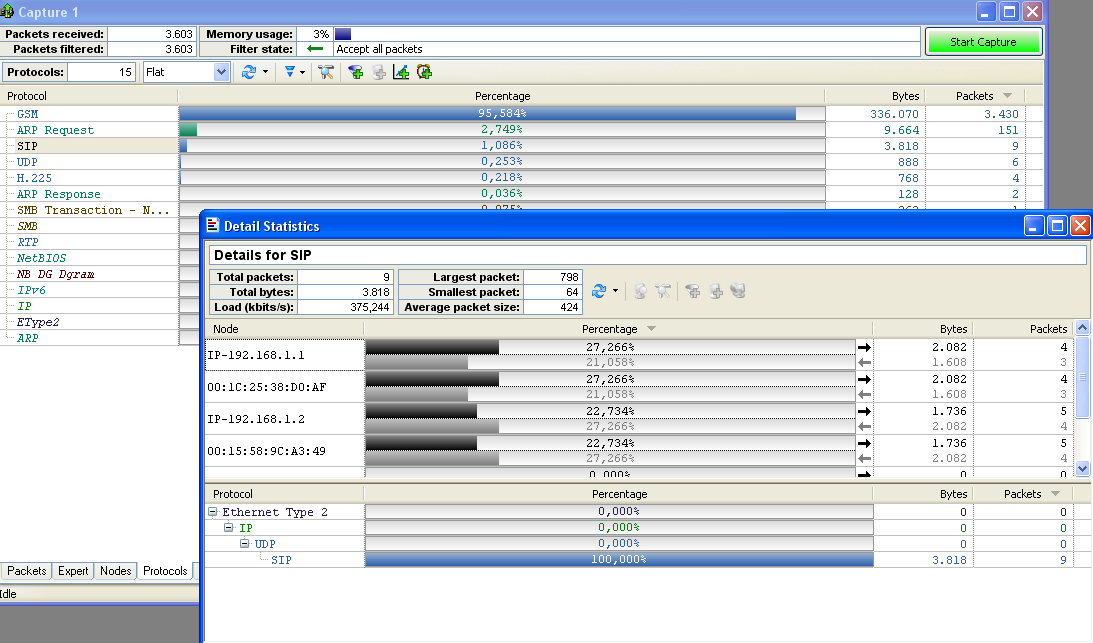
* + 1. **pav.** Grafoje „Packets“ matyti „pagautų“ paketų sąrašas, kuriame matosi siuntėjo, bei gavėjo IP adresai, paketų dydžiai baitais, paketo vėlavimo laikas, paketo „pagavimo“ laikas, balso kodavimo ir suspaudimo algoritmas.



* + 1. **pav.** Grafoje „Expert“ matyti IP adresai vartotojų, tarp kurių vyko balso paketų (RTP), bei signalizacijos paketų (SIP) perdavimas, balso perdavimo srautų skaičius, bendraujančių pusių skaičius, perduotų paketų skaičius, perduotos informacijos kiekis baitais, sesijų trukmės.

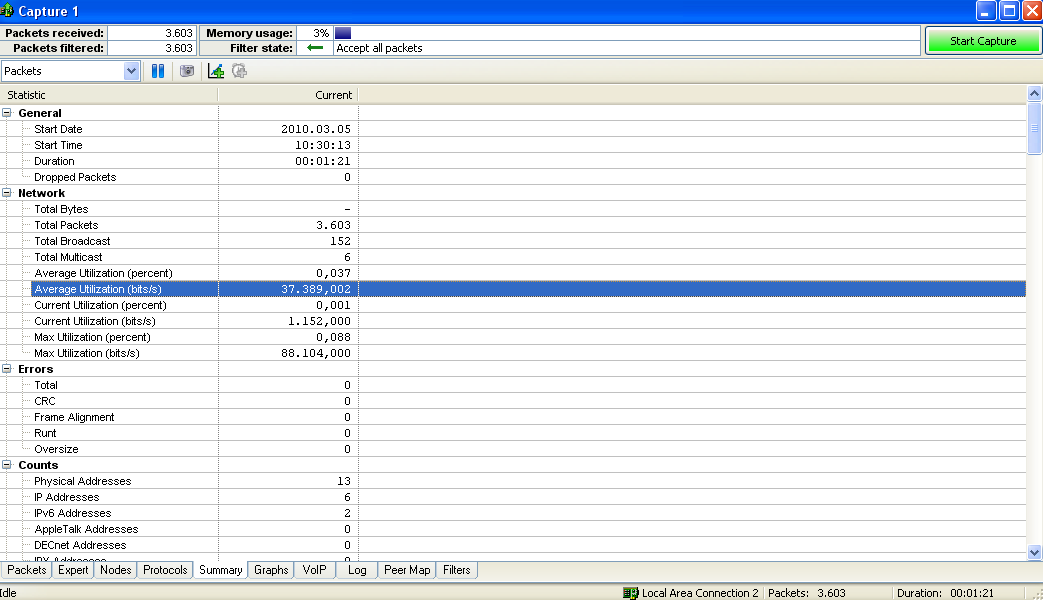


* + 1. **pav.** Grafoje „Nodes“ matyti tarp kokių tinklo mazgų, kiek paketų buvo perduota. Išskleidus tinklo mazgą, kuris dalyvavo balso paketų perdavimo sesijoje galima detaliau matyti išsiųstų ir priimtų paketų grafines priklausomybes, bei perduotų balso (RTP) ir signalizacijos (SIP) paketų procentinį pasiskirstymą.

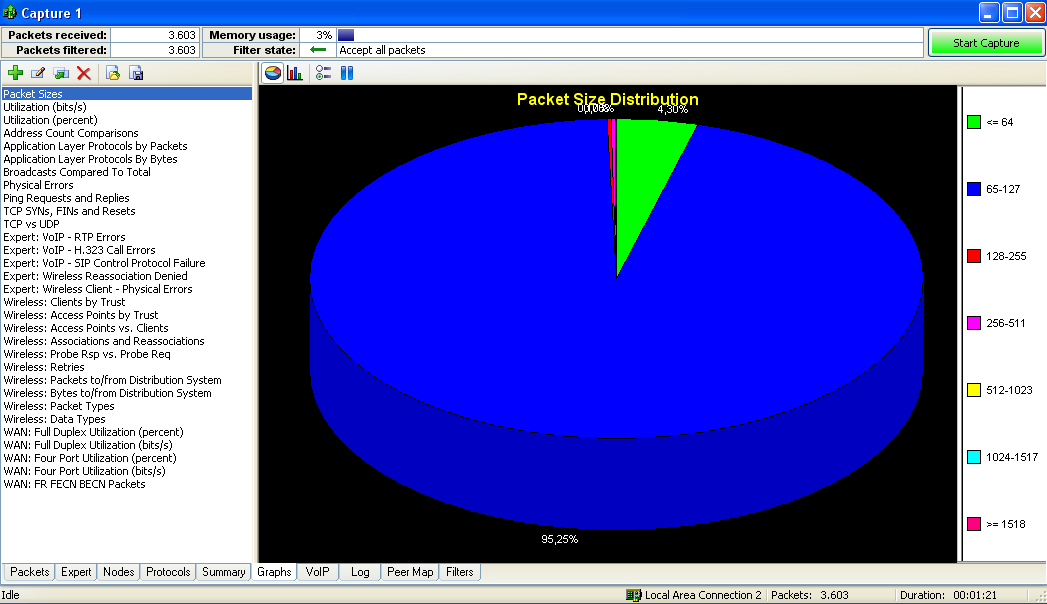


* + 1. **pav.** Grafoje „Protocols“ matyti procentinis naudojamų paketams perduoti protokolų pasiskirstymas.

Išskleidus pasirinktą protokolą (pvz., SIP) galima pamatyti bendraujančių tinklo mazgų IP, bei MAC adresus, kiek paketų iš pastarųjų mazgų buvo išsiųsta ir priimta. Žemiau matyti, kad SIP paketai buvo perduodami tinklu naudojant UDP protokolą, o UDP datagrama buvo perduodama naudojant IP protokolą.

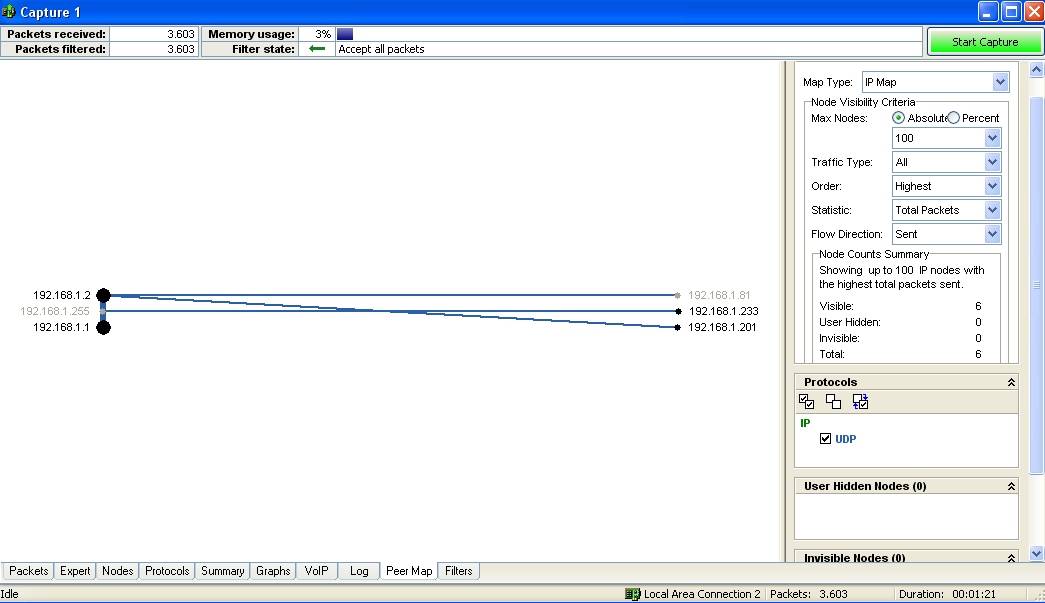


* + 1. **pav.** Grafoje „Summary“ apibendrinta perduotų tinkle paketų statistika. Reikėtų atkreipti dėmesį į tinklo išnaudojimo (Utilization) statistiką.

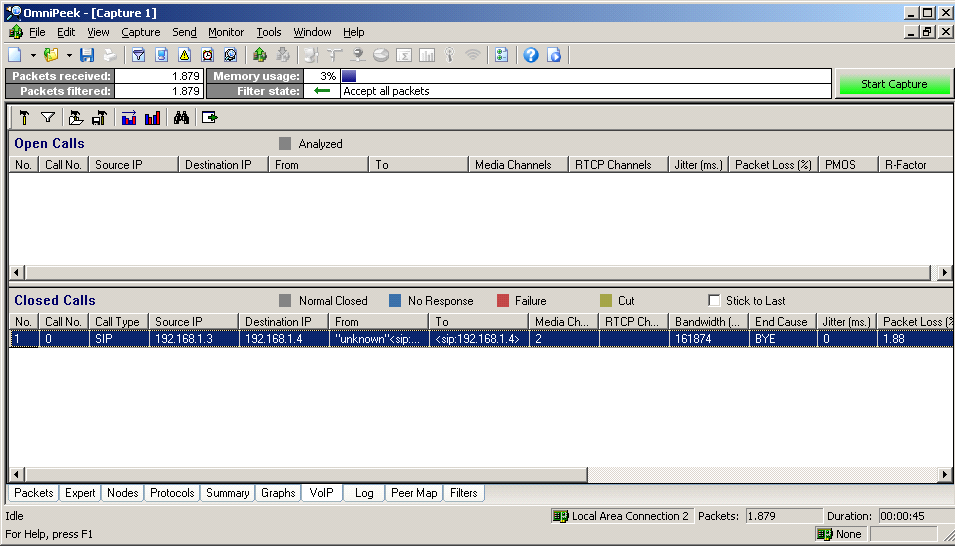


* + 1. **pav.** Grafoje „Graphs“ matyti perduotų tinkle paketų statistikos grafinės priklausomybės. Reikėtų atkreipti dėmesį į perduotų paketų dydžių (Packet Sizes), bei tinklo išnaudojimo (Utilization)

statistiką.

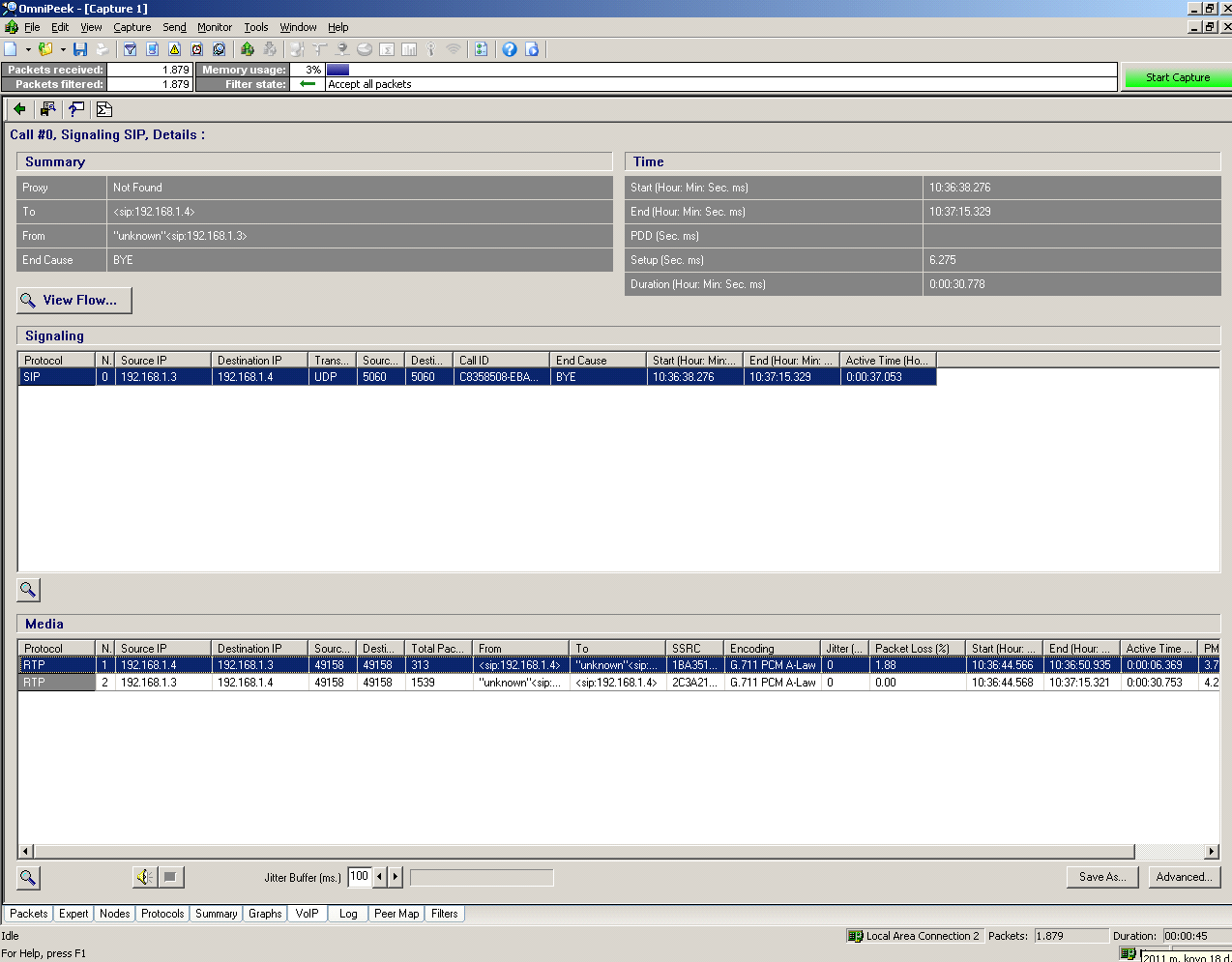


* + 1. **pav.** Grafoje „Peer Map“ matyti perduodamų tarp tinklo mazgų duomenų srautų pasiskirstymo grafinis „žemėlapis“.



Kairiu pelės klavišu du kartus spragtelti ant pasirinktos balso sesijos

* + 1. **pav.** Grafoje „VoIP“ matyti perimtos balso sesijos. Reikėtų atkreipti dėmesį į sesijų kokybines charakteristikas, t.y., pralaidumą (Bandwidth), fliuktuacijas (Jitter), paketų praradimą (Packet Loss), bei PMOS.



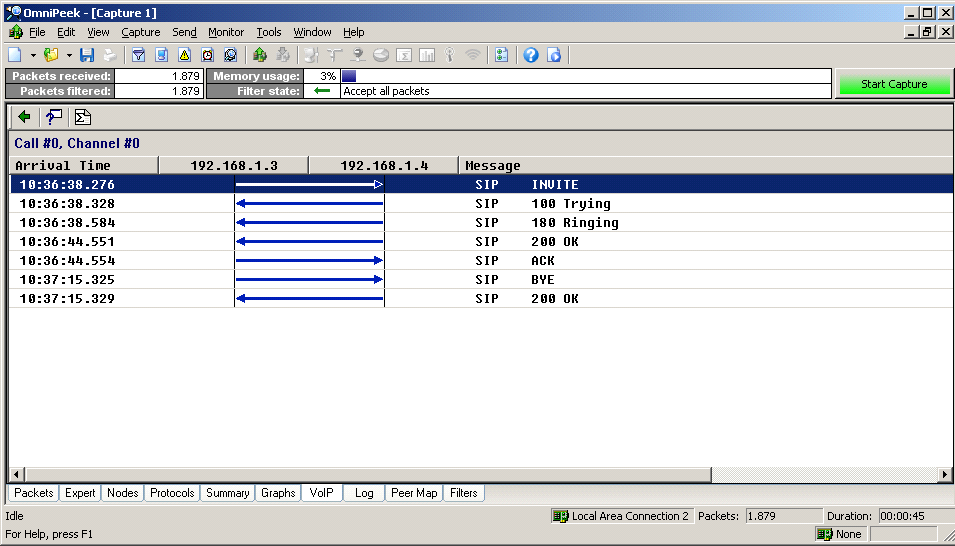
Grįžti į prieš tai buvusį langą

Kairiu pelės klavišu du kartus spragtelti ant signalinių pranešimų perdavimo sesijos

Spausti norint pasiklausyti perimtos balso sesijos metu vykusį pokalbį

Kairiu pelės klavišu du kartus spragtelti ant pasirinktos balso sesijos krypties

* + 1. **pav.** Analizuojama perimta balso sesija susideda iš dviejų skirtingų srautų, t.y., signalinių pranešimų, bei balso paketų.



Grįžti į prieš tai buvusį langą

* + 1. **pav.** Signalinių pranešimų, kurie buvo panaudoti sudarant perimtą balso sesiją, grafas.
  1. Uždaryti „Omnipeek“ programą.

1. VoIP sesijos analizę reikia atlikti keturiais skirtingais scenarijais ir gautus rezultatus pateikti 1-oje lentelėje:
2. Pasirinkti H.323 signalizacijos protokolą ir skambinti iš PC1 į PC2, perduodamų paketų analizę atlikti „Wireshark“ paketų analizatoriumi;
3. Pasirinkti SIP signalizacijos protokolą ir skambinti iš PC1 į PC2, perduodamų paketų analizę atlikti „Wireshark“ paketų analizatoriumi;
4. Pasirinkti H.323 signalizacijos protokolą ir skambinti iš PC2 į PC1, perduodamų paketų analizę atlikti „Omnipeek“ paketų analizatoriumi;
5. Pasirinkti SIP signalizacijos protokolą ir skambinti iš PC2 į PC1, perduodamų paketų analizę atlikti „Omnipeek“ paketų analizatoriumi;

**1 lentelė.** Perimtų VoIP paketų analizė naudojant „Wireshark“ ir „Omnipeek“ paketų analizatorius.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Klausimas** | **„Wireshark“, H.323** | **„Wireshark“, SIP** | **„Omnipeek“, H.323** | **„Omnipeek“, SIP** |
| 1. | Šaltinio MAC adresas | 08:00:27:95:7F:31 | 08:00:27:F0:A0:56 | 08:00:27:F0:A0:56 | 08:00:27:B5:B6:C9 |
| 2. | Paskirties MAC adresas | 08:00:27:F0:A0:56 | 08:00:27:95:7F:31 | 08:00:27:B5:B6:C9 | 08:00:27:F0:A0:56 |
| 3. | Šaltinio IP adresas | ﻿192.168.56.101 | ﻿192.168.56.102 | ﻿192.168.56.102 | ﻿192.168.56.103 |
| 4. | Paskirties IP adresas | ﻿192.168.56.102 | ﻿192.168.56.101 | ﻿192.168.56.103 | ﻿192.168.56.102 |
| 5. | Signalizavimo protokolas | H323 | SIP | h323 | SIP |
| 6. | Šaltinio VoIP signalizacijos  prievado numeris | 3000 | 5060 | 3000 | 5060 |
| 7. | Paskirties VoIP signalizacijos prievado  numeris | 1720 | 5060 | 1720 | 5060 |
| 8. | Balso paketų perdavimo  protokolas | RTP/UDP | RTP/UDP | RTP/UDP | RTP/UDP |
| 9. | Šaltinio balso paketų  perdavimo protokolo prievado numeris | 5062 | 5066 | 5062 | 5070 |
| 10. | Paskirties balso paketų  perdavimo protokolo prievado numeris | 5062 | 5062 | 5062 | 5062 |
| 11. | Balso kodavimo algoritmas | G.711 | Speedex | G.711 | Speedx |
| 12. | Prarastų paketų, % | - | - | 0 | - |
| 13. | Maks. vėlinimas, ms | - | - | 0 | - |
| 14. | Vid. fliuktuacijos, ms | - | - | 22.5 | - |
| 12. | MOS | - | - | 1.82 | - |

# Ataskaitoje pateikti:

* tinklo struktūrą su loginiais balso sesijų sudarymo ryšiais bei naudojamais IP adresais;
* perimtų balso sesijų signalinių pranešimų grafus (angl. Print Screen);
* „Wireshark“ ir Omnipeek“ paketų analizatorių balso sesijų pasiklausimo langus (angl. Print Screen);
* užpildytą 1 lentelę.

# Išvados :

# Darbo metu buvo atlikti keturi skambučiai : H.323 ir SIP protokolais. Buvo sukurtas virtualių mašinų tinklas, kuriame yra trys kompiuteriai, du kompiuteriai su Ubuntu operacine sistema ir vienas kompiuteris su Windows operacine sistema. Skambinau iš pirmojo Ubuntu kompiuterį į antrąjį Ubuntu kompiuterį naudojant H.323 protokolą. Skambinau iš antrojo Ubuntu kompiuterio į pirmajį Ubuntu kompiuterį naudojant SIP protokolą. Pirmųjų dviejų skambučių analizei buvo naudota „Wireshark“ programinė įranga.

# Skambinant iš antro kompiuterio į trečią buvo naudojamas H.323 protokolas. O skambinant iš trečio kompiuterio į antrą buvo naudojamas SIP protokolas. Skambučio analizei buvo. Naudojama „OmniPeek“ programinė įranga.

# Pirmo skambučio metu H.323 buvo skambinta iš pirmos virtualios mašinos į antrą, paketų klausiau su „Wireshark“ programine įranga. Gavau tokius rezultatus : Table Description automatically generated

# Nors pokalbio metu garso girdėti nėjo, bet matome, kad pokalbis įvyko. Graphical user interface, text Description automatically generated

# Pasiėmus konfigūracijos paketą iš H.323 paketų galime gauti daug naudingos informacijos :

# Matome abiejų pokalbio dalyvių MAC adresus :

# Siuntėjo adresas: 08:00:27:95:7F:31

# Gavėjo adresas: 08:00:27:F0:A0:56

# IP adresai:

# Siuntėjo adresas: 192.168.56.101

# Gavėjo adresas: 192.168.56.102

# Nuotraukoje taip pat galime pamatyti skambučio konfigūracijos prievadus: siuntėjo prievadas 3000 ir gavėjo prievadas 1720. Galima pamatyti taip pat ir daug kitos informacijos susijusios su skambučio konfigūracija

# Garso domenų paketo analizė matosi kitoje nuotraukoje Table Description automatically generated with low confidence

# Išanalizavus nuotrauką galima matyti naudojama „payload“ bei naudojamus garso paketas persiųsti duomenis. Iš „payload“ galima nustatyti, kad yra naudojamas G.711 protokolas, kurio pagalba galima atkoduoti ir pasiklausyti apie ką žmonės kalbėjo. Išanalizavus taip pat matome kad yra naudojamas 5062 prievadas. Antras skambutis vyko iš antros virtualios mašinos į pirmąją virtualią mašiną. Šio skambučio metu buvo naudojamas SIP protokolas. Gauti skambučio rezultatai: Table Description automatically generated

# Diagramoje iš karto matosi, kad skambučio ilgas buvo 55 sekundės. Komunikavimo protokolui yra naudojamas G.771. Matosi, kad skambinimas asmeniui buvo labai trumpas, tai reiškia, kad primos virtualios mašinos naudotojas atsiliepė labai greitai.

# Graphical user interface, text, application, email Description automatically generated

# Patikrinus pirmąjį paketą, kuris skirtas skambučio konfigūracijai, jis patvirtina, kad buvo naudotas G.771 formatas.

# Graphical user interface, text, application, email Description automatically generated

# Išanalizavus giliau šitą paketą atrandame komunikacijos MAC ir IP adresus.

# MAC adresai:

# Siuntėjo adresas: 08:00:27:F0:A0:56

# Gavėjo adresas: 08:00:27:95:7F:31

# IP adresai:

# Siuntėjo adresas: 192.168.56.102

# Gavėjo adresas: 192.168.56.101

# Table Description automatically generated

# Tiriant garso siunčiamą paketą suradau prievadus, kuriais komunikuoja kompiuteriai tarpusavyje.

# Siuntėjo prievadas: 5066

# Gavėjo prievadas: 5062 Trečias Skambutis vyko iš antros virtualios mašinos į trečią. Buvo naudojamos trys virtualios mašinos, dvi „Ubuntu“ ir viena „Windows“, kadangi „OmniPeek“ programinė įranga palaiko tik „Windows“ operacinę sistemą, dėl to buvo naudojama dar viena papildoma virtuali mašina.

# Graphical user interface, text, application, email Description automatically generated

# „OmniPeek“ programinė įranga suteikia daugiau duomenų, negi „Wireshark“ programinė įranga. Matoma, kad „flow“ diagramoje pokalbis įvyko.

# Graphical user interface Description automatically generated with low confidence

# Pirmasis paketas yra skirtas skambučio konfigūracijai, kaip ir kituose skambučiuose. Iš karto galima pastebti Naudojamus IP adresus:

# Gavėjo adresas: 192.168.56.103

# Siuntėjo adresas: 192.168.56.102

# Pastebėjus IP adresus matome iš kurio IP adreso buvo skambinta.

# Skambinimui buvo naudoti du komunikaciniai prevadai:

# Siuntėjo prievado adresas: 3000

# Gavėjo prievado adresas: 1720

# Graphical user interface Description automatically generated

# Balso siuntimui buvo naudotas 5062 prievadas. Taip pat pakete galima pastebėti ir MAC adresus į kuriuos anksčiau neatkreipėme dėmesio. Naudoti MAC adresai:

# Siuntėjo MAC adresas: 08:00:27:F0:A0:56

# Gavėjo MAC adresas: 08:00:27:B5:B6:C9

# Paketas buvo siunčiamas iš atsilieptojo naudotojo todėl MAC ir IP adresai yra sukeisti vietomis.

# Graphical user interface Description automatically generated

# Analizavimo dalis, kur yra parodyta pokalbio statistika. Įrankiui išanalizavus pokalbį buvo pamatyta, kad pokalbio kokybė buvo labai prasta.

# Paskutinio pokalbio analizė, pokalbio protokolas yra „SIP“. Skambutis buvo analizuotas „OmniPeek“ įrankio pagalba.

# Graphical user interface, text, application, email Description automatically generated

# Paskutinio pokalbio „flow“ diagramoje matome protokolus kurie buvo naudojami, skambinimui, bei pokalbio metu. Pokalbis vyko 22 sekundes. Pokalbio metu buvo naudojami du protokolai „Speedx“ ir „Theora“.

# Graphical user interface, text, application Description automatically generated

# Paketas yra skitas, skambinimui ir skambučio konfigūracijai. Pakete matome skambinimui naudojamus prievadus, IP ir MAC adresus. Naudojami prievadai:

# Siuntimo prievadas: 5060

# Gavimo prievadas: 5060

# Tada buvo surasti IP adresai:

# Siuntėjo IP adresas: 192.168.56.103

# Gavėjo IP adresas: 192.168.56.102

# Galų gale buvo surasti ir MAC adresai:

# Siuntėjo MAC adresas: 08:00:27:F0:A0:56

# Gavėjo MAC adresas: 08:00:27:B5:B6:C9

# Graphical user interface, table Description automatically generated

# Garso siuntimui iš kompiuterio į kitą kompiuterį buvo naudojami du protokolai:

# Siuntėjo protokolas: 5070

# Gavėjo protokolas: 5062

# Graphical user interface, text, application, email Description automatically generated

# Paanalizavus skambinimo paktą galima surasti, kokiu formatu buvo siunčiami garso duomenys. Šiuo atveju buvo surasta, kad naudojamas 5070 protokolas ir G.711 formatas.

# Graphical user interface Description automatically generated

# Pasirinkus pokalbio analizę, jokios informacijos apart pokalbio laiko nerodo.

# Visų rezultatų neišėjo surasti, kadangi įranga nesuteikia pilnos informacijos: Tolimesnių laukų rasti nepavyksta. Žinoma, jog jie turėtų matytis „Media“ skiltyje „OmniPeak“ programoje, tačiau skambučio metu tokia informacija nebuvo įrašyta. Priežastis nežinoma, galbūt per trumpas pokalbis ar netinkamai sukonfigūruota aparatinė įranga.