

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.


1.1 Paleisti programą „Wireshark“.

1.2 Aktyvuoti paketų „gaudymą“: Capture -> Interfaces -> Parinkti tinklo plokštę, turinčią jūsų kompiuterio IP adresą -> Start.

1.3 Paleisti „Ekiga“ programinį telefoną ir užmegzti balso ryšį **su kaimyniniu kompiuteriu**: Paleisti programą „Ekiga“ -> Adresų lauke įvesti signalizacijos protokolą ir kaimyninio kompiuterio IP

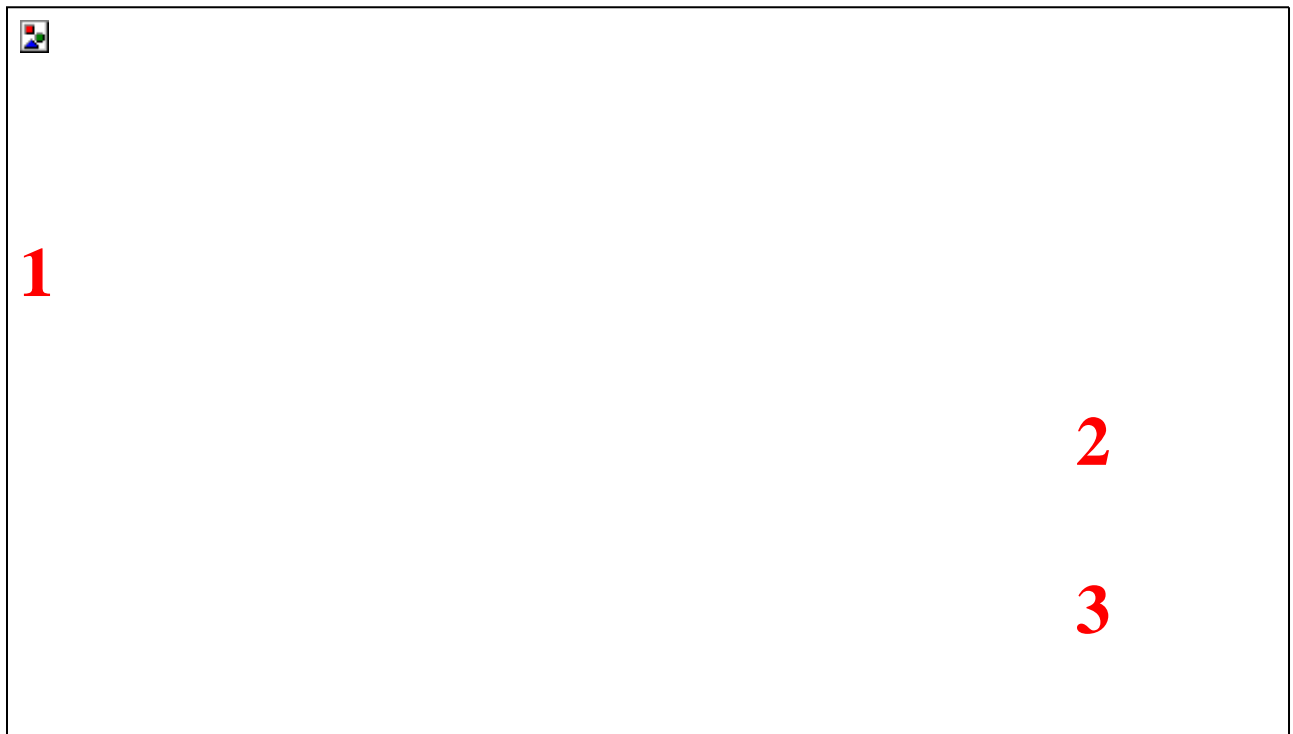
adresą (pvz.: sip:192.168.0.2 arba h323:192.168.0.2) -> paspausti  mygtuką -> Kaimyniniame

kompiuteryje pradėjus skambėti telefonui paspausti  -> Balso sesija užmegzta, trumpai VoIP

telefonu pasikalbėti su kaimynu (5 – 10 s.) -> Nutraukti balso sesiją, tam paspausti  mygtuką.

1.4 „Wireshark“ programoje sustabdyti paketų „gaudymą“: Capture -> Stop.

1.5 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 pav. Darbinis „Wireshark“ programos langas

1.6 Išnagrinėti pateiktą „pagautų“ paketų statistiką:

2 Statistics -> Paiešai 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.

3 Telephony -> RTP -> Show All Streams -> 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.

4 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.

1.7 Uždaryti „Wireshark“ programą.

2. Atlikti paketų analizę naudojant „Omnipeek“ paketų analizatorių, gautus rezultatus pateikti 1 lentelėje.

2.1 Paleisti programą „Omnipeek“.

2.2 Aktyvuoti paketų „gaudymą“: New Capture -> „Local Area Connection x“ tinklo plokštę -> OK -> Start Capture.

2.3 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



tam paspausti

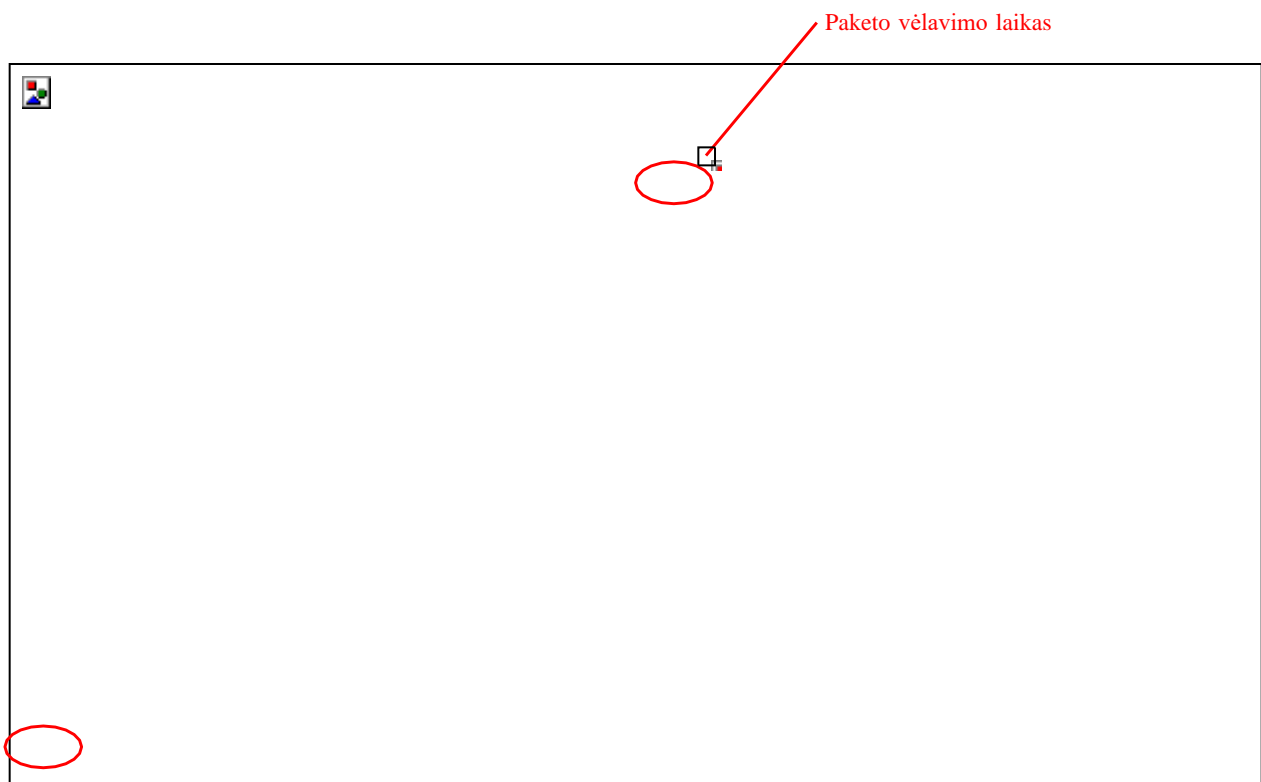


mygtuką.

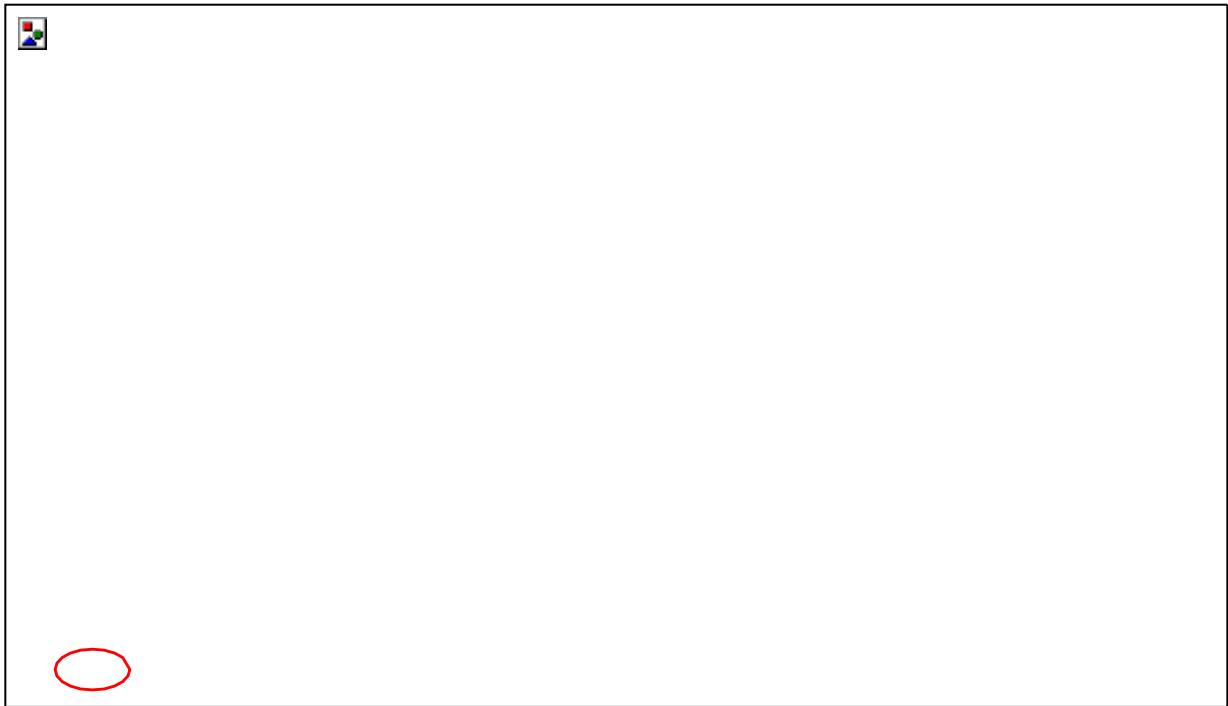
2.4 „Omnipeek“ programoje sustabdyti paketų „gaudymą“, tam paspausti „Stop Capture“.

2.5 Patyrinėti balso paketų struktūrą ir dydžius, tam ant pasirinkto paketo du kartus spragtelti kairiu pelės klavišu. Kokie pagrindiniai skirtumai tarp įeinančių ir išėinančių balso paketų?

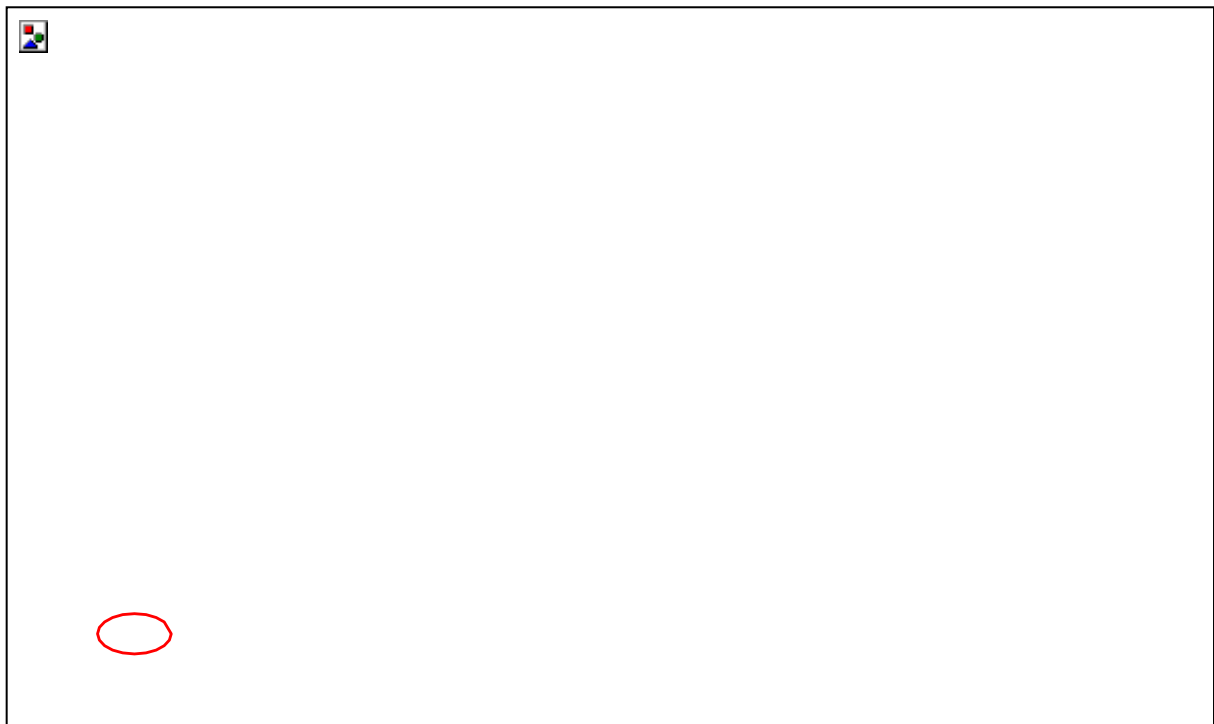
2.6 Išnagrinėti pateiktą „pagautų“ paketų statistiką. Paketų analizės pavyzdžiai pateikti 2 – 11 pav. **Ypatingą dėmesį atkreipkite į 9 – 11 pav., čia pateikta detali balso sesijos analizė.**



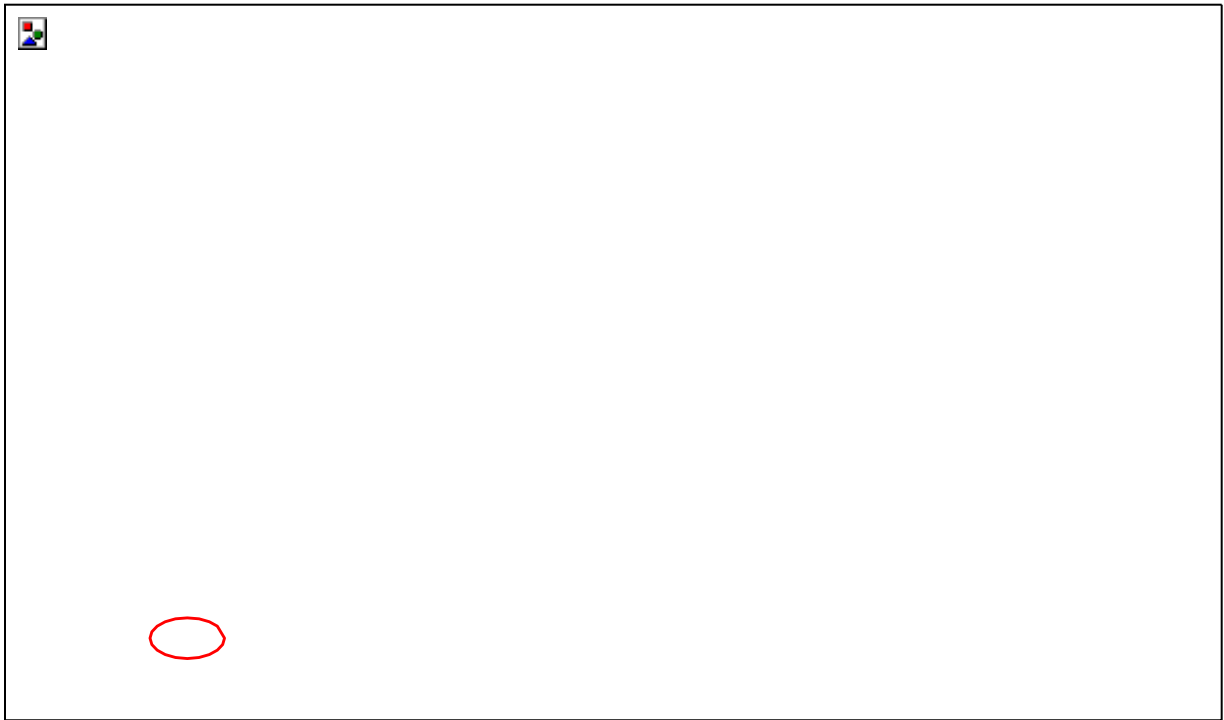
2 pav. Grafoje „Packets“ matyti „pagautų“ paketų sąrašas, kuriame matosi siuntėjo, bei gavėjo IP adresai, paketų dydžiai baitais, paketo vėlavimo laikas, paketo „pagavimo“ laikas, balso kodavimo ir suspaudimo algoritmas.



3 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.

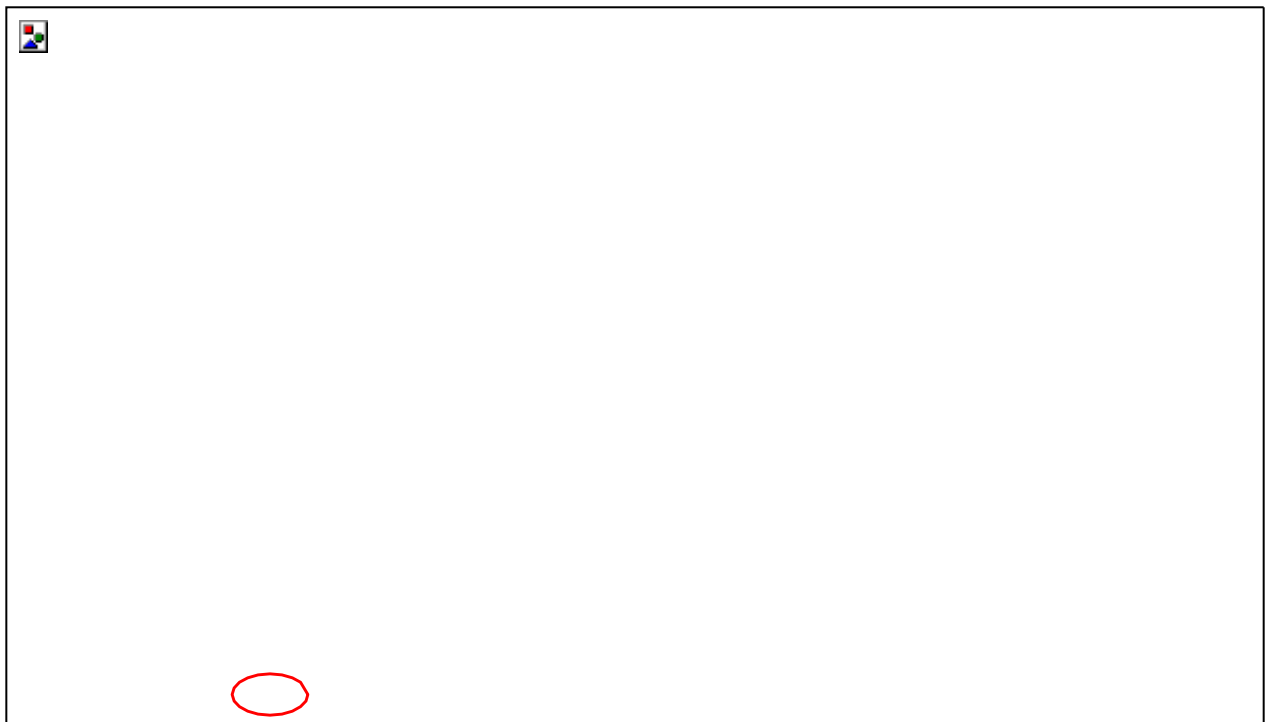


4 pav. Grafoje „Nodes“ matyti tarp kokių tinklo mazgų, kiek paketų buvo perduota. Išskleidus tinklo mazgą, kuris dalyvavo balso paketų perdavimo sesijoje galima detaliau matyti išsiųstų ir priimtų paketų grafines priklausomybes, bei perduotų balso (RTP) ir signalizacijos (SIP) paketų procentinį pasiskirstymą.

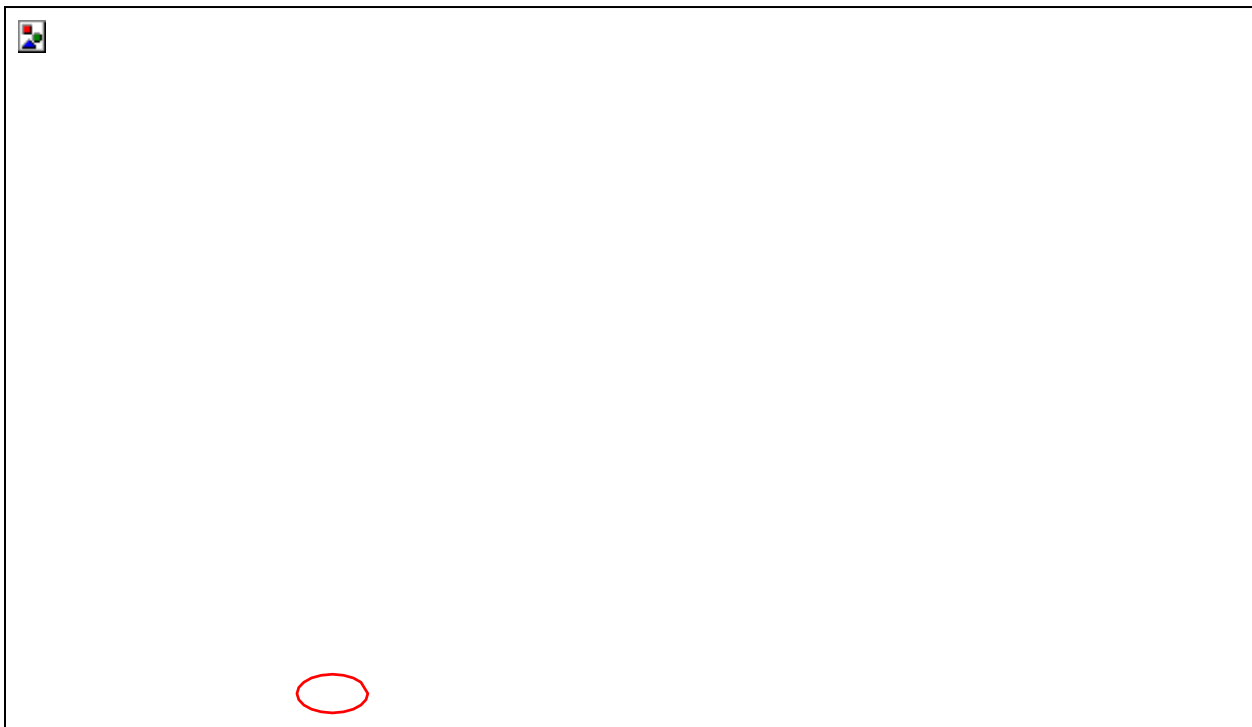


5

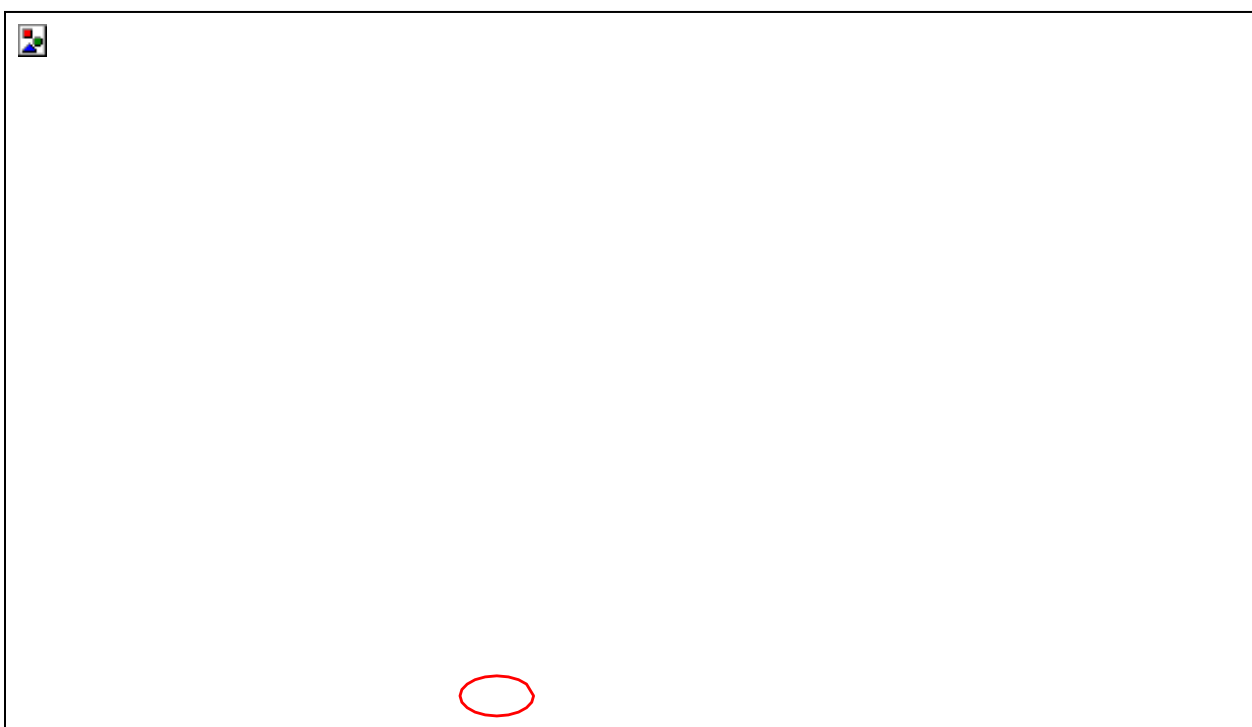
pav. Grafoje „Protocols“ matyti procentinis naudojamų paketams perduoti protokolų pasiskirstymas. Išskleidus pasirinktą protokolą (pvz., SIP) galima pamatyti bendraujančių tinklo mazgų IP, bei MAC adresus, kiek paketų iš pastarųjų mazgų buvo išsiųsta ir priimta. Žemiau matyti, kad SIP paketai buvo perduodami tinklu naudojant UDP protokolą, o UDP datagrama buvo perduodama naudojant IP protokolą.



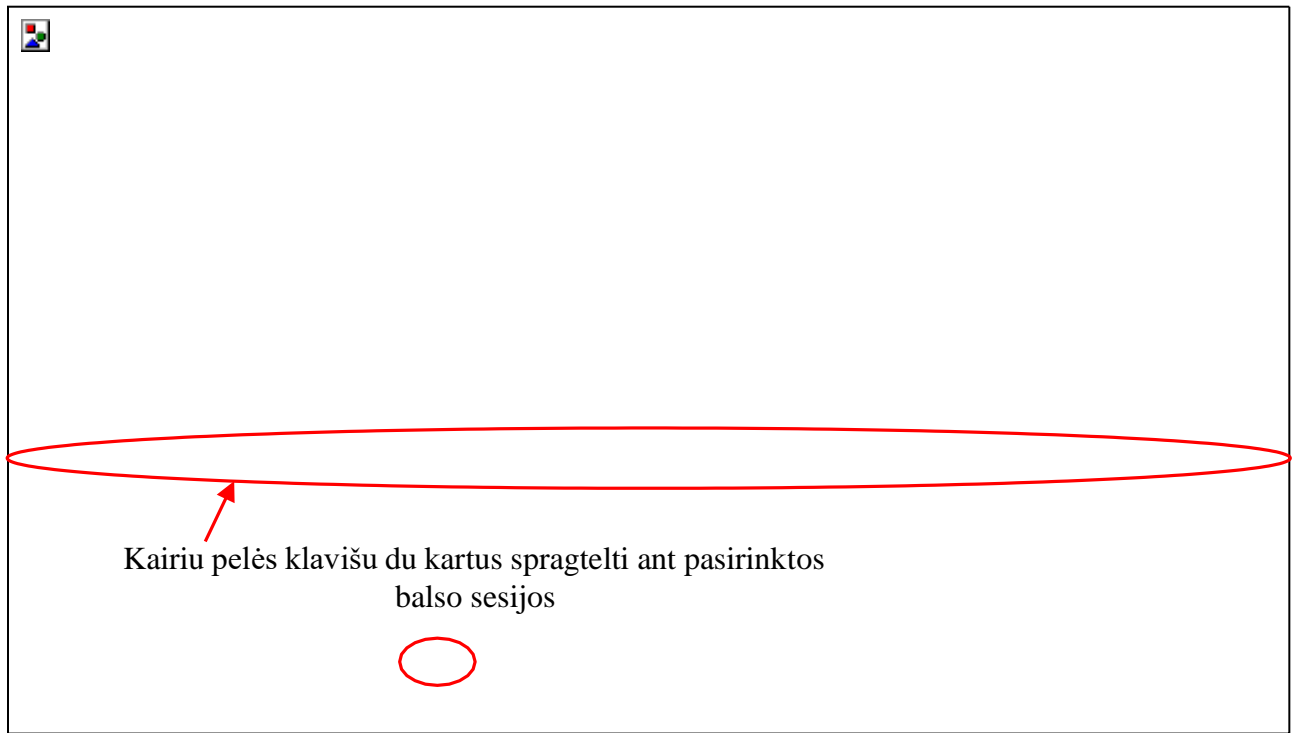
6 pav. Grafoje „Summary“ apibendrinta perduotų tinkle paketų statistika. Reikėtų atkreipti dėmesį į tinklo išnaudojimo (Utilization) statistiką.



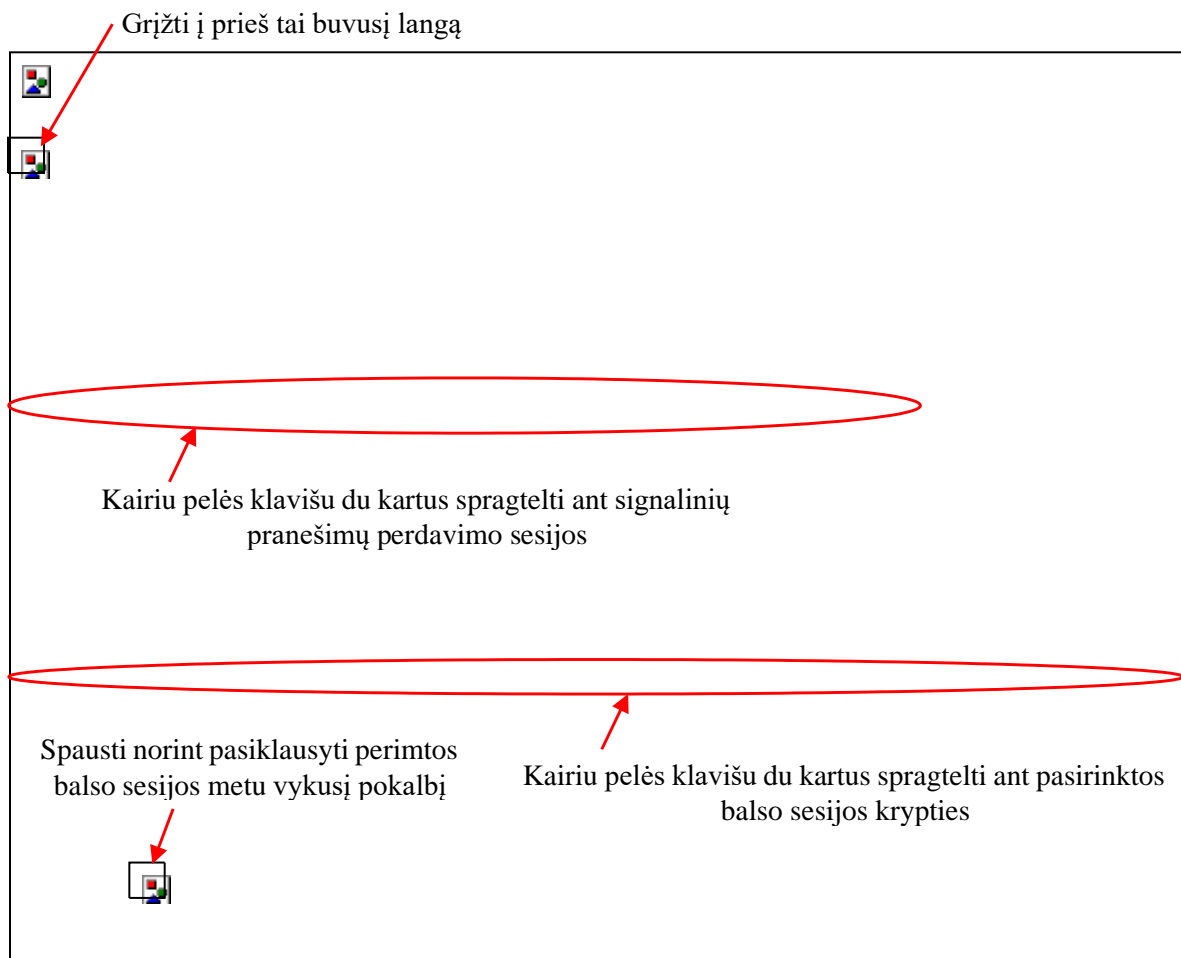
7 pav. Grafoje „Graphs“ matyti perduotų tinkle paketų statistikos grafinės priklausomybės. Reikėtų atkreipti dėmesį į perduotų paketų dydžių (Packet Sizes), bei tinklo išnaudojimo (Utilization) statistiką.



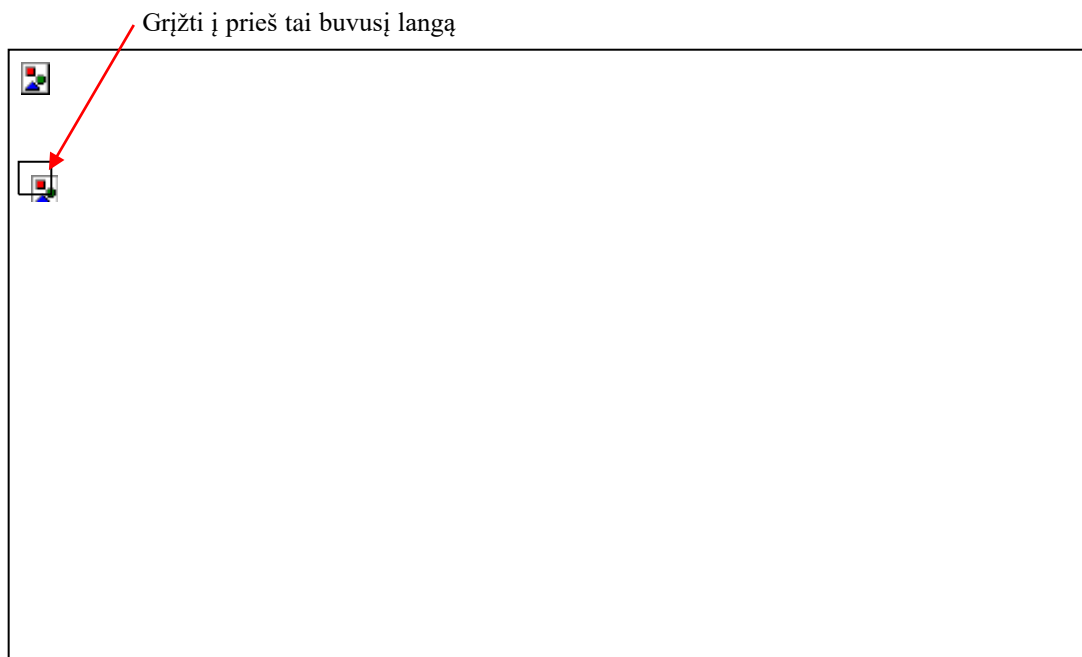
8 pav. Grafoje „Peer Map“ matyti perduodamų tarp tinklo mazgų duomenų srautų pasiskirstymo grafinis „žemėlapis“.



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



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



11 pav. Signalinių pranešimų, kurie buvo panaudoti sudarant perimtą balso sesiją, grafas.

2.7 Uždaryti „Omnipeek“ programą.

3. VoIP sesijos analizę reikia atlikti keturiais skirtingais scenarijais ir gautus rezultatus pateikti 1-oje lentelėje:

1. Pasirinkti H.323 signalizacijos protokolą ir skambinti iš PC1 į PC2, perduodamų paketų analizę atlikti „Wireshark“ paketų analizatoriumi;
2. Pasirinkti SIP signalizacijos protokolą ir skambinti iš PC1 į PC2, perduodamų paketų analizę atlikti „Wireshark“ paketų analizatoriumi;
3. Pasirinkti H.323 signalizacijos protokolą ir skambinti iš PC2 į PC1, perduodamų paketų analizę atlikti „Omnipeek“ paketų analizatoriumi;
4. 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. fliktuacijos, 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 pasiklausymo 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 pirmąjį Ubuntu kompiuterį naudojant SIP protokolą. Pirmųjų dviejų skambučių analizei buvo naudota „Wireshark“ programinė įranga. Skambinant iš antro kompiuterio į trečią buvo naudojamas H.323 protokolą. O skambinant iš trečio kompiuterio į antrą buvo naudojamas SIP protokolą. 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 :

Time	192.168.56.101	192.168.56.102	Comment
0.051435711	30000	1720	H225 From: To: TunnH245:on FS:on
0.058086747	30000	1720	H225 TunnH245:on FS:off
0.105039963	30000	1720	H245 terminalCapabilitySet H245 terminalCapa...
0.105284716	30000	1720	H225 TunnH245:on FS:off
0.116512005	30000	1720	H245 terminalCapabilitySetAck H245 masterSI...
0.117067711	30000	1720	H245 roundTripDelayRequest
0.117819089	30000	1720	H245 roundTripDelayResponse
2.391045064	5062	5062	RTP, 808 packets. Duration: 16.14s SSRC: 0xA3...
2.478179429	5064	5064	RTP, 477 packets. Duration: 16.08s SSRC: 0x54...
2.488703415	30000	1720	H225 TunnH245:on FS:on
2.728150938	5062	5062	RTP, 794 packets. Duration: 15.84s SSRC: 0x5D...
18.566971664	30000	1720	H225 Q931 Rel Cause (16):Normal call clearing
18.570911389	30000	1720	H225 Q931 Rel Cause (16):Normal call clearing

Nors pokalbio metu garso girdėti nėjo, bet matome, kad pokalbis įvyko.

h323.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
8	0.051435711	192.168.56.101	192.168.56.102	H.225...	1449	CS: setup OpenLogicalChannel terminalCapabilitySet mas
9	0.051461033	192.168.56.102	192.168.56.101	TCP	66	1720 → 30000 [ACK] Seq=1 Ack=1384 Win=64128 Len=0 TSva
10	0.058086747	192.168.56.102	192.168.56.101	H.225.0	174	CS: callProceeding
11	0.058698753	192.168.56.101	192.168.56.102	TCP	66	30000 → 1720 [ACK] Seq=1384 Ack=109 Win=64256 Len=0 TS
12	0.105039963	192.168.56.102	192.168.56.101	H.225...	460	CS: empty terminalCapabilitySet terminalCapabilitySetA
13	0.105284716	192.168.56.102	192.168.56.101	H.225.0	174	CS: alerting
14	0.105341393	192.168.56.101	192.168.56.102	TCP	66	30000 → 1720 [ACK] Seq=1384 Ack=503 Win=64128 Len=0 TS
15	0.105501104	192.168.56.101	192.168.56.102	TCP	66	30000 → 1720 [ACK] Seq=1384 Ack=611 Win=64128 Len=0 TS
16	0.116512005	192.168.56.101	192.168.56.102	H.225...	112	CS: empty terminalCapabilitySetAck masterSlaveDetermin
17	0.116529624	192.168.56.102	192.168.56.101	TCP	66	1720 → 30000 [ACK] Seq=611 Ack=1430 Win=64128 Len=0 TS
18	0.117067711	192.168.56.102	192.168.56.101	H.225...	106	CS: empty roundTripDelayRequest
19	0.117437498	192.168.56.101	192.168.56.102	TCP	66	30000 → 1720 [ACK] Seq=1430 Ack=651 Win=64128 Len=0 TS
20	0.117819089	192.168.56.101	192.168.56.102	H.225...	109	CS: empty roundTripDelayResponse
21	0.117828310	192.168.56.102	192.168.56.101	TCP	66	1720 → 30000 [ACK] Seq=651 Ack=1473 Win=64128 Len=0 TS

Frame 8: 1449 bytes on wire (11592 bits), 1449 bytes captured (11592 bits) on interface 0

Ethernet II, Src: PcsCompu_95:7f:31 (08:00:27:95:7f:31), Dst: PcsCompu_f0:a0:56 (08:00:27:f0:a0:56)

- Destination: PcsCompu_f0:a0:56 (08:00:27:f0:a0:56)
- Source: PcsCompu_95:7f:31 (08:00:27:95:7f:31)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 1435
- Identification: 0xa181 (41345)
- Flags: 0x4000, Don't fragment
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0xa1bf [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.56.101
- Destination: 192.168.56.102

Transmission Control Protocol, Src Port: 30000, Dst Port: 1720, Seq: 1, Ack: 1, Len: 1383

- Source Port: 30000
- Destination Port: 1720
- [Stream index: 0]

0000 08 00 27 f0 a0 56 08 00 27 95 7f 31 08 00 45 00 ...V...1..E..

0010 05 9b a1 81 40 00 40 06 a1 bf c0 a8 38 65 c0 a8 ...@.@...8e...

0020 38 66 75 30 06 b8 ae 13 41 27 7a e2 de 5b 80 18 8fu0...A'z...[...

0030 01 f6 ac 7d 00 00 01 01 08 0a f6 ab d8 69 f8 64 ...}...i..d

0040 4d 17 03 00 05 67 08 02 68 72 05 04 04 88 18 ff M...g...hr.....

0050 a5 28 0c 6f 73 62 6f 78 65 73 2e 6f 72 67 00 7e ..(osbox es.org~

0060 05 47 05 20 b8 06 00 08 91 4a 00 06 01 40 06 00 ..G...J...@...

0070 6f 00 73 00 62 00 6f 00 78 00 65 00 73 22 c0 09 o-s-b-o-x-e-s"...

0080 00 00 3d 02 00 00 22 34 2e 30 2e 31 20 28 4f"4.0.1 (0

Frame (1449 bytes) booleanArray (1 byte) unsignedMin (2 bytes) unsignedMin (2 bytes) unsignedMin (2 bytes) unsignedMin (2 bytes) boole

h323.pcapng Packets: 2126 · Displayed: 2126 (100.0%) Profile: Default

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.

h323.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
20	0.117819089	192.168.56.101	192.168.56.102	H.225...	109	CS: empty roundTripDelayResponse
21	0.117828310	192.168.56.102	192.168.56.101	TCP	66	1720 → 30000 [ACK] Seq=651 Ack=1473 Win=64128 Len=0 TS
22	2.391045064	192.168.56.102	192.168.56.101	RTP	106	PT=DynamicRTP-Type-109, SSRC=0xA352435F, Seq=64885, Ti
23	2.410892536	192.168.56.102	192.168.56.101	RTP	106	PT=DynamicRTP-Type-109, SSRC=0xA352435F, Seq=64886, Ti
24	2.437818888	192.168.56.102	192.168.56.101	RTP	106	PT=DynamicRTP-Type-109, SSRC=0xA352435F, Seq=64887, Ti
25	2.460596439	192.168.56.102	192.168.56.101	RTP	106	PT=DynamicRTP-Type-109, SSRC=0xA352435F, Seq=64888, Ti
26	2.460954653	192.168.56.102	192.168.56.101	RTP	106	PT=DynamicRTP-Type-109, SSRC=0xA352435F, Seq=64889, Ti
27	2.478179429	192.168.56.102	192.168.56.101	H.261	1077	H.261 message
28	2.478319867	192.168.56.102	192.168.56.101	H.261	444	H.261 message
29	2.485872186	192.168.56.102	192.168.56.101	RTP	106	PT=DynamicRTP-Type-109, SSRC=0xA352435F, Seq=64890, Ti
30	2.488703415	192.168.56.102	192.168.56.101	H.225.0	394	CS: connect OpenLogicalChannel
31	2.488999553	192.168.56.101	192.168.56.102	TCP	66	30000 → 1720 [ACK] Seq=1473 Ack=979 Win=64128 Len=0 TS
32	2.507296630	192.168.56.102	192.168.56.101	H.261	1076	H.261 message
33	2.507328270	192.168.56.102	192.168.56.101	H.261	436	H.261 message

Frame 26: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0

Ethernet II, Src: PcsCompu_f0:a0:56 (08:00:27:f0:a0:56), Dst: PcsCompu_95:7f:31 (08:00:27:95:7f:31)

Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101

User Datagram Protocol, Src Port: 5062, Dst Port: 5062

Source Port: 5062

Destination Port: 5062

Length: 72

Checksum: 0xf275 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

Real-Time Transport Protocol

0000 08 00 27 95 7f 31 08 00 27 f0 a0 56 08 00 45 b8 ... 1 ... V ... E

0010 00 5c bf 8d 40 00 40 11 88 2f c0 a8 38 66 c0 a8 ... @ @ @ / ... 8f

0020 38 65 13 c6 13 c6 00 48 f2 75 80 6d fd 79 00 00 ... 8e ... H ... u ... m ... y

0030 05 00 a3 52 43 5f 2e 9d 1b 9a 20 02 01 7f ff ff ... RC ...

0040 ff ff ff 81 00 bf ff ff ff ff ff c0 80 5f ff ff ...

0050 ff ff ff e0 40 2f ff ff ff ff ff fa 3b 60 b5 ad ... @ / ... , ...

0060 60 b5 ad 60 b5 ad 60 b5 ad 67 ... g

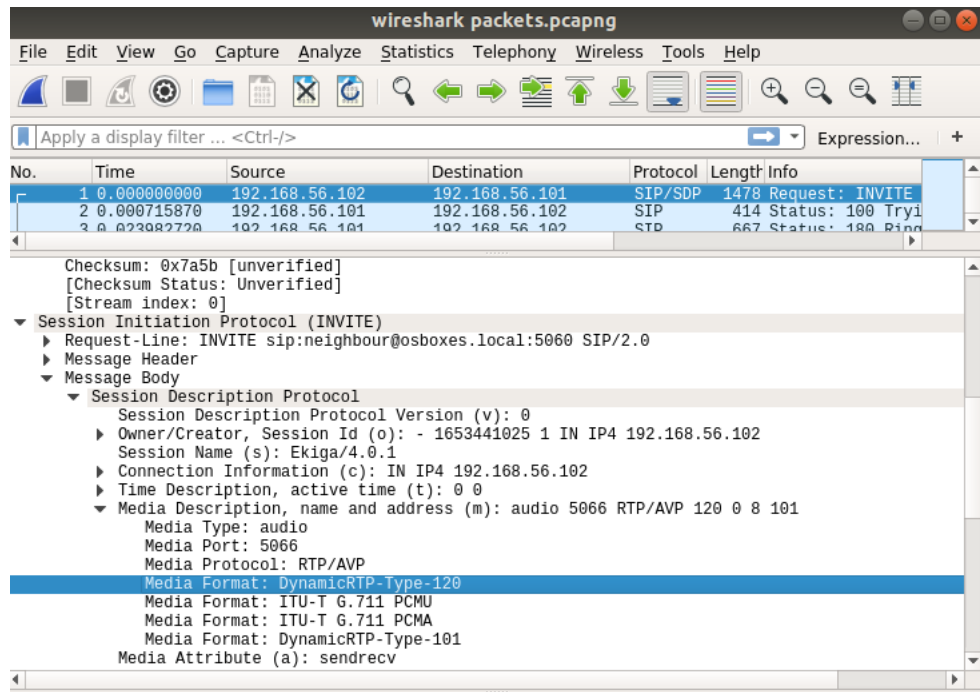
h323.pcapng Packets: 2126 · Displayed: 2126 (100.0%) Profile: Default

Išanalizavus nuotrauką galima matyti naudojama „payload“ bei naudojamus garso paketas persiūsti duomenis. Iš „payload“ galima nustatyti, kad yra naudojamas G.711 protokolai, kurio pagalba galima atkoduoti ir pasiklausyti apie ką žmonės kalbėjo. Išanalizavus taip pat matome kad yra naudojamas 5062 prievadas.

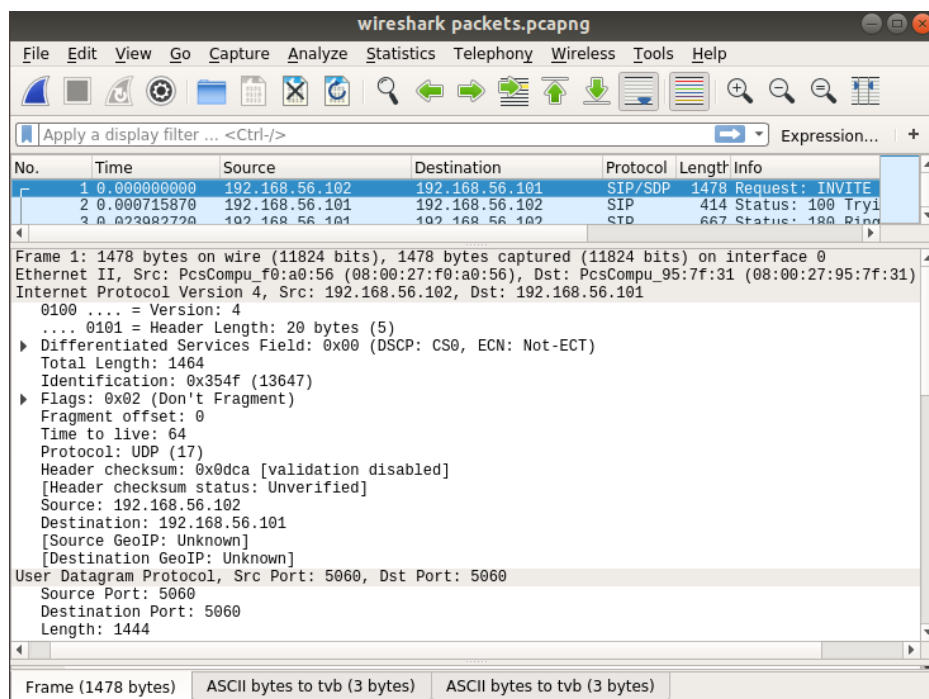
Antras skambutis vyko iš antros virtualios mašinos į pirmąją virtualią mašiną. Šio skambučio metu buvo naudojamas SIP protokolai. Gauti skambučio rezultatai:

Time	192.168.56.102	192.168.56.101	Comment
0.000000000	5060	5060	SIP INVITE From: "Eligijus" <sip:eligijus@192.168.5...
0.000715870	5060	5060	SIP Status 100 Trying
0.023982720	5060	5060	SIP Status 180 Ringing
0.025130136	5060	5060	SIP PRACK From: "Eligijus" <sip:eligijus@192.168....
0.025510530	5060	5060	SIP Status 200 OK
1.385094809	5066	5062	RTP (Speex)
1.403742265	5060	5060	SIP Status 200 OK
1.406514558	5060	5060	SIP Request INVITE ACK 200 CSeq:1
1.452000183	5068	5064	RTP (theora)
1.538678754	5066	5062	RTP (Speex)
1.576236302	5068	5064	RTP (theora)
55.243814325	5060	5060	SIP Request BYE CSeq:3
55.244606328	5060	5060	SIP Status 200 OK

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 pirmos virtualios mašinos naudotojas atsiliepė labai greitai.



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



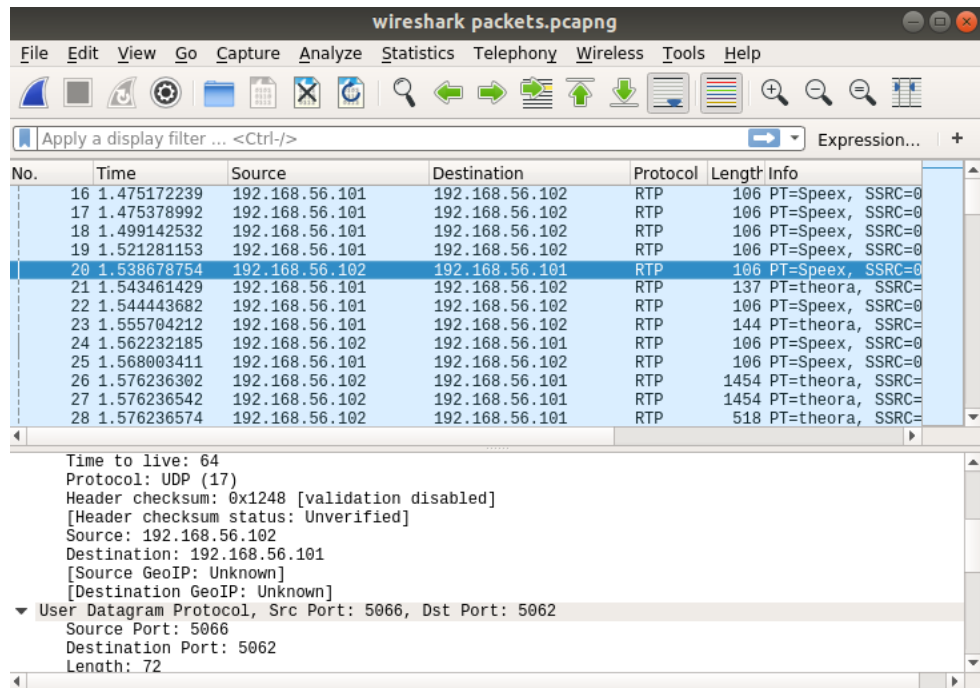
Išanalizavus giliau šitą paketą atrandame komunikacijos MAC ir IP adresus.

MAC adresai:

- Siuntėjo adresas: 08:00:27:F0:A0:56
- Gavėjo adresas: 08:00:27:95:7F:31

IP adresai:

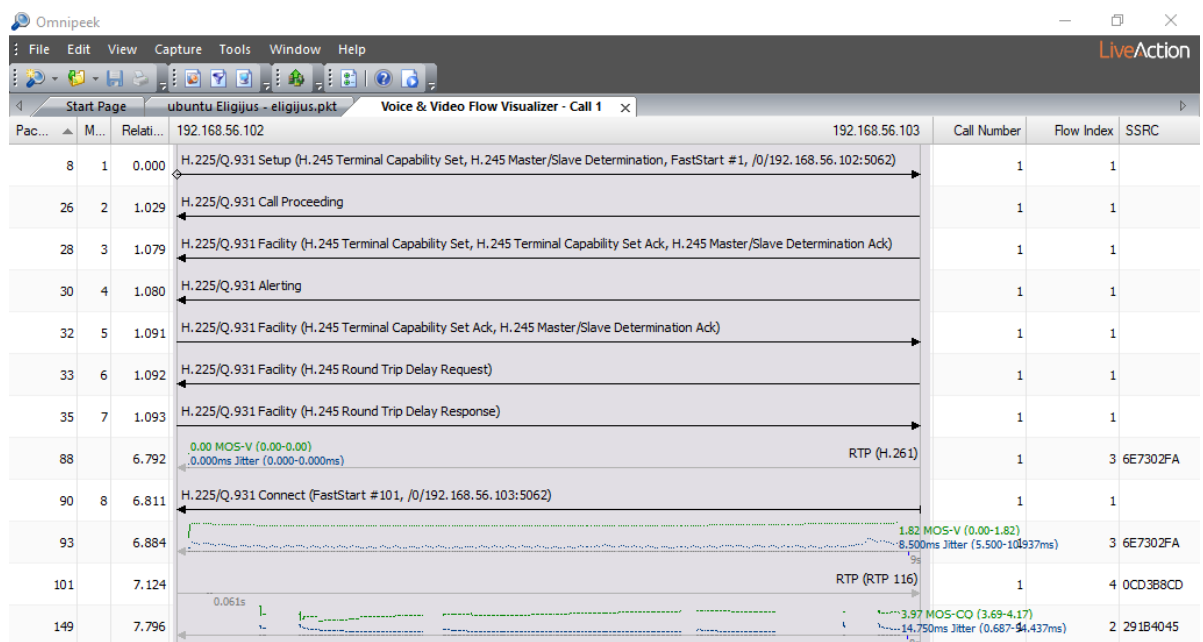
- Siuntėjo adresas: 192.168.56.102
- Gavėjo adresas: 192.168.56.101



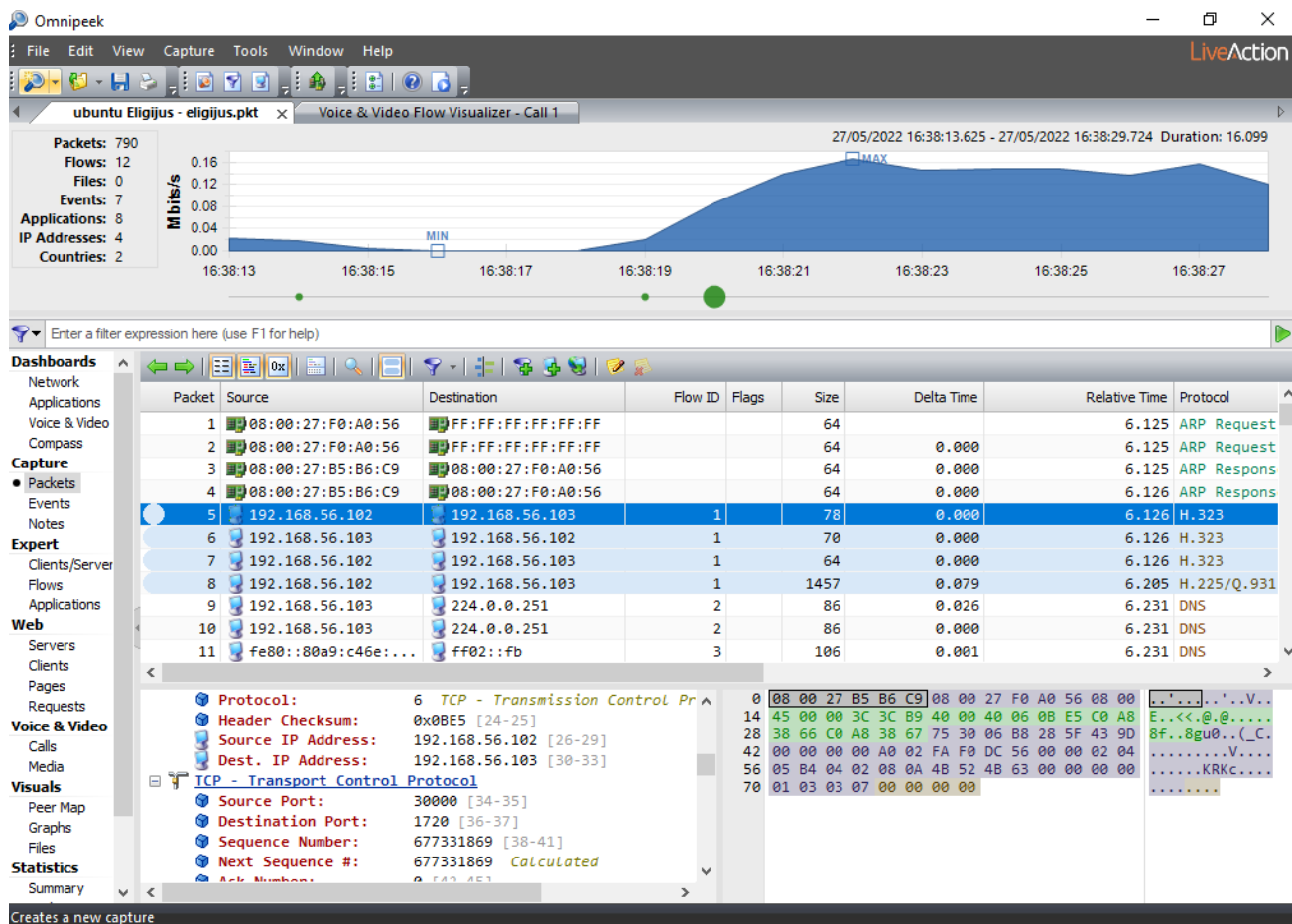
Tiriant garso siunčiamą paketą suradau prievadus, kuriais komunikuoja kompiuteriai tarpusavyje.

- 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.



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



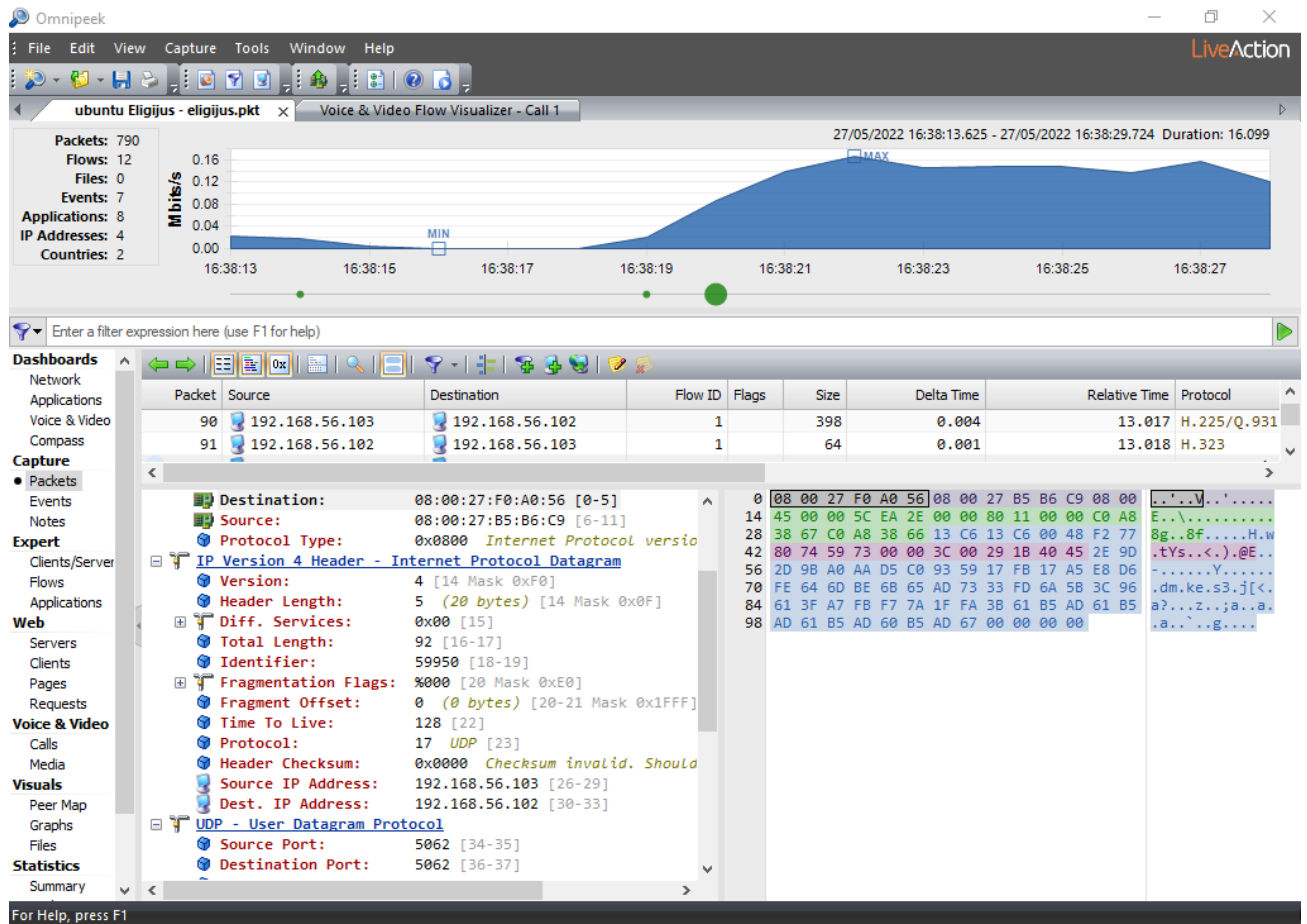
Pirmasis paketas yra skirtas skambučio konfigūracijai, kaip ir kituose skambučiuose. Iš karto galima pastebėti Naudojamus IP adresus:

- 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:

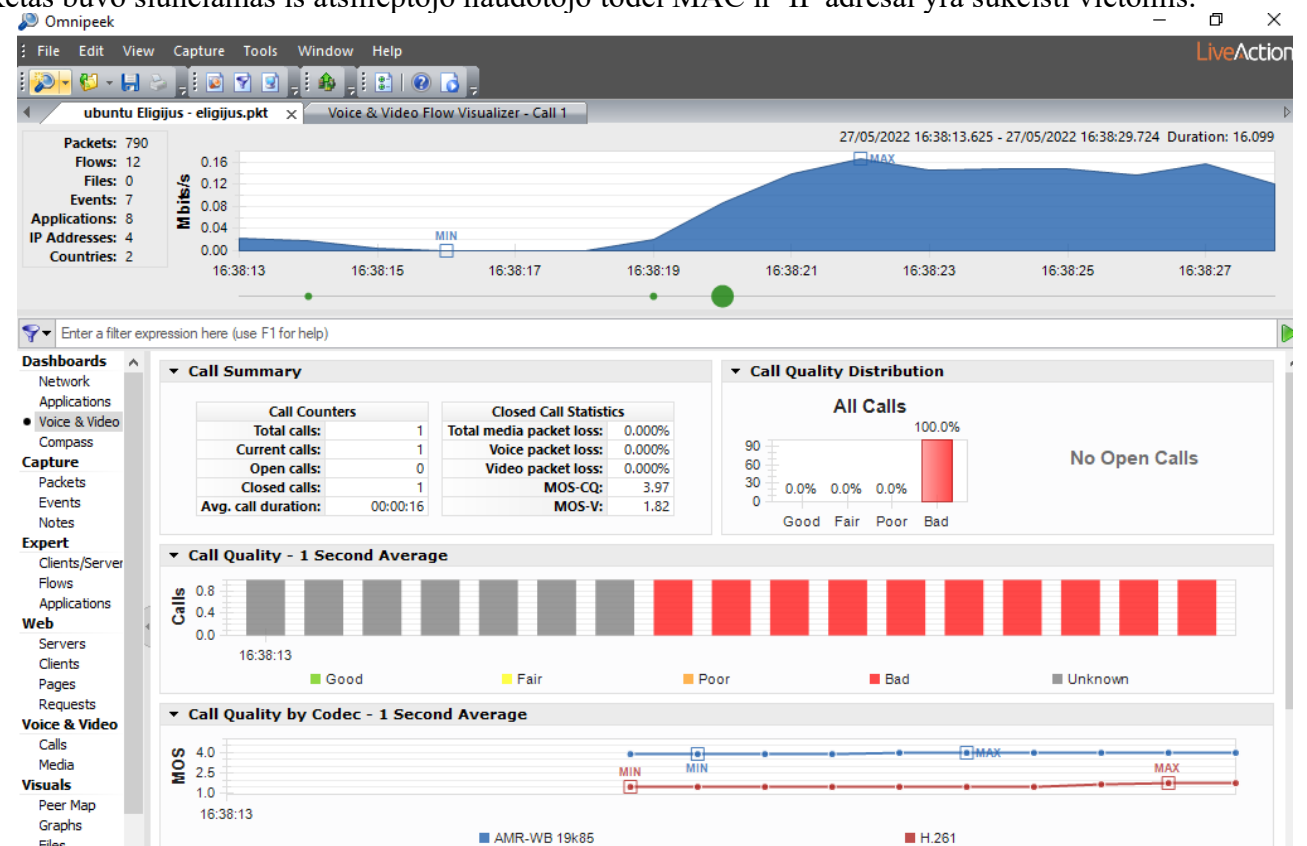
- Siuntėjo prievado adresas: 3000
- Gavėjo prievado adresas: 1720



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

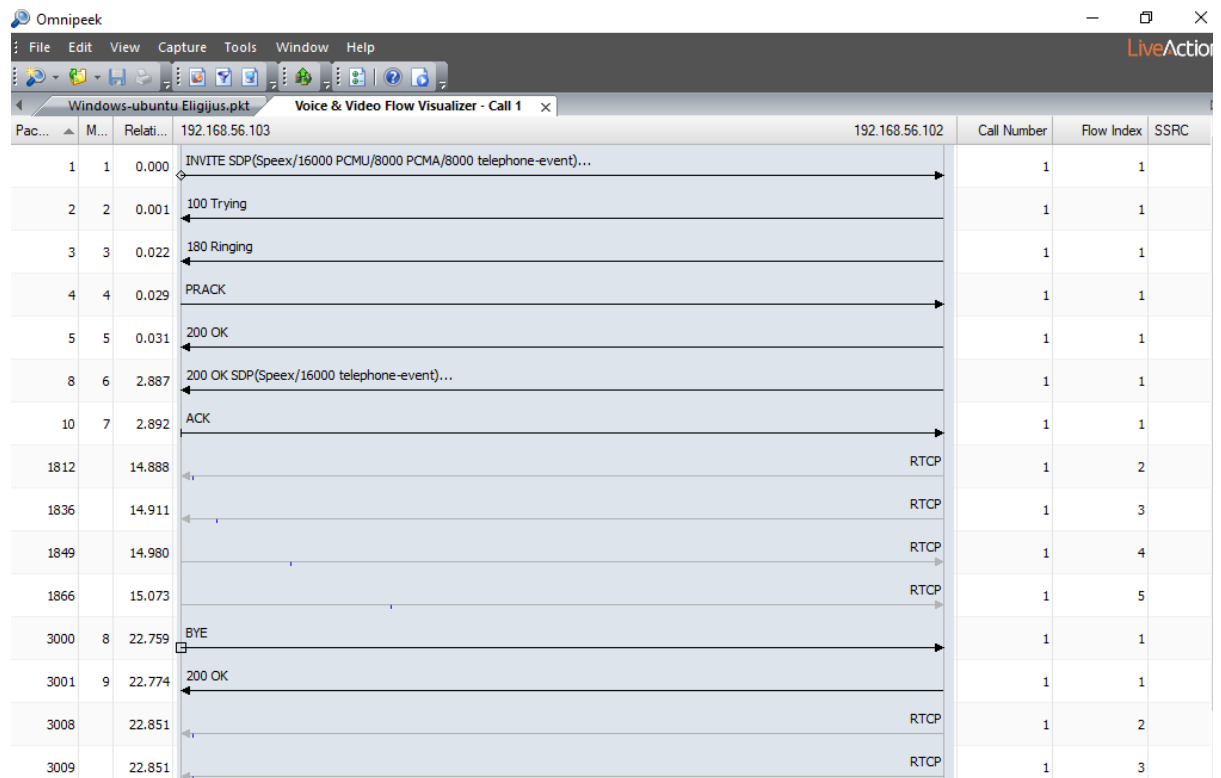
- Siuntėjo MAC adresas: 08:00:27:F0:A0:56
- Gavėjo MAC adresas: 08:00:27:B5:B6:C9

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

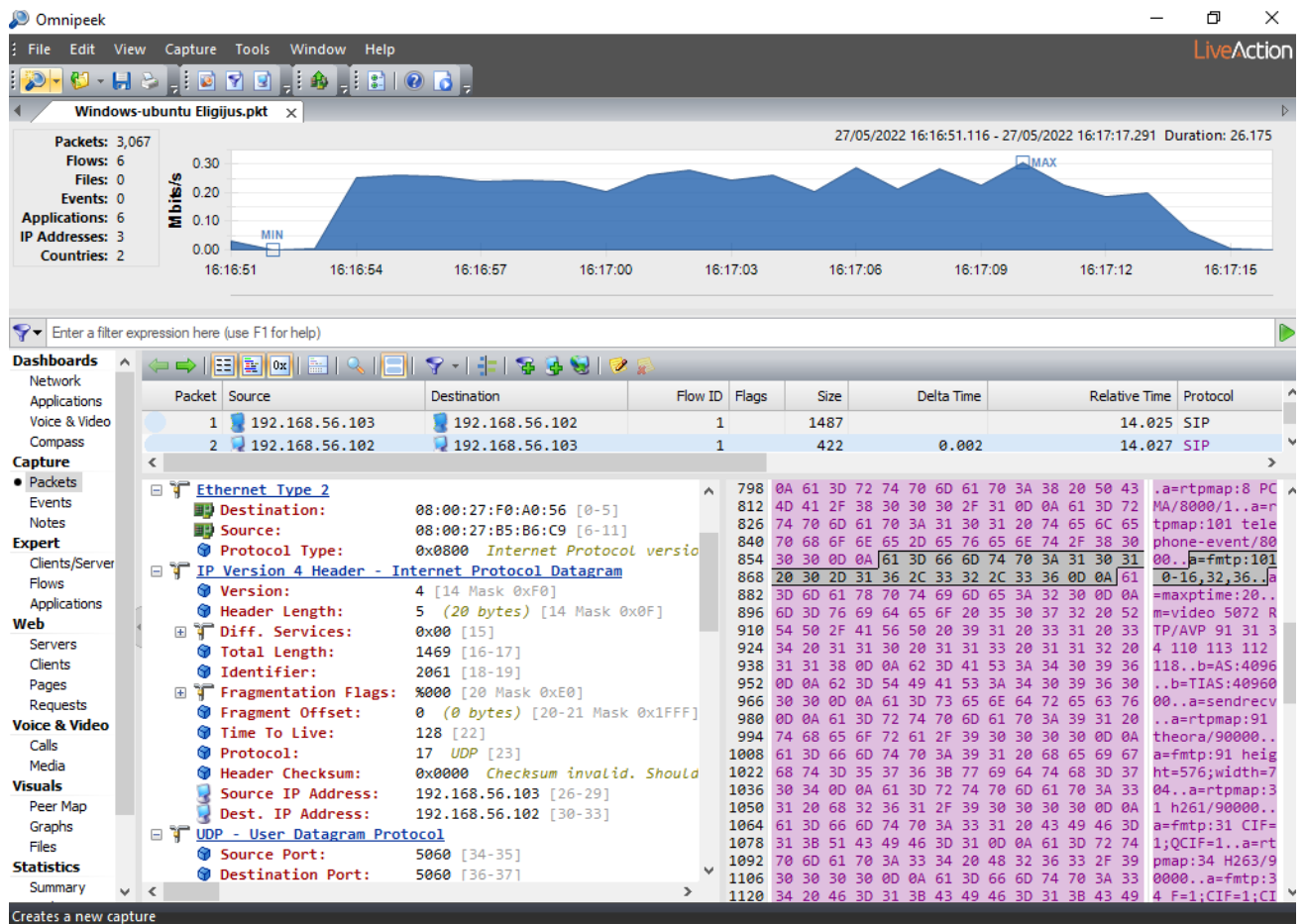


Analizavimo dalis, kur yra parodyta pokalbio statistika. Įrankiui išanalizavus pokalbį buvo pamatyta, kad pokalbio kokybė buvo labai prasta.

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



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“.



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

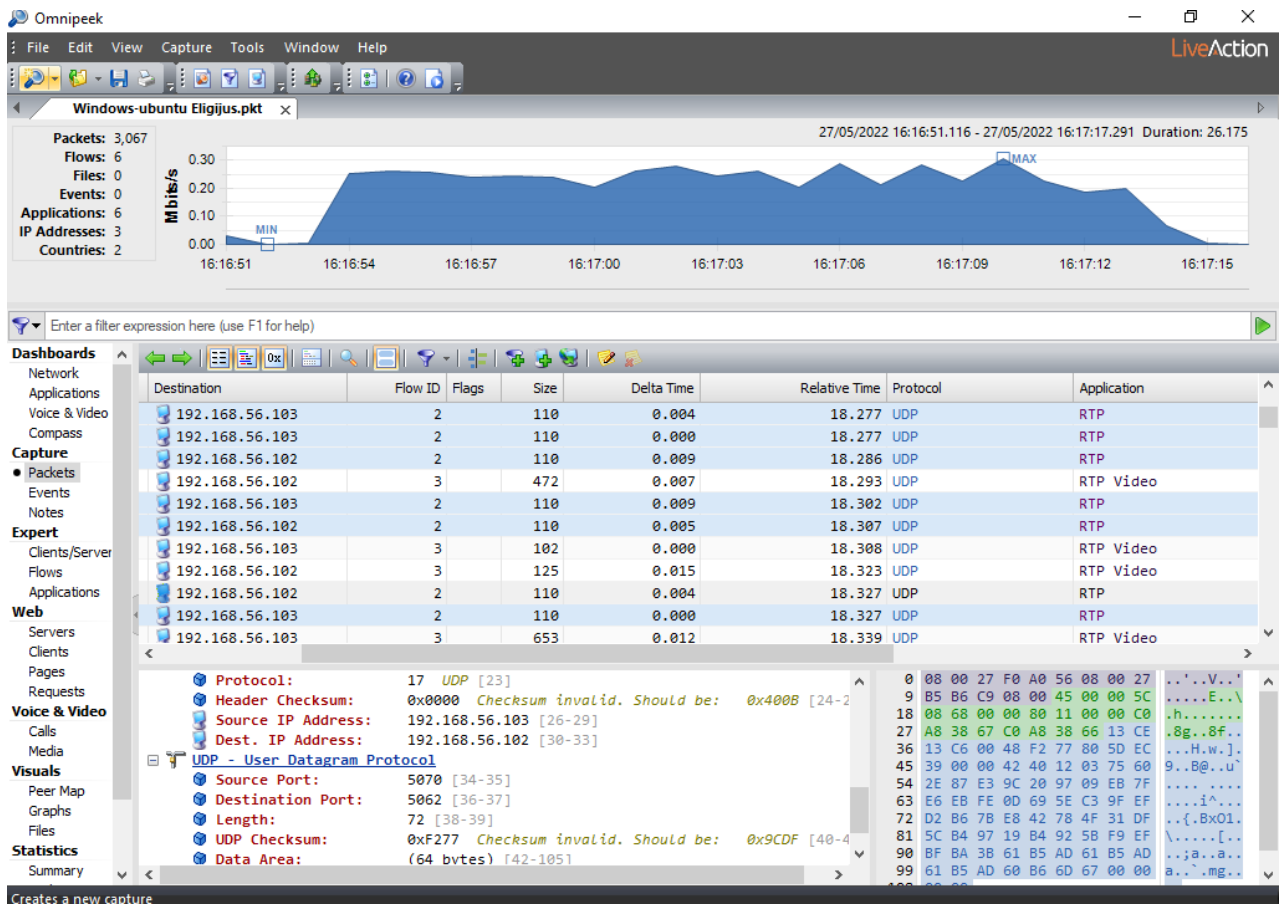
- Siuntimo prievadas: 5060
- Gavimo prievadas: 5060

Tada buvo surasti IP adresai:

- Siuntėjo IP adresai: 192.168.56.103
- Gavėjo IP adresai: 192.168.56.102

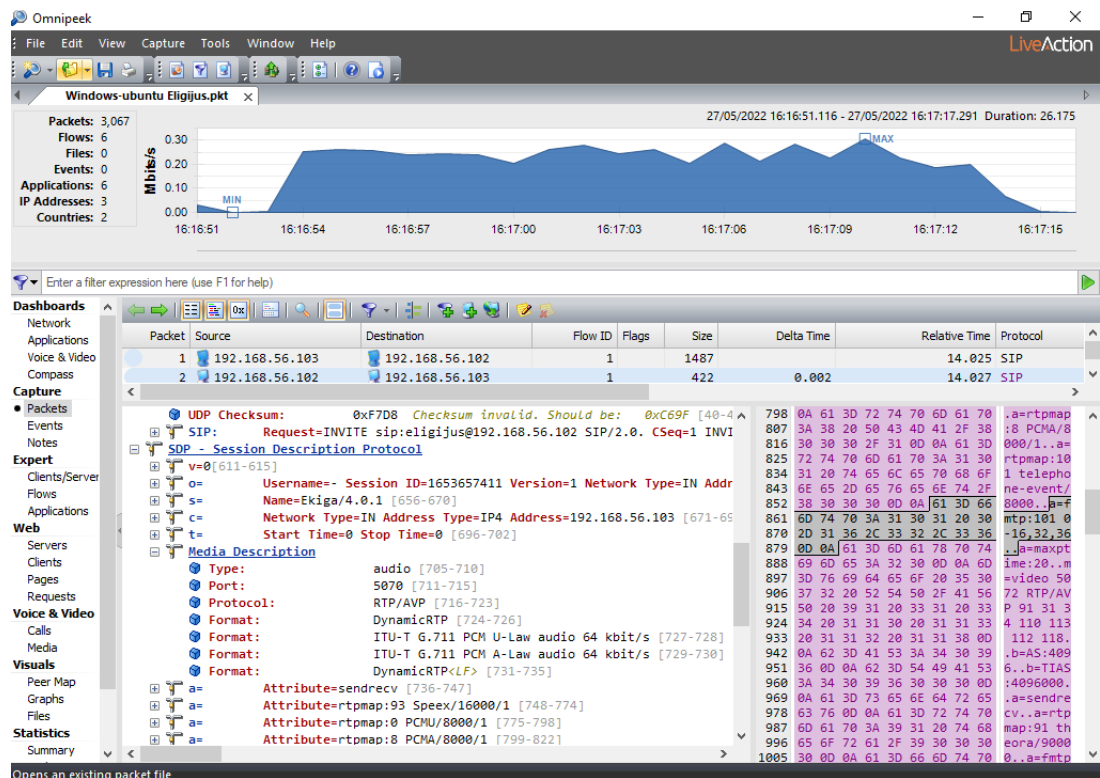
Galų gale buvo surasti ir MAC adresai:

- Siuntėjo MAC adresai: 08:00:27:F0:A0:56
- Gavėjo MAC adresai: 08:00:27:B5:B6:C9

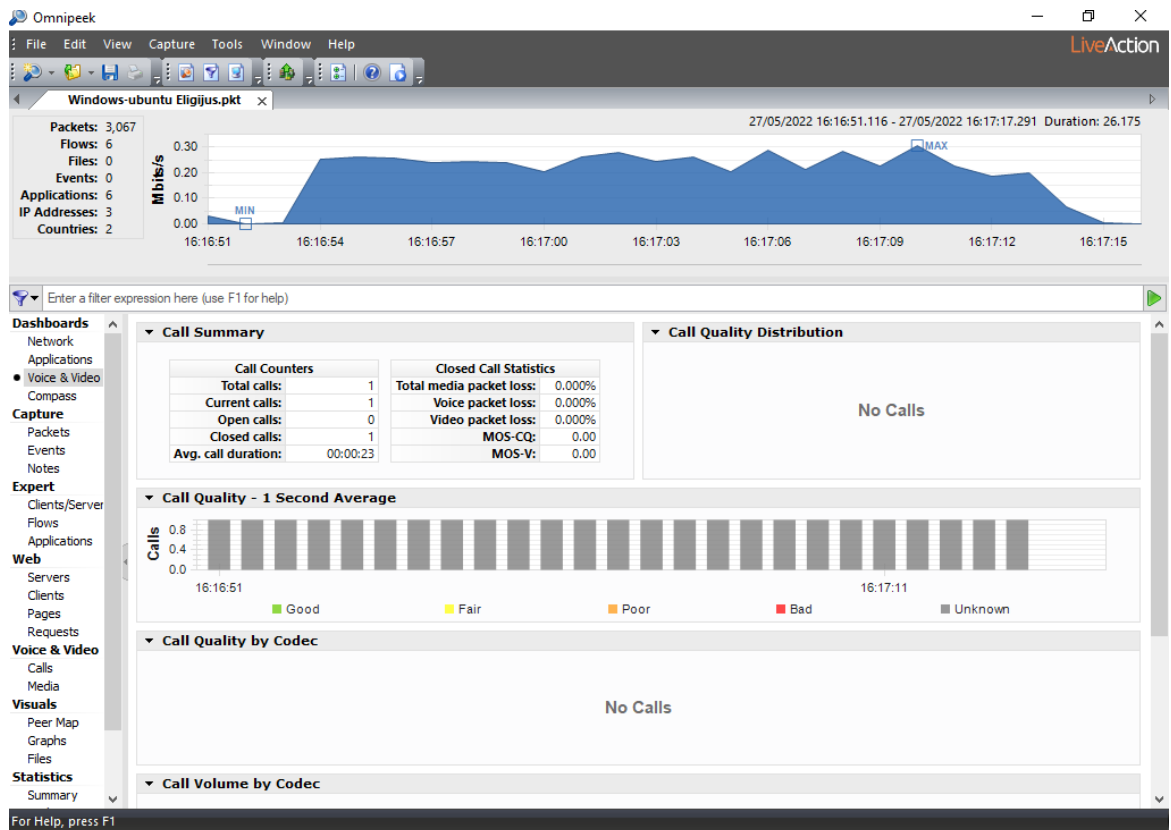


Garso siuntimui iš kompiuterio į kitą kompiuterį buvo naudojami du protokolai:

- Siuntėjo protokolas: 5070
- Gavėjo protokolas: 5062



Paanalizavus skambinimo paketą galima surasti, kokių formatu buvo siunčiami garso duomenys. Šiuo atveju buvo surasta, kad naudojamas 5070 protokolas ir G.711 formatai.



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.