



Kauno technologijos universitetas

Informatikos fakultetas

Duomenų srauto įrašo tyrimas

Kompiuterių tinklų sauga (T120M151)

Atliko:

IFM-1/3 gr. studentas

Eligijus Kiudys

2021 m. lapkričio 29 d.

Priėmė:

lekt. Dangis Rimkus

Kaunas, 2021

Turiny

Paveikslų sąrašas	3
1. Įvadas.....	4
2. Tyrimo eiga	5
2.1. Aplankytų svetainių analizė	6
2.2. Elektroninio pašto analizė	10
2.1. Naudoto serverio analizė	13
2.1. Pokalbių kambario analizė	16
2.1. Užkuoduotų paketų analizė	17
3. Išvados	19

Paveikslų sąrašas

pav. 1 Wireshark „Protocol Hierarchy“ langas	5
pav. 2 Wireshark „Conversations“ langas	5
pav. 3 Wireshark „Endpoint“ langas	5
pav. 4 Wireshark „HTTP object list“ langas	6
pav. 5 Filtras skirtas youtube.com svetainei.....	7
pav. 6 Filtras skirtas apple.com svetainei	7
pav. 7 Filtras skirtas unimelb.edu.au svetainei	8
pav. 8 Filtras skirtas yahoo.com svetainei	8
pav. 9 Filtras skirtas google.com svetainei, pirma dalis.....	9
pav. 10 Filtras skirtas google.com svetainei, antra dalis	9
pav. 11 Filtras skirtas wikipedia.org svetainei	10
pav. 12 Filtras skirtas ox.ac.uk svetainei	10
pav. 13 Elektroninio laiško protokolo filtravimas	11
pav. 14 Filtruojama informacija su prisijungimo duomenimis.....	11
pav. 15 Elektroninio pašto naudotojo vardas ir elektroninis paštas.	11
pav. 16 Elektroninio pašto laiškų informacija	12
pav. 17 Išsiųstas el. laiškas	12
pav. 18 Išsiųsto el. laiško vidus naudojant „Wireshark“	13
pav. 19 Išsiųsto el. laiško vidus naudojant „NetworkMiner“	13
pav. 20 „FTP“ protokolo filtras	14
pav. 21 „FTP“ protokolo filtras su naudotojo prisijungimu	14
pav. 22 „FTP-DATA“ protokolo filtras.....	14
pav. 23 „LIST“ komandos panaudojimas serveryje	15
pav. 24 „LIST“ komandos rezultatai	15
pav. 25 README failo vidus	16
pav. 26 „IRC“ protokolo filtras	16
Pav. 27 „WHO“ komandos rezultatai.....	17
pav. 28 „TLS“ paketų filtravimo daliniai rezultatai	17
pav. 29 Paketo sekimo rezultatas.....	18
pav. 30 Paketo sekimo rezultatas.....	18

1. Įvadas

Inžinerinio projekto metu reikia išanalizuoti naudotojo tinklą, kuriame galima rasti naudotojo veiksmus. Analizuojant naudotojo veiksmus galima pamatyti, kokiuose puslapiuose naudotojas lankėsi, galima rasti naudotojo IP adresus bei jo duomenis.

Varianto numeris: 12a.pcap

Įrašo datą ir laikas: 2012-04-12

Trukmė: 269.755436 sekundės

Esminio vartotojo IP: 10.0.2.15

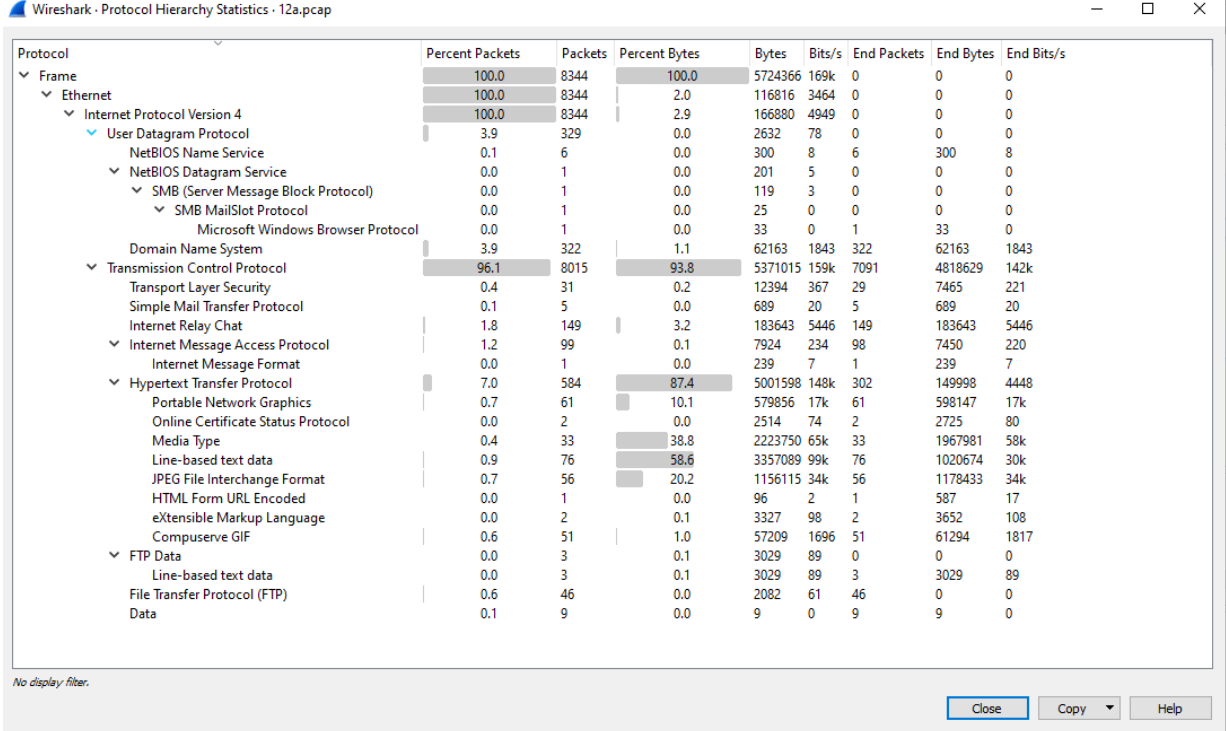
MAC adresus: 08:00:27:8a:d6:9d

OS: Windows NT 5.1 – Windows XP

Klientinės programos: Safari 5.0.5, Thunderbird 11.0.1

2. Tyrimo eiga

Atsidarius failą kurį analizuojama naudojant „Wireshark“ programą, kur paspaudžiame ant **Statistics->Protocol Hierarchy**, atsivertus informacijos langą (pav. 1) matome, kad buvo apsilankyta puslapiuose, buvo siunčiami elektroniniai laiškai.



Wireshark - Protocol Hierarchy Statistics - 12a.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	8344	100.0	5724366	169k	0	0	0
Ethernet	100.0	8344	2.0	116816	3464	0	0	0
Internet Protocol Version 4	100.0	8344	2.9	166880	4949	0	0	0
User Datagram Protocol	3.9	329	0.0	2632	78	0	0	0
NetBIOS Name Service	0.1	6	0.0	300	8	6	300	8
NetBIOS Datagram Service	0.0	1	0.0	201	5	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	3	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	0	1	33	0
Domain Name System	3.9	322	1.1	62163	1843	322	62163	1843
Transmission Control Protocol	96.1	8015	93.8	5371015	159k	7091	4818629	142k
Transport Layer Security	0.4	31	0.2	12394	367	29	7465	221
Simple Mail Transfer Protocol	0.1	5	0.0	689	20	5	689	20
Internet Relay Chat	1.8	149	3.2	183643	5446	149	183643	5446
Internet Message Access Protocol	1.2	99	0.1	7924	234	98	7450	220
Internet Message Format	0.0	1	0.0	239	7	1	239	7
Hypertext Transfer Protocol	7.0	584	87.4	5001598	148k	302	149998	4448
Portable Network Graphics	0.7	61	10.1	579856	17k	61	598147	17k
Online Certificate Status Protocol	0.0	2	0.0	2514	74	2	2725	80
Media Type	0.4	33	38.8	2223750	65k	33	1967981	58k
Line-based text data	0.9	76	58.6	3357089	99k	76	1020674	30k
JPEG File Interchange Format	0.7	56	20.2	1156115	34k	56	1178433	34k
HTML Form URL Encoded	0.0	1	0.0	96	2	1	587	17
eXtensible Markup Language	0.0	2	0.1	3327	98	2	3652	108
CompuServe GIF	0.6	51	1.0	57209	1696	51	61294	1817
FTP Data	0.0	3	0.1	3029	89	0	0	0
Line-based text data	0.0	3	0.1	3029	89	3	3029	89
File Transfer Protocol (FTP)	0.6	46	0.0	2082	61	46	0	0
Data	0.1	9	0.0	9	0	9	9	0

No display filter.

Close Copy Help

pav. 1 Wireshark „Protocol Hierarchy“ langas

Pasinaudojus „Wireshark Conversations“ langu (pav. 2) matome du pagrindinius MAC adresus, tarp kurių vyko komunikacija, viso įrašymo laikotarpiu.

Wireshark · Conversations · 12a.pcap

Ethernet · 2		IPv4 · 53		IPv6		TCP · 155		UDP · 163			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
08:00:27:8a:d6:9d	52:54:00:12:35:02	8,337	5723k	3,344	337k	4,993	5385k	0.000000	269.7554	10k	
08:00:27:8a:d6:9d	ff:ff:ff:ff:ff:ff	7	795	7	795	0	0	13.752547	213.2462	29	

pav. 2 Wireshark „Conversations“ langas

Atsivertus „Endpoint“ langą (pav. 3), matome tokius pačius MAC adresus kaip ir „Conversations“ lange (pav. 2).

Wireshark · Endpoints · 12a.pcap

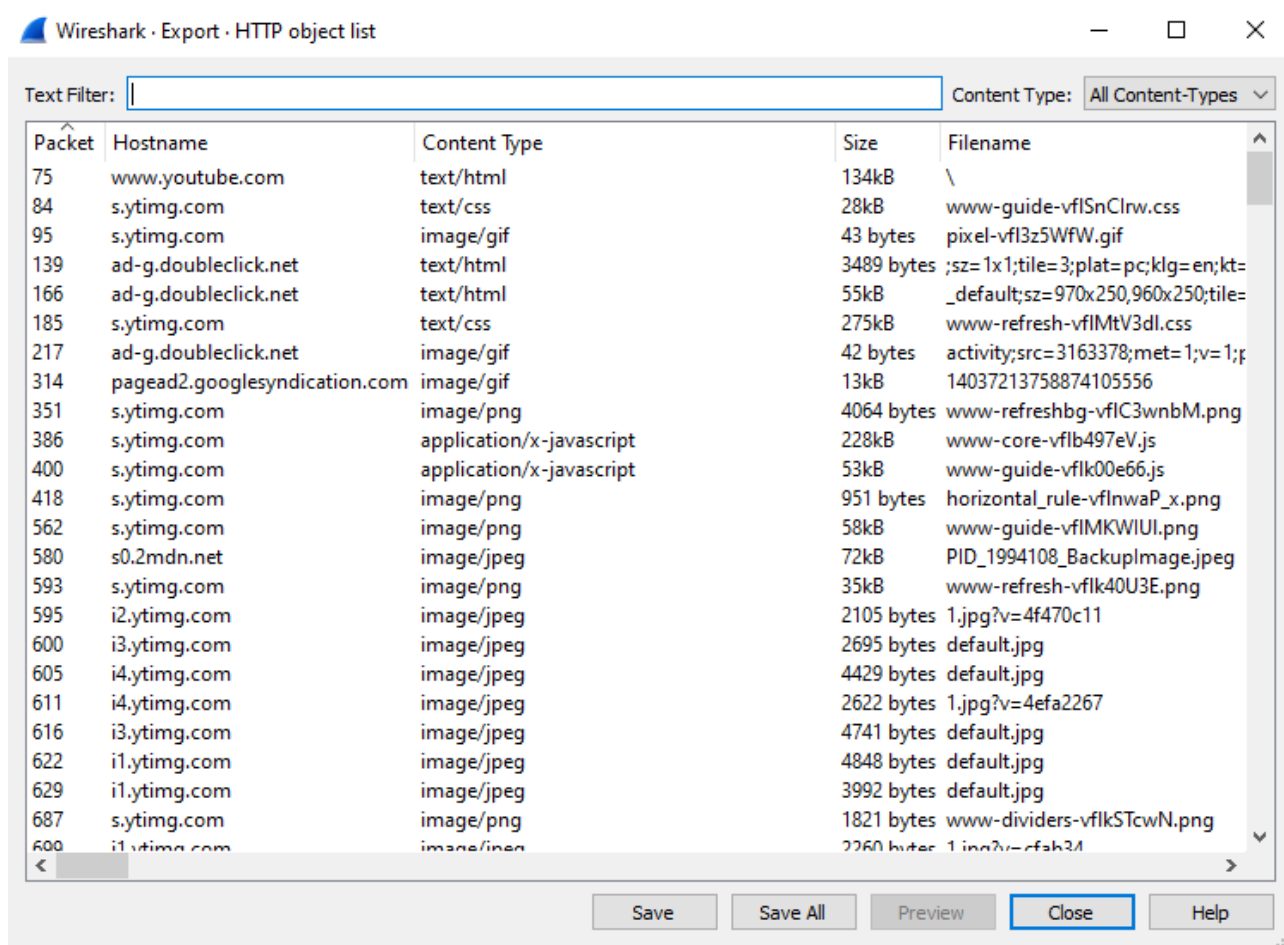
Ethernet · 3	IPv4 · 54	IPv6	TCP · 207	UDP · 163		
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
08:00:27:8a:d6:9d	8,344	5724k	3,351	338k	4,993	
52:54:00:12:35:02	8,337	5723k	4,993	5385k	3,344	
ff:ff:ff:ff:ff:ff	7	795	0	0	7	

pav. 3 Wireshark „Endpoint“ langas

Išanalizavus „Conversations“ ir „Endpoint“ langus tarp naudotojo ir galimo interneto šaltinio vykčius duomenų mainus galime analizuoti naudotojo veiklą toliau. Rastų adresų pagalba galime toliau analizuoti naudotojo veiklą.

2.1. Aplankytų svetainių analizė

Norint išsiaiškinti naudotojo aplankytus puslapius bei jų tipą reikia pasirinkti **File->Export Objects->HTTP**. Pasirinkus šią pasirinkimą atsidarys langas su naudotojo aplankytais puslapiais. Išanalizavus puslapius buvo aišku, kokiuose puslapiuose naudotojas naršė. Paaikškėjo jog naudotojas naršė puslapiuose: www.apple.com, www.youtube.com, www.unimelb.edu.au, www.yahoo.com, www.google.com, www.wikipedia.org, www.ox.ac.uk. Pasinaudojus šia komanda buvo galima pamatyti ne vien puslapius, bet ir kartu su puslapiais atsiunčiamus paveikslėlius, JavaScript priedus ir t.t. Žemiau pateiktoje nuotraukoje (pav. 4) galima pamatyti panaudotos komandos rezultatų dalį.

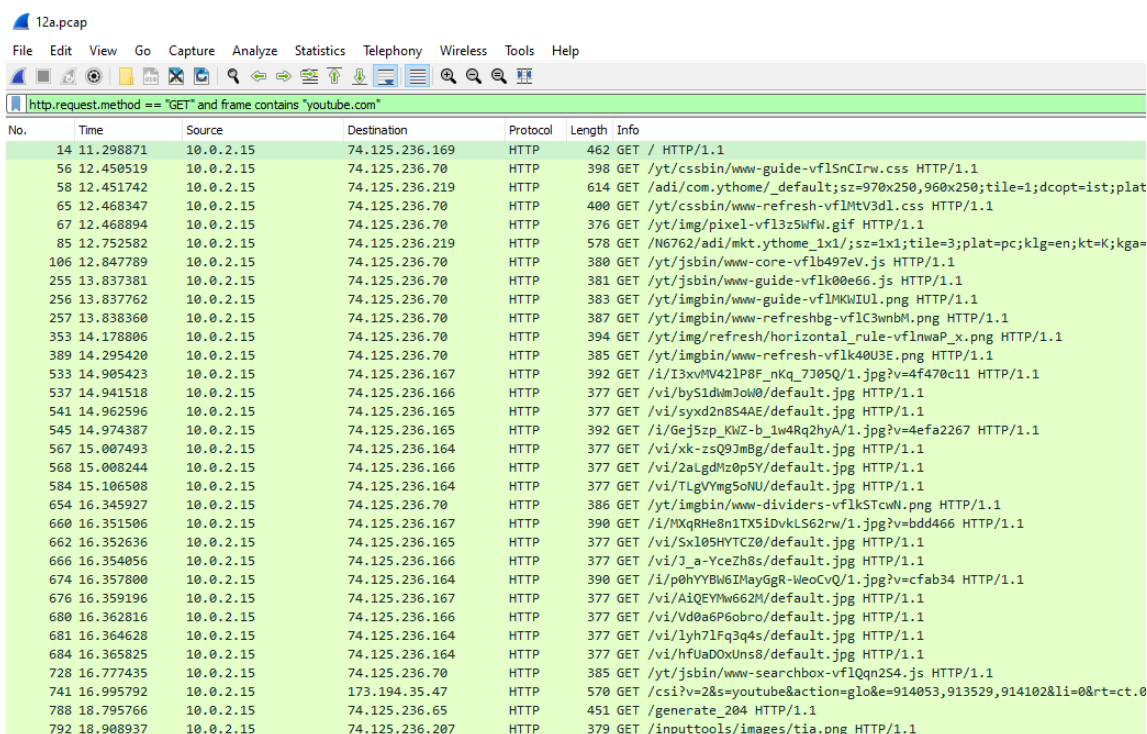


pav. 4 Wireshark „HTTP object list“ langas

Suradus puslapius, galima juos atfiltruoti ir patikrinti pasirinkto puslapio užklaudas. Tokių užklausių filtravimui bus naudojamas GET užklaudos filtravimas su pasirinktu puslapiu.

Suradus informaciją apie puslapius galime jų paketus atfiltruoti ir išsiaiškinti, ką naudotojas veikė tokiuose puslapiuose. Bendram puslapių filtravimui yra naudojama `http.request.method == "GET"` filtras. Norint sumažinti visų puslapių paketus iki pasirinkto puslapio reikia pridėti prie filtravimo `and frame contains „youtube.com“`. Atfiltravus pirmąjį puslapį www.youtube.com yra matomi

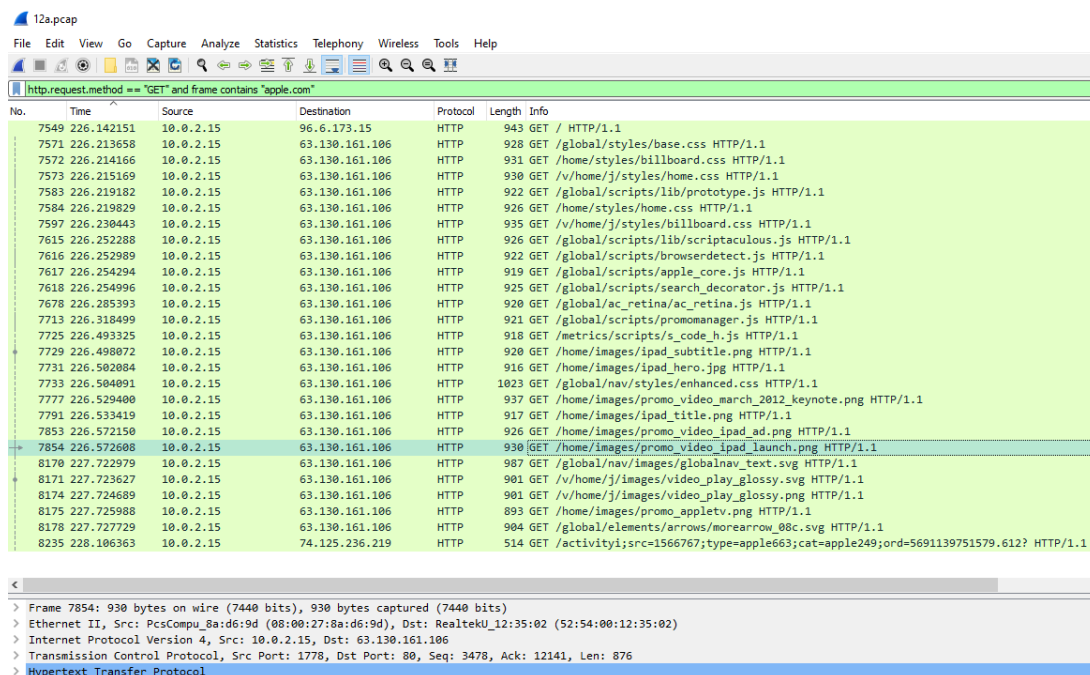
atfiltruoti rezultatai (pav. 5). Iš viso buvo rasta 32 paketai, kurių pagalba yra išanalizuojama veikla youtube.com puslapyje.



No.	Time	Source	Destination	Protocol	Length	Info
14	11.298871	10.0.2.15	74.125.236.169	HTTP	462	GET / HTTP/1.1
56	12.450519	10.0.2.15	74.125.236.70	HTTP	398	GET /yt/cssbin/www-guide-vfl5nCIrw.css HTTP/1.1
58	12.451742	10.0.2.15	74.125.236.219	HTTP	614	GET /adi/com.ythome/_default;sz=970x250,960x250;tile=1;dcopt=ist;plat=
65	12.468347	10.0.2.15	74.125.236.70	HTTP	400	GET /yt/cssbin/www-refresh-vflMtV3dL.css HTTP/1.1
67	12.468894	10.0.2.15	74.125.236.70	HTTP	376	GET /yt/img/pixel-vfl3z5WfW.gif HTTP/1.1
85	12.752582	10.0.2.15	74.125.236.219	HTTP	578	GET /N6762/adi/mkt.ythome_1x1/sz=1x1;tile=3;plat=pc;klg=en;kt=K;kg=
106	12.847789	10.0.2.15	74.125.236.70	HTTP	380	GET /yt/jsbin/www-core-vflb497eV.js HTTP/1.1
255	13.837381	10.0.2.15	74.125.236.70	HTTP	381	GET /yt/jsbin/www-guide-vflk00e66.js HTTP/1.1
256	13.837762	10.0.2.15	74.125.236.70	HTTP	383	GET /yt/imgbin/www-guide-vflMKWlU1.png HTTP/1.1
257	13.838360	10.0.2.15	74.125.236.70	HTTP	387	GET /yt/imgbin/www-refreshbg-vflC3wmbM.png HTTP/1.1
353	14.178806	10.0.2.15	74.125.236.70	HTTP	394	GET /yt/img/refresh/horizontal_rule-vflnwaP_x.png HTTP/1.1
389	14.295420	10.0.2.15	74.125.236.70	HTTP	385	GET /yt/imgbin/www-refresh-vflk40U3E.png HTTP/1.1
533	14.905423	10.0.2.15	74.125.236.167	HTTP	392	GET /i/I3xvVM42lP8F_nKq_7J05Q/1.jpg?v=4f470c11 HTTP/1.1
537	14.941518	10.0.2.15	74.125.236.166	HTTP	377	GET /vi/byS1dwm3oH0/default.jpg HTTP/1.1
541	14.962596	10.0.2.15	74.125.236.165	HTTP	377	GET /vi/syxd2n8S4AE/default.jpg HTTP/1.1
545	14.974387	10.0.2.15	74.125.236.165	HTTP	392	GET /i/Gej5zp_KNz-b_1w4Rq2hyA/1.jpg?v=defa2267 HTTP/1.1
567	15.007493	10.0.2.15	74.125.236.164	HTTP	377	GET /vi/xk-zsQ9Jm8g/default.jpg HTTP/1.1
568	15.008244	10.0.2.15	74.125.236.166	HTTP	377	GET /vi/2aLgdH20p5Y/default.jpg HTTP/1.1
584	15.106508	10.0.2.15	74.125.236.164	HTTP	377	GET /vi/TLgVmg5oNU/default.jpg HTTP/1.1
654	16.345927	10.0.2.15	74.125.236.70	HTTP	386	GET /yt/imgbin/www-dividers-vflk5TCwN.png HTTP/1.1
660	16.351506	10.0.2.15	74.125.236.167	HTTP	390	GET /i/MXqRHeBn1TX5iDvkLS62rw/1.jpg?v=bdd466 HTTP/1.1
662	16.352636	10.0.2.15	74.125.236.165	HTTP	377	GET /vi/Sx105HYTC20/default.jpg HTTP/1.1
666	16.354056	10.0.2.15	74.125.236.166	HTTP	377	GET /vi/3_a-YceZh8s/default.jpg HTTP/1.1
674	16.357800	10.0.2.15	74.125.236.164	HTTP	390	GET /i/p0hYYBw6IMayGgR-WeoCvQ/1.jpg?v=cfab34 HTTP/1.1
676	16.359196	10.0.2.15	74.125.236.167	HTTP	377	GET /vi/AiQEYw662M/default.jpg HTTP/1.1
680	16.362816	10.0.2.15	74.125.236.166	HTTP	377	GET /vi/Vd0a6P6obro/default.jpg HTTP/1.1
681	16.364628	10.0.2.15	74.125.236.164	HTTP	377	GET /vi/lyh7lFq3q4s/default.jpg HTTP/1.1
684	16.365825	10.0.2.15	74.125.236.164	HTTP	377	GET /vi/hfUaD0xUns8/default.jpg HTTP/1.1
728	16.777435	10.0.2.15	74.125.236.70	HTTP	385	GET /yt/jsbin/www-searchbox-vflQqn254.js HTTP/1.1
741	16.995792	10.0.2.15	173.194.35.47	HTTP	570	GET /csi?v=2&s=youtube&action=gl&e=914053,913529,914102&li=0&rt=ct.0
788	18.795766	10.0.2.15	74.125.236.65	HTTP	451	GET /generate_204 HTTP/1.1
792	18.908937	10.0.2.15	74.125.236.207	HTTP	379	GET /inputtools/images/tia.png HTTP/1.1

pav. 5 Filtras skirtas youtube.com svetainei

Išfiltravus pirmąjį puslapį, galime filtruoti sekantį puslapį, kuris yra apple.com. Pasirinkto puslapio filtras yra: *http.request.method == "GET" and frame contains "apple.com"*. Atfiltravus pasirinktą puslapį buvo rasti 27 paketai (pav. 6). Pirmas paketas yra skirtas puslapio atidarymui, o kiti paketai yra skirti nuotraukų ar kitokių failų atsisiuntimui.



No.	Time	Source	Destination	Protocol	Length	Info
7549	226.142151	10.0.2.15	96.6.173.15	HTTP	943	GET / HTTP/1.1
7571	226.213658	10.0.2.15	63.130.161.106	HTTP	928	GET /global/styles/base.css HTTP/1.1
7572	226.214166	10.0.2.15	63.130.161.106	HTTP	931	GET /home/styles/billboard.css HTTP/1.1
7573	226.215169	10.0.2.15	63.130.161.106	HTTP	930	GET /v/home/j/styles/home.css HTTP/1.1
7583	226.219182	10.0.2.15	63.130.161.106	HTTP	922	GET /global/scripts/lib/prototype.js HTTP/1.1
7584	226.219829	10.0.2.15	63.130.161.106	HTTP	926	GET /home/styles/home.css HTTP/1.1
7597	226.230443	10.0.2.15	63.130.161.106	HTTP	935	GET /v/home/j/styles/billboard.css HTTP/1.1
7615	226.252288	10.0.2.15	63.130.161.106	HTTP	926	GET /global/scripts/lib/scriptaculous.js HTTP/1.1
7616	226.252989	10.0.2.15	63.130.161.106	HTTP	922	GET /global/scripts/browserdetect.js HTTP/1.1
7617	226.254294	10.0.2.15	63.130.161.106	HTTP	919	GET /global/scripts/apple_core.js HTTP/1.1
7618	226.254996	10.0.2.15	63.130.161.106	HTTP	925	GET /global/scripts/search_decorator.js HTTP/1.1
7678	226.285393	10.0.2.15	63.130.161.106	HTTP	920	GET /global/ac_retina/ac_retina.js HTTP/1.1
7713	226.318499	10.0.2.15	63.130.161.106	HTTP	921	GET /global/scripts/promomanager.js HTTP/1.1
7725	226.493325	10.0.2.15	63.130.161.106	HTTP	918	GET /metrics/scripts/s_code_h.js HTTP/1.1
7729	226.498072	10.0.2.15	63.130.161.106	HTTP	920	GET /home/images/ipad_subtitle.png HTTP/1.1
7731	226.502084	10.0.2.15	63.130.161.106	HTTP	916	GET /home/images/ipad_hero.jpg HTTP/1.1
7733	226.504091	10.0.2.15	63.130.161.106	HTTP	1023	GET /global/nav/styles/enhanced.css HTTP/1.1
7777	226.529400	10.0.2.15	63.130.161.106	HTTP	937	GET /home/images/promo_video_march_2012_keynote.png HTTP/1.1
7791	226.533419	10.0.2.15	63.130.161.106	HTTP	917	GET /home/images/ipad_title.png HTTP/1.1
7853	226.572150	10.0.2.15	63.130.161.106	HTTP	926	GET /home/images/promo_video_ipad_ad.png HTTP/1.1
7854	226.572608	10.0.2.15	63.130.161.106	HTTP	930	GET /home/images/promo_video_ipad_launch.png HTTP/1.1
8170	227.722979	10.0.2.15	63.130.161.106	HTTP	987	GET /global/nav/images/globalnav_text.svg HTTP/1.1
8171	227.723627	10.0.2.15	63.130.161.106	HTTP	901	GET /v/home/j/images/video_play_glossy.svg HTTP/1.1
8174	227.724689	10.0.2.15	63.130.161.106	HTTP	901	GET /v/home/j/images/video_play_glossy.png HTTP/1.1
8175	227.725988	10.0.2.15	63.130.161.106	HTTP	893	GET /home/images/promo_appletv.png HTTP/1.1
8178	227.727729	10.0.2.15	63.130.161.106	HTTP	904	GET /global/elements/arrows/morearrow_08c.svg HTTP/1.1
8235	228.106363	10.0.2.15	74.125.236.219	HTTP	514	GET /activity?src=1566767;type=apple663;cat=apple249;ord=5691139751579.612? HTTP/1.1

<

>

> Frame 7854: 930 bytes on wire (7440 bits), 930 bytes captured (7440 bits)

> Ethernet II, Src: PcsCompu_8a:d6:9d (08:00:27:8a:d6:9d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

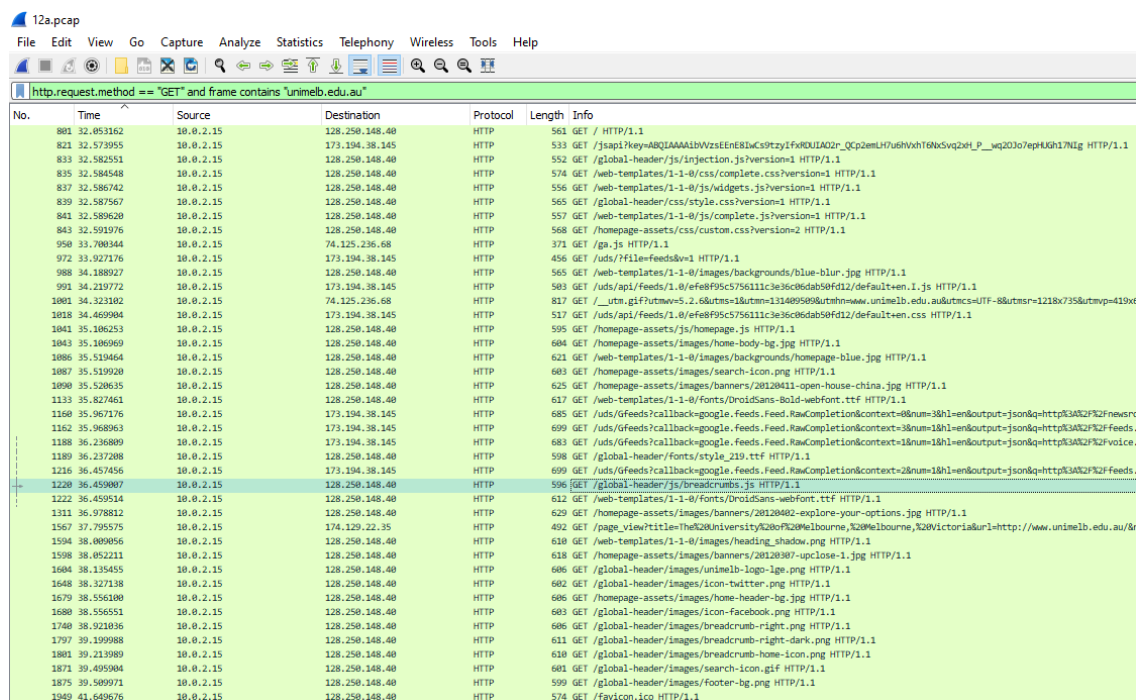
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 63.130.161.106

> Transmission Control Protocol, Src Port: 1778, Dst Port: 80, Seq: 3478, Ack: 12141, Len: 876

> Hypertext Transfer Protocol

pav. 6 Filtras skirtas apple.com svetainei

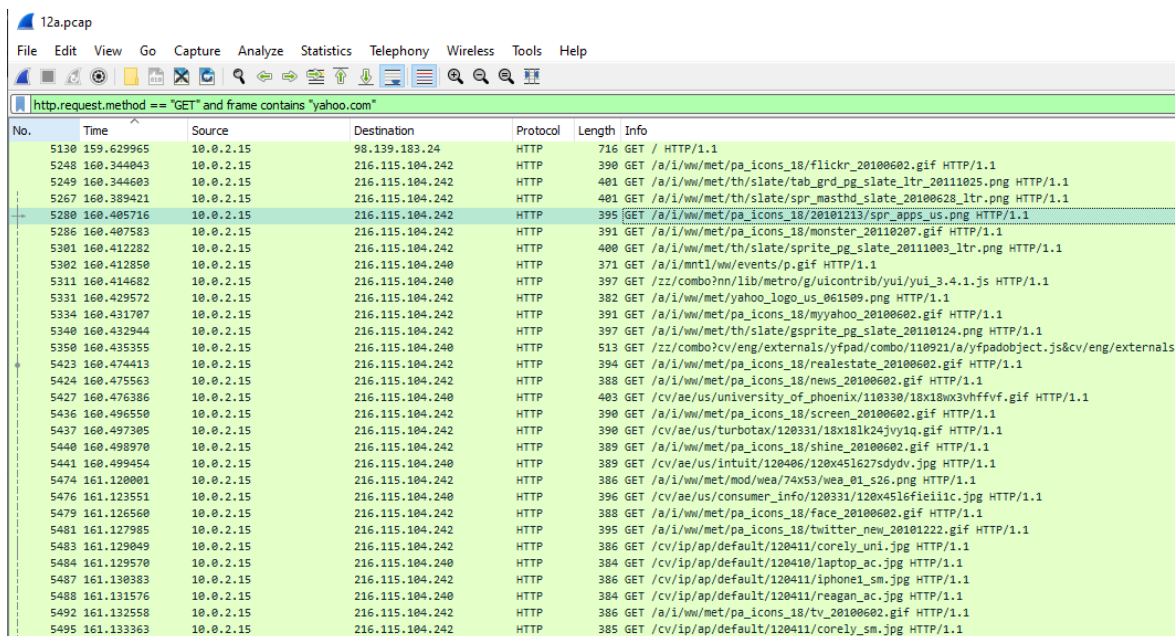
Tęsiame puslapių paketų filtravimą su kitu naudotojo naršytu puslapiu. Kitas pasirinktas puslapis buvo unimelb.edu.au. Filtravimui yra naudojamas toks filtras: *http.request.method == "GET" and frame contains "unimelb.edu.au"*. Atfiltravus paketus buvo rasta 41 paketas (pav. 7). Pirmasis paketas yra skirtas pačio puslapio atvertimui, kiti paketai yra skirti nuotraukų ir kitų failų atidarymui.



No.	Time	Source	Destination	Protocol	Length	Info
801	32.053162	10.0.2.15	128.250.148.40	HTTP	563	GET / HTTP/1.1
821	32.573955	10.0.2.15	173.194.38.145	HTTP	533	GET /jsapi?key=AQIAAAABVzstEeK8wCstzIfxR0UQA2n_QCp2mHvUshVxH6N6SvQ2eH_P_wq2037epHkH7Nig HTTP/1.1
833	32.582551	10.0.2.15	128.250.148.40	HTTP	552	GET /global-header/js/injection.js?version=1 HTTP/1.1
835	32.584548	10.0.2.15	128.250.148.40	HTTP	574	GET /web-templates/1-1-0/css/complete.css?version=1 HTTP/1.1
837	32.586742	10.0.2.15	128.250.148.40	HTTP	556	GET /web-templates/1-1-0/js/widgets.js?version=1 HTTP/1.1
839	32.587967	10.0.2.15	128.250.148.40	HTTP	565	GET /global-header/css/style.css?version=1 HTTP/1.1
841	32.589620	10.0.2.15	128.250.148.40	HTTP	557	GET /web-templates/1-1-0/js/complete.js?version=1 HTTP/1.1
843	32.591976	10.0.2.15	128.250.148.40	HTTP	568	GET /homepage-assets/css/custom.css?version=2 HTTP/1.1
950	33.700344	10.0.2.15	74.125.236.68	HTTP	371	GET /ga.js HTTP/1.1
972	33.927176	10.0.2.15	173.194.38.145	HTTP	456	GET /uds/?file=feeds&v=1 HTTP/1.1
988	34.188927	10.0.2.15	128.250.148.40	HTTP	565	GET /web-templates/1-1-0/images/backgrounds/blue-blur.jpg HTTP/1.1
993	34.219772	10.0.2.15	173.194.38.145	HTTP	517	GET /uds/api/feeds/1.0/efef8f9c575611c3e3c06dab58fd12/default+en.1.js HTTP/1.1
1001	34.323182	10.0.2.15	74.125.236.68	HTTP	817	GET /_utm_gif?utmwv=5.2.6&utms=1&utm=131489589&utmn=www.unimelb.edu.au&utmc=UTP-8&utmsr=1218x735&utmp=419x610 HTTP/1.1
1010	34.469984	10.0.2.15	173.194.38.145	HTTP	595	GET /homepage-assets/js/homepage.js HTTP/1.1
1043	35.106253	10.0.2.15	128.250.148.40	HTTP	604	GET /homepage-assets/images/home-body-bg.jpg HTTP/1.1
1043	35.106969	10.0.2.15	128.250.148.40	HTTP	621	GET /web-templates/1-1-0/images/backgrounds/homepage-blue.jpg HTTP/1.1
1088	35.539464	10.0.2.15	128.250.148.40	HTTP	603	GET /homepage-assets/images/search-icon.png HTTP/1.1
1087	35.539920	10.0.2.15	128.250.148.40	HTTP	625	GET /homepage-assets/images/banners/20120411-open-house-china.jpg HTTP/1.1
1090	35.528635	10.0.2.15	128.250.148.40	HTTP	617	GET /web-templates/1-1-0/fonts/DroidSans-Bold-webfont.ttf HTTP/1.1
1133	35.827461	10.0.2.15	173.194.38.145	HTTP	685	GET /uds/feeds?callback=google.feeds.Feed.RawCompletionContext+0&num=3&hl=en&output=json&q=http%3A%2F%2Fnewsr.com HTTP/1.1
1160	35.967176	10.0.2.15	173.194.38.145	HTTP	699	GET /uds/feeds?callback=google.feeds.Feed.RawCompletionContext+3&num=1&hl=en&output=json&q=http%3A%2F%2Fnewsr.com HTTP/1.1
1162	35.968963	10.0.2.15	173.194.38.145	HTTP	683	GET /uds/feeds?callback=google.feeds.Feed.RawCompletionContext+3&num=1&hl=en&output=json&q=http%3A%2F%2Fnewsr.com HTTP/1.1
1180	36.216809	10.0.2.15	128.250.148.40	HTTP	508	GET /global-header/fonts/style_219.ttf HTTP/1.1
1189	36.237208	10.0.2.15	128.250.148.40	HTTP	609	GET /uds/feeds?callback=google.feeds.Feed.RawCompletionContext+2&num=1&hl=en&output=json&q=http%3A%2F%2Fnewsr.com HTTP/1.1
1216	36.457456	10.0.2.15	173.194.38.145	HTTP	596	GET /global-header/js/breadcrumbs.js HTTP/1.1
1220	36.459007	10.0.2.15	128.250.148.40	HTTP	612	GET /web-templates/1-1-0/fonts/DroidSans-webfont.ttf HTTP/1.1
1222	36.459514	10.0.2.15	128.250.148.40	HTTP	629	GET /homepage-assets/images/banners/20120402-explore-your-options.jpg HTTP/1.1
1311	36.978812	10.0.2.15	128.250.148.40	HTTP	492	GET /page_view?title=The%20University%20of%20Melbourne,%20Victoria&url=http://www.unimelb.edu.au/kr HTTP/1.1
1367	37.795575	10.0.2.15	174.129.22.35	HTTP	610	GET /web-templates/1-1-0/images/heading_shadow.png HTTP/1.1
1594	38.009956	10.0.2.15	128.250.148.40	HTTP	618	GET /homepage-assets/images/banners/20120307-up-close-1.jpg HTTP/1.1
1598	38.052211	10.0.2.15	128.250.148.40	HTTP	606	GET /global-header/images/unimelb-logo-lge.png HTTP/1.1
1604	38.135455	10.0.2.15	128.250.148.40	HTTP	602	GET /global-header/images/icon-twitter.png HTTP/1.1
1648	38.327138	10.0.2.15	128.250.148.40	HTTP	606	GET /homepage-assets/images/home-header-bg.jpg HTTP/1.1
1679	38.556100	10.0.2.15	128.250.148.40	HTTP	603	GET /global-header/images/icon-facebook.png HTTP/1.1
1680	38.556551	10.0.2.15	128.250.148.40	HTTP	606	GET /global-header/images/breadcrumb-right.png HTTP/1.1
1740	38.921036	10.0.2.15	128.250.148.40	HTTP	611	GET /global-header/images/breadcrumb-right-dark.png HTTP/1.1
1797	39.199988	10.0.2.15	128.250.148.40	HTTP	610	GET /global-header/images/breadcrumb-home-icon.png HTTP/1.1
1801	39.213989	10.0.2.15	128.250.148.40	HTTP	601	GET /global-header/images/search-icon.gif HTTP/1.1
1871	39.405984	10.0.2.15	128.250.148.40	HTTP	599	GET /global-header/images/footer-bg.png HTTP/1.1
1875	39.506971	10.0.2.15	128.250.148.40	HTTP	574	GET /favicon.ico HTTP/1.1
1940	41.649676	10.0.2.15	128.250.148.40	HTTP		

pav. 7 Filtras skirtas unimelb.edu.au svetainei

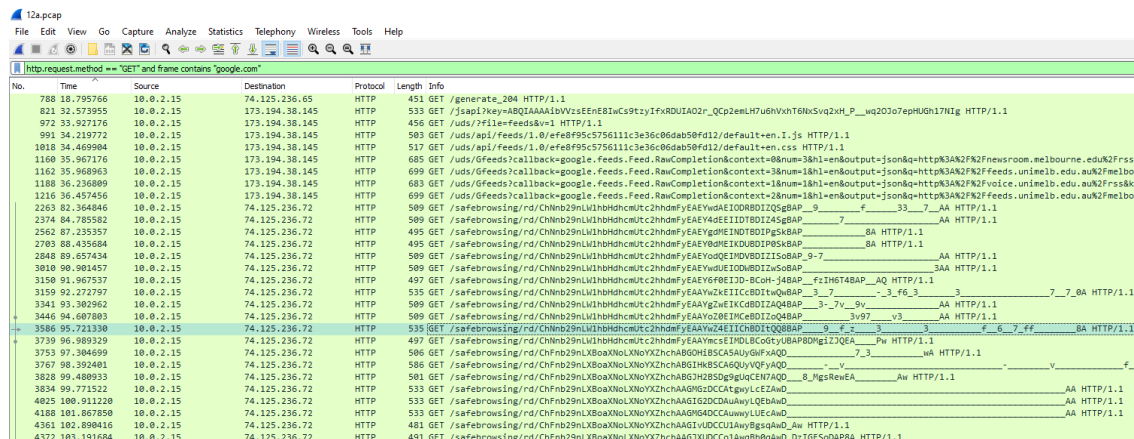
Išfiltravus kitą pasirinktą puslapį, kuris yra yahoo.com, buvo gauti išfiltruoti pasirinkto puslapio paketai. Puslapio paketų filtravimui yra naudojamas filtras: *http.request.method == "GET" and frame contains "yahoo.com"*. Atfiltruotų paketų kiekis yra 88 paketai. Kadangi buvo atfiltruota tiek daug paketų, nuotraukoje yra matoma ne visi paketai (pav. 8). Pirmasis paketas yra skirtas puslapio užklausai, visi kiti paketai yra skirti failų atsisiuntimams, kaip ir kituose puslapiuose.



No.	Time	Source	Destination	Protocol	Length	Info
5130	159.629965	10.0.2.15	98.139.183.24	HTTP	716	GET / HTTP/1.1
5248	160.344043	10.0.2.15	216.115.104.242	HTTP	390	GET /a/1/wm/met/pa_icons_18/flickr_20100602.gif HTTP/1.1
5249	160.344603	10.0.2.15	216.115.104.242	HTTP	401	GET /a/1/wm/met/th/slate/tab_grd_pg_slate_ltr_20111025.png HTTP/1.1
5267	160.389421	10.0.2.15	216.115.104.242	HTTP	401	GET /a/1/wm/met/th/slate/spr_masthd_slate_20100628_ltr.png HTTP/1.1
5280	160.405716	10.0.2.15	216.115.104.242	HTTP	395	GET /a/1/wm/met/pa_icons_18/20101213/spr_apps_us.png HTTP/1.1
5286	160.407583	10.0.2.15	216.115.104.242	HTTP	391	GET /a/1/wm/met/pa_icons_18/monster_20110207.gif HTTP/1.1
5301	160.412282	10.0.2.15	216.115.104.242	HTTP	400	GET /a/1/wm/met/th/slate/sprite_pg_slate_20111003_ltr.png HTTP/1.1
5302	160.412850	10.0.2.15	216.115.104.240	HTTP	371	GET /a/1/mnt/1/wm/events/p.gif HTTP/1.1
5311	160.414682	10.0.2.15	216.115.104.240	HTTP	397	GET /zz/combo?nn/lib/metro/g/uicontrib/yui/yui_3.4.1.js HTTP/1.1
5331	160.429572	10.0.2.15	216.115.104.242	HTTP	382	GET /a/1/wm/met/yahoo_logo_us_061509.png HTTP/1.1
5334	160.431707	10.0.2.15	216.115.104.242	HTTP	391	GET /a/1/wm/met/pa_icons_18/myyahoo_20100602.gif HTTP/1.1
5340	160.432944	10.0.2.15	216.115.104.242	HTTP	397	GET /a/1/wm/met/th/slate/gsprite_pg_slate_20110124.png HTTP/1.1
5350	160.435355	10.0.2.15	216.115.104.240	HTTP	513	GET /zz/combo?cv/eng/externals/yfpad/combo/110921/a/yfpadobject.js&cv/eng/externals HTTP/1.1
5423	160.474413	10.0.2.15	216.115.104.242	HTTP	394	GET /a/1/wm/met/pa_icons_18/realstate_20100602.gif HTTP/1.1
5424	160.475563	10.0.2.15	216.115.104.242	HTTP	388	GET /a/1/wm/met/pa_icons_18/news_20100602.gif HTTP/1.1
5427	160.476386	10.0.2.15	216.115.104.240	HTTP	403	GET /cv/ae/us/university_of_phoenix/110330/181818x3vhhfuf.gif HTTP/1.1
5436	160.496550	10.0.2.15	216.115.104.242	HTTP	390	GET /a/1/wm/met/pa_icons_18/screen_20100602.gif HTTP/1.1
5437	160.497305	10.0.2.15	216.115.104.242	HTTP	390	GET /cv/ae/us/turbotax/120331/181818x24jyvj1.gif HTTP/1.1
5440	160.498970	10.0.2.15	216.115.104.242	HTTP	389	GET /a/1/wm/met/pa_icons_18/shine_20100602.gif HTTP/1.1
5441	160.499454	10.0.2.15	216.115.104.240	HTTP	389	GET /cv/ae/us/intuit/120406/120x451627dydv.jpg HTTP/1.1
5474	161.120081	10.0.2.15	216.115.104.242	HTTP	386	GET /a/1/wm/met/mod/wea/74x53/wea_01_s26.png HTTP/1.1
5476	161.123551	10.0.2.15	216.115.104.240	HTTP	396	GET /cv/ae/us/consumer_info/120331/120x4516f1e1ic.jpg HTTP/1.1
5479	161.126560	10.0.2.15	216.115.104.242	HTTP	388	GET /a/1/wm/met/pa_icons_18/face_20100602.gif HTTP/1.1
5481	161.127985	10.0.2.15	216.115.104.242	HTTP	395	GET /a/1/wm/met/pa_icons_18/twitter_new_20101222.gif HTTP/1.1
5483	161.129489	10.0.2.15	216.115.104.242	HTTP	386	GET /cv/ip/ap/default/120411/corely_uni.jpg HTTP/1.1
5484	161.129570	10.0.2.15	216.115.104.240	HTTP	384	GET /cv/ip/ap/default/120410/laptop_ac.jpg HTTP/1.1
5487	161.130383	10.0.2.15	216.115.104.242	HTTP	386	GET /cv/ip/ap/default/120411/iphone1_sm.jpg HTTP/1.1
5488	161.131576	10.0.2.15	216.115.104.240	HTTP	384	GET /cv/ip/ap/default/120411/reagan_ac.jpg HTTP/1.1
5492	161.132558	10.0.2.15	216.115.104.242	HTTP	386	GET /a/1/wm/met/pa_icons_18/tv_20100602.gif HTTP/1.1
5495	161.133363	10.0.2.15	216.115.104.242	HTTP	385	GET /cv/ip/ap/default/120411/corely_sm.jpg HTTP/1.1

pav. 8 Filtras skirtas yahoo.com svetainei

Kitas puslapis, kuris filtruojamas yra google.com. Šis puslapis yra populiariausias paieškos puslapis. Filtravimui yra naudojamas filtras: *http.request.method == "GET" and frame contains "google.com"*. Atfiltravus pasirinktą puslapį buvo gauti 43 paketai. Pirmoje nuotraukoje (pav. 9) pagal URL adresą galima nustatyti, kad naudotojas po paieškos bandė eiti į nesaugų puslapį. Einant į nesaugius puslapius per google.com pasikeičia URI kuris pradžioje yra „safebrowsing“.



No.	Time	Source	Destination	Protocol	Length	Info
788	10.795766	10.0.2.15	74.125.236.65	HTTP	451	GET /generate_204 HTTP/1.1
823	32.573955	10.0.2.15	173.194.38.145	HTTP	533	GET /jsapi?key=ABQI... HTTP/1.1
973	33.927176	10.0.2.15	173.194.38.145	HTTP	456	GET /uds/?file=feeds&v=1 HTTP/1.1
993	34.219772	10.0.2.15	173.194.38.145	HTTP	503	GET /uds/api/feeds/1.0/efe8f95c575611c3e36c06dab50fd12/default+en.i.js HTTP/1.1
1018	34.469904	10.0.2.15	173.194.38.145	HTTP	517	GET /uds/api/feeds/1.0/efe8f95c575611c3e36c06dab50fd12/default+en.css HTTP/1.1
1168	35.967176	10.0.2.15	173.194.38.145	HTTP	685	GET /uds/feeds/callback-google.feeds.Feed.RawCompletionContext+0&num=1&hl=en&output=json&q=http%3A%2F%2Fnewsroom.melbourne.edu.au%2Frss&... HTTP/1.1
1167	35.968063	10.0.2.15	173.194.38.145	HTTP	689	GET /uds/feeds/callback-google.feeds.Feed.RawCompletionContext+3&num=1&hl=en&output=json&q=http%3A%2F%2Ffeeds.unimelb.edu.au%2Frss&... HTTP/1.1
1188	36.236889	10.0.2.15	173.194.38.145	HTTP	683	GET /uds/feeds/callback-google.feeds.Feed.RawCompletionContext+1&num=1&hl=en&output=json&q=http%3A%2F%2Fvoice.unimelb.edu.au%2Frss&... HTTP/1.1
1216	36.457456	10.0.2.15	173.194.38.145	HTTP	699	GET /uds/feeds/callback-google.feeds.Feed.RawCompletionContext+2&num=1&hl=en&output=json&q=http%3A%2F%2Ffeeds.unimelb.edu.au%2Frss&... HTTP/1.1
2263	82.364846	10.0.2.15	74.125.236.72	HTTP	589	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_9_... HTTP/1.1
2374	84.785582	10.0.2.15	74.125.236.72	HTTP	589	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_7_... HTTP/1.1
2562	87.235537	10.0.2.15	74.125.236.72	HTTP	495	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8A HTTP/1.1
2783	88.435604	10.0.2.15	74.125.236.72	HTTP	495	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8A HTTP/1.1
2848	89.657434	10.0.2.15	74.125.236.72	HTTP	589	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_9-7_... HTTP/1.1
3010	90.981457	10.0.2.15	74.125.236.72	HTTP	589	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_3v97_v3_... HTTP/1.1
3158	91.967537	10.0.2.15	74.125.236.72	HTTP	497	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_Fz1H6T4BAP_AQ HTTP/1.1
3159	92.272797	10.0.2.15	74.125.236.72	HTTP	535	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_3_7_... HTTP/1.1
3341	93.382982	10.0.2.15	74.125.236.72	HTTP	589	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_3_7v_9v_... HTTP/1.1
3446	94.607883	10.0.2.15	74.125.236.72	HTTP	589	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_3v97_v3_... HTTP/1.1
3588	95.721330	10.0.2.15	74.125.236.72	HTTP	535	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_9_7_... HTTP/1.1
3739	96.989329	10.0.2.15	74.125.236.72	HTTP	497	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_Pw HTTP/1.1
3753	97.384699	10.0.2.15	74.125.236.72	HTTP	586	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_7_3_... HTTP/1.1
3767	98.302481	10.0.2.15	74.125.236.72	HTTP	586	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_7_3_... HTTP/1.1
3828	99.477522	10.0.2.15	74.125.236.72	HTTP	501	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8_... HTTP/1.1
3834	99.771522	10.0.2.15	74.125.236.72	HTTP	533	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8_... HTTP/1.1
4029	100.911220	10.0.2.15	74.125.236.72	HTTP	533	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8_... HTTP/1.1
4188	101.867858	10.0.2.15	74.125.236.72	HTTP	533	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8_... HTTP/1.1
4361	102.898416	10.0.2.15	74.125.236.72	HTTP	481	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8_... HTTP/1.1
4372	103.191684	10.0.2.15	74.125.236.72	HTTP	491	GET /safebrowsing/rd/ChNb29nLWl1bHhhdnctc2hhdmFyEAY6dE1D10B1Z4g8AP_8_... HTTP/1.1

pav. 9 Filtras skirtas google.com svetainei, pirma dalis

Toliau išanalizavus atfiltruotus google.com paketus galime pastebėti ko naudotojas ieškojo ir kur toliau lankėsi (pav. 10). Paketų rezultatuose matoma, kad naudotojas ieškojo „cross site scripting“ raktažodžio. Atvertus paieškos rezultatą naudotojas atsivertė wikipedia.org puslapį apie „cross site scripting“. Grįžęs iš wikipedia.org puslapio į google.com puslapį naudotojas atliko kitą paiešką apie „denial of service“. Google pateikęs paieškos rezultatą naudotojas atsivertė kitą wikipedia.org puslapį kuris buvo apie „Denial-of-service attack“.



4593	139.457395	10.0.2.15	74.125.235.48	HTTP	750	GET /search?hl=en&output=search&client=psy-ab&q=cross+site+scripting&btnk= HTTP/1.1
4672	140.323069	10.0.2.15	74.125.235.48	HTTP	731	GET /images/nav_logo107.png HTTP/1.1
4693	140.473104	10.0.2.15	74.125.235.48	HTTP	610	GET /sdcch/t0-65Pr1.dct HTTP/1.1
4722	140.678774	10.0.2.15	74.125.235.55	HTTP	746	GET /verify/EAAAAK2w0hL0rMv7xytPouccogk.gif HTTP/1.1
4773	141.049305	10.0.2.15	74.125.235.48	HTTP	866	GET /search?hl=en&output=search&client=psy-ab&q=cross+site+scripting&gbv=l&sei=pvyFT5rDCCf3Rqel-ZjV8g HTTP/1.1
4819	141.468523	10.0.2.15	74.125.235.48	HTTP	765	GET /images/nav_logo_h20.png HTTP/1.1
4858	141.815130	10.0.2.15	74.125.236.207	HTTP	519	GET /gb/images/b_BdSafce09.png HTTP/1.1
4891	144.569593	10.0.2.15	74.125.235.48	HTTP	941	GET /ur/l?http://en.wikipedia.org/wiki/Cross-site_scripting&sa=U&ei=p_yFT6jdsKqrAeUz7HC8&ved=0CB4QFjAA&usg=AF... HTTP/1.1
4897	144.868168	10.0.2.15	208.80.154.225	HTTP	581	GET /wiki/Cross-site_scripting HTTP/1.1
7232	209.628167	10.0.2.15	74.125.235.48	HTTP	672	GET / HTTP/1.1
7370	217.195400	10.0.2.15	74.125.235.48	HTTP	815	GET /search?client=psy-ab&hl=en&site=source=hp&q=denial+of+service&btnk=Google+Search HTTP/1.1
7399	218.075123	10.0.2.15	74.125.236.160	HTTP	755	GET /news/tbn/ymQAr2ARmHJ/6.jpg HTTP/1.1
7426	223.662026	10.0.2.15	74.125.235.48	HTTP	930	GET /ur/l?http://en.wikipedia.org/wiki/Denial-of-service_attack&sa=U&ei=8_yFT_nIN9DMwQFLk_2_Bg&ved=0CBwQFjAA&usg=AF... HTTP/1.1
7432	223.969787	10.0.2.15	208.80.154.225	HTTP	570	GET /wiki/Denial-of-service_attack HTTP/1.1

pav. 10 Filtras skirtas google.com svetainei, antra dalis

Filtruojam toliau internetinių puslapių užklausas. Kitas internetinis puslapis kurio paketai filtruoti yra wikipedia.org. Atfiltravus pasirinkto puslapio paketus yra rasta tik 17 paketų (pav. 11). Tarp atfiltruotų paketų yra du paketai, kurie skirti pačio puslapio atvertimui, kiti paketai yra skirti gauti puslapio failus.

No.	Time	Source	Destination	Protocol	Length	Info
1961	53.547293	64.12.143.164	10.0.2.15	IMAP	72	Response: * OK IMAP4 ready
1964	53.672246	10.0.2.15	64.12.143.164	IMAP	68	Request: 1 capability
1966	53.694892	64.12.143.164	10.0.2.15	IMAP	171	Response: 1 OK completed
1969	53.726789	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
1973	53.777575	64.12.143.164	10.0.2.15	IMAP	291	Response: 3 OK LOGIN completed
1974	53.778803	10.0.2.15	64.12.143.164	IMAP	67	Request: 4 namespace
1979	53.803237	64.12.143.164	10.0.2.15	IMAP	112	Response: 4 OK NAMESPACE completed
1982	53.805470	10.0.2.15	64.12.143.164	IMAP	102	Request: 5 ID ("name" "Thunderbird" "version" "11.0.1")
1984	53.828747	64.12.143.164	10.0.2.15	IMAP	163	Response: 5 OK ID completed
1985	53.839045	10.0.2.15	64.12.143.164	IMAP	69	Request: 6 lsub "" ""
1987	53.862613	64.12.143.164	10.0.2.15	IMAP	353	Response: 6 OK LSUB completed
1988	53.864244	10.0.2.15	64.12.143.164	IMAP	73	Request: 7 list "" "INBOX"
1993	53.886327	64.12.143.164	10.0.2.15	IMAP	112	Response: 7 OK LIST completed
1994	53.889146	10.0.2.15	64.12.143.164	IMAP	72	Request: 8 select "INBOX"
1996	53.918465	64.12.143.164	10.0.2.15	IMAP	694	Response: 8 OK [READ-WRITE] SELECT completed
1997	53.919190	10.0.2.15	64.12.143.164	IMAP	78	Request: 9 getquotaroot "INBOX"
1999	53.942952	64.12.143.164	10.0.2.15	IMAP	104	Response: 9 OK GETQUOTAROOT completed
2005	54.094165	10.0.2.15	64.12.143.164	IMAP	63	Request: 10 IDLE
2007	54.117134	64.12.143.164	10.0.2.15	IMAP	65	Response: + idling
2018	68.890612	64.12.143.164	10.0.2.15	IMAP	72	Response: * OK IMAP4 ready
2019	68.891627	10.0.2.15	64.12.143.164	IMAP	68	Request: 1 capability
2021	68.913674	64.12.143.164	10.0.2.15	IMAP	171	Response: 1 OK completed
2022	68.928601	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
2024	68.985664	64.12.143.164	10.0.2.15	IMAP	291	Response: 3 OK LOGIN completed
2025	68.986667	10.0.2.15	64.12.143.164	IMAP	102	Request: 4 ID ("name" "Thunderbird" "version" "11.0.1")
2027	69.033990	64.12.143.164	10.0.2.15	IMAP	163	Response: 4 OK ID completed
2028	69.035016	10.0.2.15	64.12.143.164	IMAP	106	Request: 5 STATUS "Drafts" (UIDNEXT MESSAGES UNSEEN RECENT)
2030	69.057813	64.12.143.164	10.0.2.15	IMAP	137	Response: 5 OK STATUS completed

pav. 13 Elektroninio laiško protokolo filtravimas

Išsiaiškinus, kad naudotojas naudojo elektroninį paštą buvo toliau ieškoma paketų su informacija apie naudotoją. Panaudojus *imap and frame contains "login"* filtrą buvo rasti penki paketai kurie yra susieti su prisijungimo informacija (pav. 14). Pirmame pakete iškarto yra matomas naudotojo prisijungimas ir slaptažodis prie elektroninio pašto paskyros. Esminiai paketai: 1969 2022 2054 ir 2222 atskleidžia naudotojo prisijungimo vardą "frederickflintstone" ir slaptažodį „1234abcd“.

No.	Time	Source	Destination	Protocol	Length	Info
1969	53.726789	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
2022	68.928601	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
2054	70.230017	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
2222	71.281443	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
4447	104.966593	10.0.2.15	64.12.143.164	IMAP	566	Request: Message-ID: <4F85FC82.2070708@aol.com>

pav. 14 Filtruojama informacija su prisijungimo duomenimis

Pakeitus filtro nustatymus į *imap and frame contains "frederickflintstone"* aptikome paketą su naudotojo elektroniniu pašto adresu ir vardu, iš kurio buvo siųstas elektroninis laiškas. Paketo numeris: 4475. Rastas vardas „frederick“ ir elektroninis paštas frederickflintstone@aol.com.

No.	Time	Source	Destination	Protocol	Length	Info
1969	53.726789	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
2022	68.928601	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
2054	70.230017	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
2222	71.281443	10.0.2.15	64.12.143.164	IMAP	96	Request: 3 login "frederickflintstone" "1234abcd"
4447	104.966593	10.0.2.15	64.12.143.164	IMAP	566	Request: Message-ID: <4F85FC82.2070708@aol.com>
4475	118.465731	64.12.143.164	10.0.2.15	IMAP/I...	528	from: frederick <frederickflintstone@aol.com>, subject: User Information, (text/plain)

pav. 15 Elektroninio pašto naudotojo vardas ir elektroninis paštas.

Pasinaudojus filtru *imap and frame contains "STATUS"* galima atfiltruoti elektroninio pašto informaciją su elektroninių laiškų kiekiu (pav. 12). Elektroninio pašto juodraščiuose yra 7 laiškai,

išsaugotų laiškų yra 17, parašytų IM žinučių yra 259, išsiųstu žinučių yra 294, šlamšto žinučių yra 5 ir į šiukšliadėžę perkeltų žinučių yra 301.

12a.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

imap and frame contains "STATUS"

No.	Time	Source	Destination	Protocol	Length	Info
2028	69.035016	10.0.2.15	64.12.143.164	IMAP	106	Request: 5 STATUS "Drafts" (UIDNEXT MESSAGES UNSEEN RECENT)
2030	69.057813	64.12.143.164	10.0.2.15	IMAP	137	Response: 5 OK STATUS completed
2032	69.263978	10.0.2.15	64.12.143.164	IMAP	105	Request: 6 STATUS "Saved" (UIDNEXT MESSAGES UNSEEN RECENT)
2034	69.290495	64.12.143.164	10.0.2.15	IMAP	137	Response: 6 OK STATUS completed
2038	69.733048	10.0.2.15	64.12.143.164	IMAP	114	Request: 7 STATUS "Saved/SavedIMs" (UIDNEXT MESSAGES UNSEEN RECENT)
2040	69.777837	64.12.143.164	10.0.2.15	IMAP	147	Response: 7 OK STATUS completed
2044	70.119178	10.0.2.15	64.12.143.164	IMAP	104	Request: 8 STATUS "Sent" (UIDNEXT MESSAGES UNSEEN RECENT)
2046	70.143653	64.12.143.164	10.0.2.15	IMAP	137	Response: 8 OK STATUS completed
2138	70.548649	10.0.2.15	64.12.143.164	IMAP	104	Request: 9 STATUS "Spam" (UIDNEXT MESSAGES UNSEEN RECENT)
2140	70.570888	64.12.143.164	10.0.2.15	IMAP	135	Response: 9 OK STATUS completed
2211	70.934684	10.0.2.15	64.12.143.164	IMAP	106	Request: 10 STATUS "Trash" (UIDNEXT MESSAGES UNSEEN RECENT)
2213	70.958958	64.12.143.164	10.0.2.15	IMAP	139	Response: 10 OK STATUS completed

<

> Frame 2030: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits)
 > Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_8a:d6:9d (08:00:27:8a:d6:9d)
 > Internet Protocol Version 4, Src: 64.12.143.164, Dst: 10.0.2.15
 > Transmission Control Protocol, Src Port: 143, Dst Port: 1695, Seq: 482, Ack: 157, Len: 83
 > Internet Message Access Protocol
 > Line: * STATUS "Drafts" (MESSAGES 0 RECENT 0 UIDNEXT 7 UNSEEN 0)\r\n
 > Line: 5 OK STATUS completed\r\n

pav. 16 Elektroninio pašto laiškų informacija

Išsiaiškinus el. pašto statusą, atfiltravau galimus išsiųstų laiškų paketus. El. laiškų filtras: *imap and contains „Message“*. Atfiltravus paketus yra matoma, kad buvo išsiųstas vienas el. laiškas, kurio paketo numeris yra: 4447 (pav. 17).

12a.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

imap and frame contains "Message"

No.	Time	Source	Destination	Protocol	Length	Info
4447	104.966593	10.0.2.15	64.12.143.164	IMAP	566	Request: Message-ID: <4F85FC82.2070708@aol.com>
4473	118.442541	10.0.2.15	64.12.143.164	IMAP	229	Request: 14 UID fetch 301 (UID RFC822.SIZE FLAGS BODY.PEEK[HEADER.FIELDS (From To Cc Bcc)]
4475	118.465731	64.12.143.164	10.0.2.15	IMAP/I...	528	from: frederick <frederickflintstone@aol.com>, subject: User Information, (text/plain)

pav. 17 Išsiųstas el. laiškas

El. laiško skaitymui galima panaudoti „Follow TCP Stream“ funkcionalumą, pritaikant ant el. laiško paketo (pav. 18). Taip pat pasinaudojau „NetworkMiner“ programa, kuri lengviau leidžia perskaityti išsiųstus laiškus (pav. 19). Rastame turinyje matome, kad laiškas buvo siųstas iš frederickflintstone@aol.com į h138869@rppkn.com. Išsiųsto laiško tema yra: „User Information“, o laiško viduje yra siunčiama prisijungimo informacija.

```

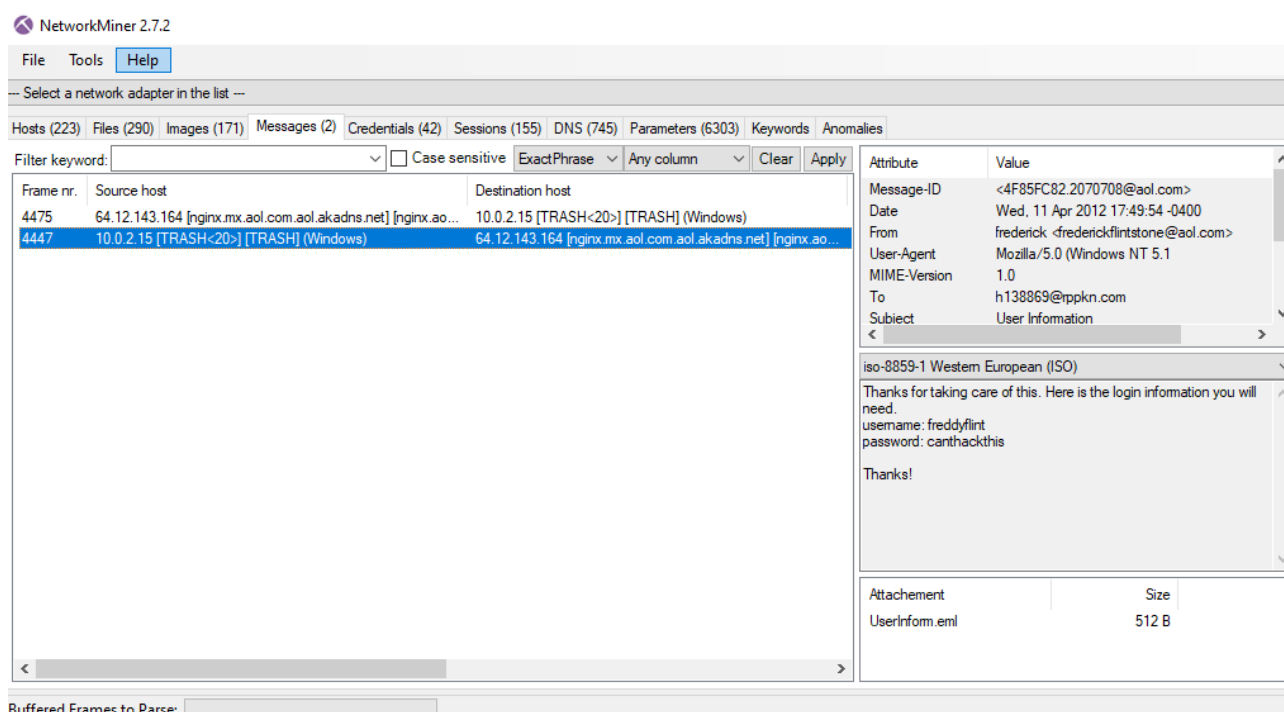
XAOL-GOOD XAOL-GOODCHECK-DONE]] Permanent flags
5 OK [READ-WRITE] SELECT completed
6 getquotaroot "Sent"
* QUOTAROOT "Sent"
6 OK GETQUOTAROOT completed
7 IDLE
+ idling
DONE
7 OK IDLE completed
8 append "Sent" (\Seen) {512+}
Message-ID: <4F85FC82.2070708@aol.com>
Date: Wed, 11 Apr 2012 17:49:54 -0400
From: frederick <frederickflintstone@aol.com>
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20120327 Thunderbird/11.0.1
MIME-Version: 1.0
To: h138869@rppkn.com
Subject: User Information
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

Thanks for taking care of this. Here is the login information you will need.
username: freddyflint
password: canthackthis

Thanks!

```

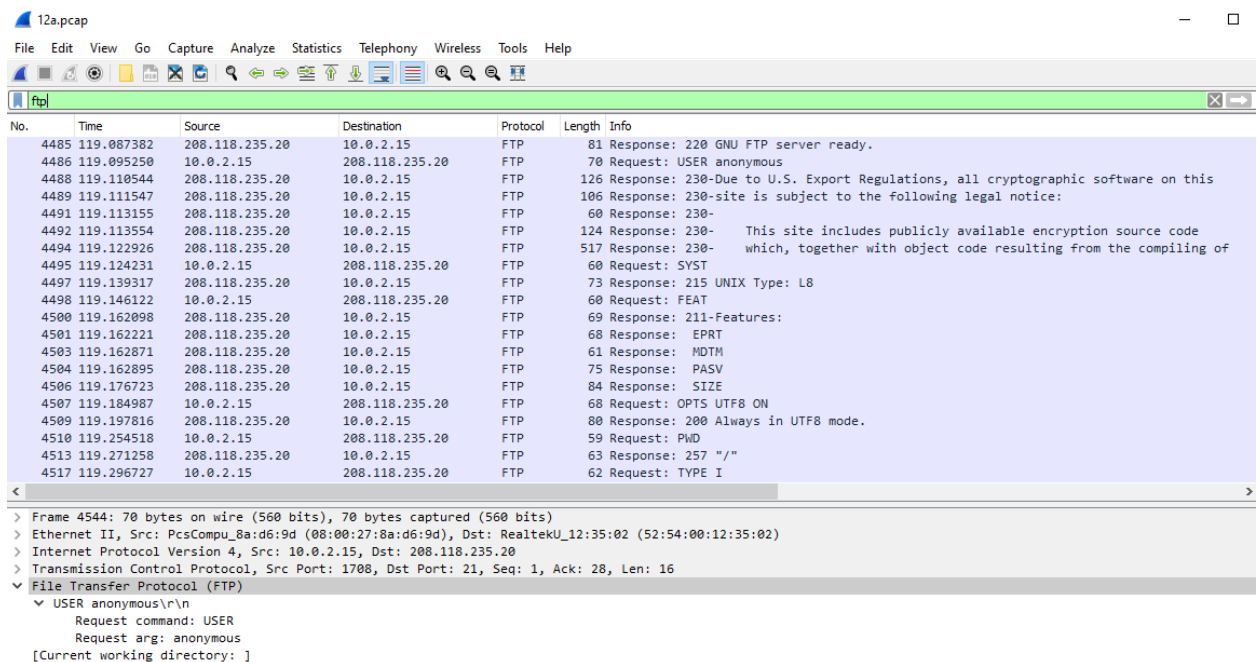
pav. 18 Išsiųsto el. laiško vidus naudojant „Wireshark“



pav. 19 Išsiųsto el. laiško vidus naudojant „NetworkMiner“

2.1. Naudoto serverio analizė

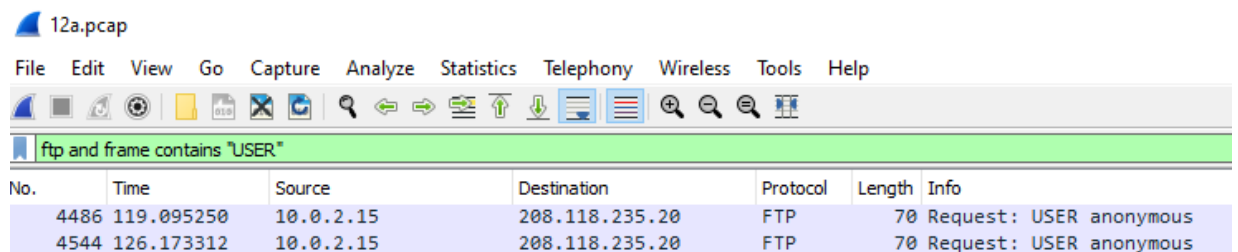
Filtruojant „FTP“ protokolą matome, kad naudotojas naudojosi failo perkėlimą iš serverio (pav. 20). Paketas, kurio numeris: 4486. Šis paketas rodo, kad naudotojas prisijungė kaip anonimas (nežinomas naudotojas).



No.	Time	Source	Destination	Protocol	Length	Info
4485	119.087382	208.118.235.20	10.0.2.15	FTP	81	Response: 220 GNU FTP server ready.
4486	119.095250	10.0.2.15	208.118.235.20	FTP	70	Request: USER anonymous
4488	119.110544	208.118.235.20	10.0.2.15	FTP	126	Response: 230-Due to U.S. Export Regulations, all cryptographic software on this
4489	119.111547	208.118.235.20	10.0.2.15	FTP	106	Response: 230-site is subject to the following legal notice:
4491	119.113155	208.118.235.20	10.0.2.15	FTP	60	Response: 230-
4492	119.113554	208.118.235.20	10.0.2.15	FTP	124	Response: 230- This site includes publicly available encryption source code
4494	119.122926	208.118.235.20	10.0.2.15	FTP	517	Response: 230- which, together with object code resulting from the compiling of
4495	119.124231	10.0.2.15	208.118.235.20	FTP	60	Request: SYST
4497	119.139317	208.118.235.20	10.0.2.15	FTP	73	Response: 215 UNIX Type: L8
4498	119.146122	10.0.2.15	208.118.235.20	FTP	60	Request: FEAT
4500	119.162098	208.118.235.20	10.0.2.15	FTP	69	Response: 211-Features:
4501	119.162221	208.118.235.20	10.0.2.15	FTP	68	Response: EPRT
4503	119.162871	208.118.235.20	10.0.2.15	FTP	61	Response: MDTM
4504	119.162895	208.118.235.20	10.0.2.15	FTP	75	Response: PASV
4506	119.176723	208.118.235.20	10.0.2.15	FTP	84	Response: SIZE
4507	119.184987	10.0.2.15	208.118.235.20	FTP	68	Request: OPTS UTF8 ON
4509	119.197816	208.118.235.20	10.0.2.15	FTP	80	Response: 200 Always in UTF8 mode.
4510	119.254518	10.0.2.15	208.118.235.20	FTP	59	Request: PHD
4513	119.271258	208.118.235.20	10.0.2.15	FTP	63	Response: 257 "/"
4517	119.296727	10.0.2.15	208.118.235.20	FTP	62	Request: TYPE I

pav. 20 „FTP“ protokolo filtras

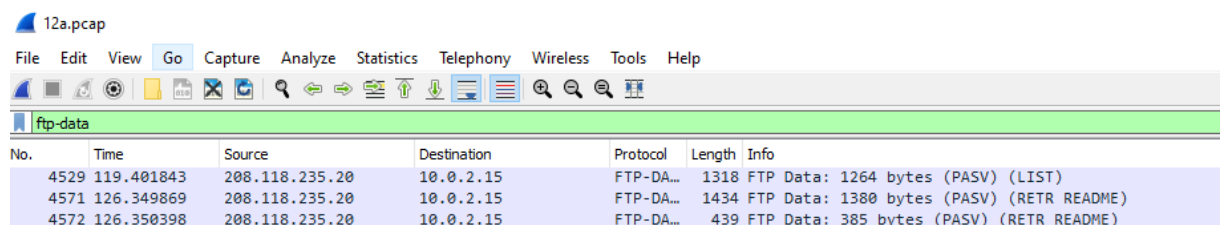
Atfiltravus naudotojo prisijungimo vardą su „FTP“ protokolu galima surasti kiek kartų naudotojas jungėsi prie serverio (pav. 21). Šio atveju naudotojas jungėsi du kartus su „anonymous“ prisijungimu. Serverio adresas į kurį jungėsi yra: 208.118.235.20.



No.	Time	Source	Destination	Protocol	Length	Info
4486	119.095250	10.0.2.15	208.118.235.20	FTP	70	Request: USER anonymous
4544	126.173312	10.0.2.15	208.118.235.20	FTP	70	Request: USER anonymous

pav. 21 „FTP“ protokolo filtras su naudotojo prisijungimu

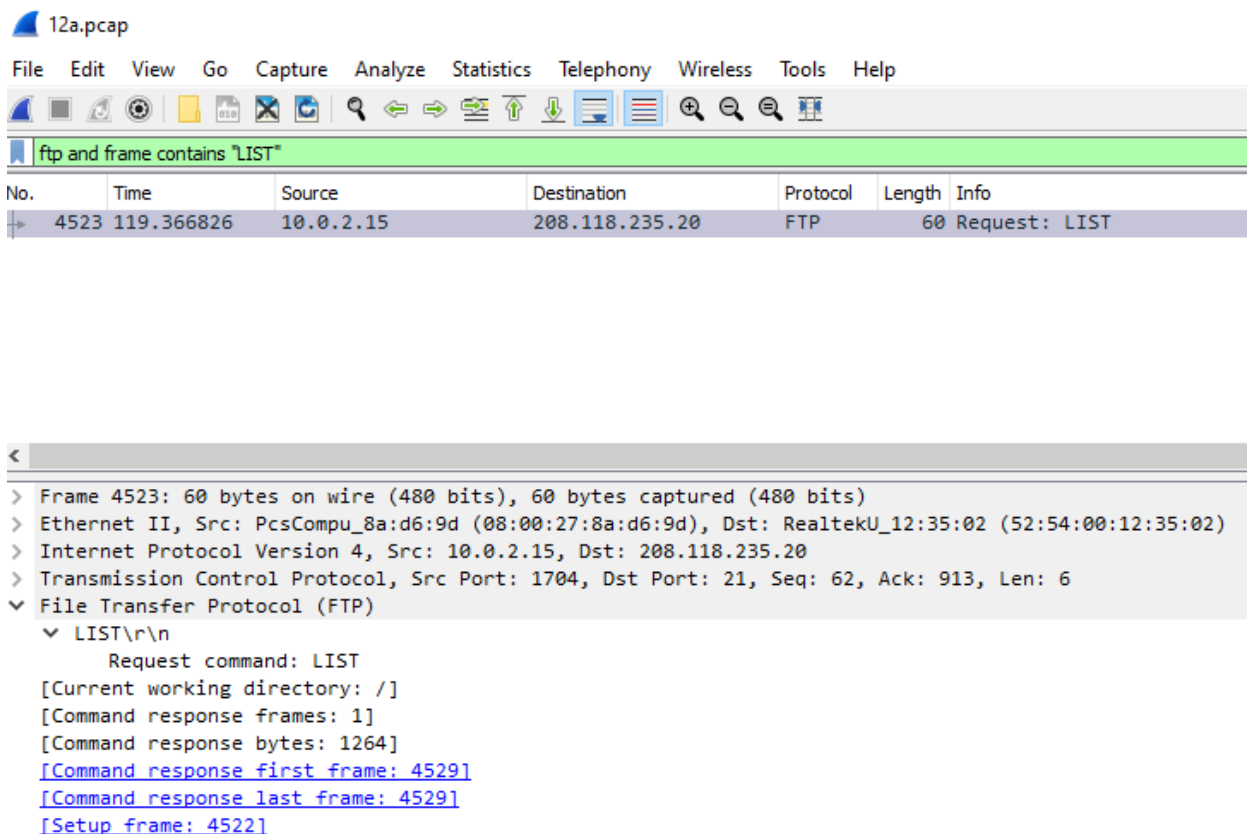
Panaudojus *ftp-data* filtrą yra atfiltruoti trys paketai su duomenimis (pav. 22). Šio filtro pagalba galima surasti naudotus failus, ar terminalo komandos rezultatus.



No.	Time	Source	Destination	Protocol	Length	Info
4529	119.401843	208.118.235.20	10.0.2.15	FTP-DA...	1318	FTP Data: 1264 bytes (PASV) (LIST)
4571	126.349869	208.118.235.20	10.0.2.15	FTP-DA...	1434	FTP Data: 1380 bytes (PASV) (RETR README)
4572	126.350398	208.118.235.20	10.0.2.15	FTP-DA...	439	FTP Data: 385 bytes (PASV) (RETR README)

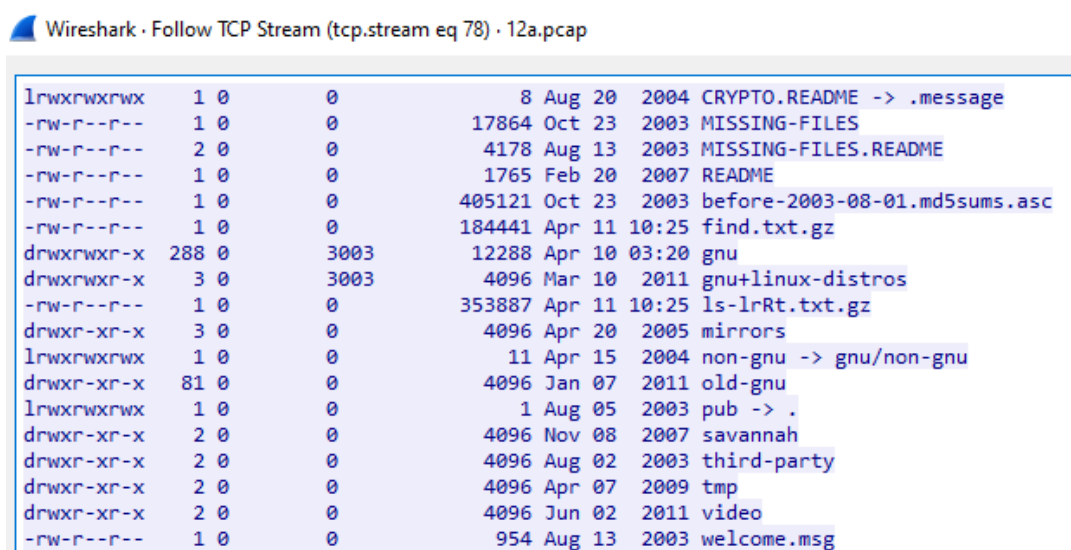
pav. 22 „FTP-DATA“ protokolo filtras

Filtruojant „FTP“ paketus su *ftp and frame contains „LIST“* filtru (pav. 23). Yra matoma, kad „LIST: komanda buvo naudojama tik vieną kartą, kai naudotojas buvo pagrindiniame serverio aplankale.



pav. 23 „LIST“ komandos panaudojimas serveryje

Galime paanalizuoti, kokie rezultatai buvo pateikti panaudojant „list“ komandą. Paveikslėlyje buvo pateiktas paketas su „list“ komandos rezultatu paketu kurį galime išanalizuoti (pav. 22). Peržiūrima 4592 paketo informaciją (pav. 24), pasinaudojus „Follow TCP Stream“ funkciją. Atsidarius „list“ komandos rezultatą matome esančius failus, serverio pagrindiniame aplankale. Pateikta informacija atskleidžia failų pavadinimus ir prieiga prie jų.



pav. 24 „LIST“ komandos rezultatai

Panaudojus „Follow TCP Stream“ komandą ant failo paketo galime atsiversti failą ir pamatyti failo vidų (pav. 25). Šitas failas susidaro iš dviejų paketų.

This is ftp.gnu.org, the FTP server of the the GNU project.

Comments, suggestions, problems and complaints should be reported via email to <gnu@gnu.org>.

gnu/ Contains GNU programs and documents that we develop for the GNU system (or pointers on where to get the programs, if we don't keep the files here). These are programs that fit the definition of GNU software at:
<http://www.gnu.org/philosophy/categories.html#GNUsoftware>

old-gnu/ Older versions of GNU software.

non-gnu/ We distribute some non-GNU programs through our FTP server, or provide pointers to where they are. We put these programs/pointers in this directory since they are not developed by the GNU project. They are, of course, part of the GNU system. See:
<http://www.gnu.org/philosophy/categories.html#TheGNUsystem>

third-party Contains GNU software that has been modified by third parties. We don't necessarily know the specifics of what these modifications do or how these modified versions work. We provide this directory as a service to GNU users who might find these modifications useful.

iso Contains bootable CD images (ISO9660) of a development snapshot of the Debian GNU/Hurd complete operating system.

ls-lrR.txt.gz The output of `ls -lrR` run from this directory. This can be used to see what files are here. This is a gzip'ed version of the file.

There are also .asc files, which contain GPG signatures of the above files, automatically signed by the same script that generates them.

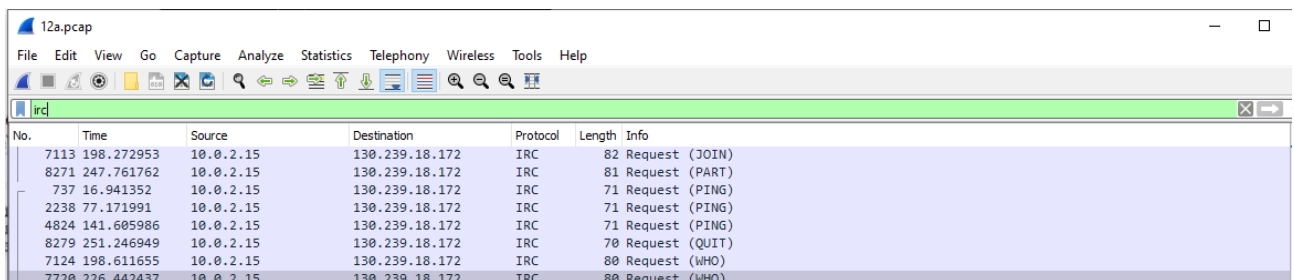
You can verify the signatures for gnu project files with keys from:
<ftp://ftp.gnu.org/gnu/gnu-keyring.gpg>

lpf.README A description of where to find information on the League for Programming Freedom, since this information is not kept here anymore.

pav. 25 README failo vidus

2.1. Pokalbių kambario analizė

Panaudojus *irc* filtrą randame paketus, kurie yra skirti žinučių siuntimui (pav. 26). Matome, kad buvo panaudota ne viena komanda. Pasirinkau analizuoti „WHO“ komandą, kurią panaudojus yra išvedami visi prisijungę prie pokalbio kambario naudotojai.



No.	Time	Source	Destination	Protocol	Length	Info
7113	198.272953	10.0.2.15	130.239.18.172	IRC	82	Request (JOIN)
8271	247.761762	10.0.2.15	130.239.18.172	IRC	81	Request (PART)
737	16.941352	10.0.2.15	130.239.18.172	IRC	71	Request (PING)
2238	77.171991	10.0.2.15	130.239.18.172	IRC	71	Request (PING)
4824	141.605986	10.0.2.15	130.239.18.172	IRC	71	Request (PING)
8279	251.246949	10.0.2.15	130.239.18.172	IRC	70	Request (QUIT)
7124	198.611655	10.0.2.15	130.239.18.172	IRC	80	Request (WHO)
7720	226.442437	10.0.2.15	130.239.18.172	IRC	80	Request (WHO)

pav. 26 „IRC“ protokolo filtras

Pasinaudojus „Follow TCP Stream“ funkciją yra gaunami pasirinkto paketo rezultatai. Pasirikus „WHO“ komandos paketą, galima pamatyti. Kas buvo prisijungę tuo metu prie pokalbio kambario (Pav. 27).

Wireshark - Follow TCP Stream (tcp.stream eq 29) - 12a.pcap

```

WHO #python-unregistered
:leguin.freemote.net 352 frederick_flints #python-unregistered ~frederick 128.238.64.31 leguin.freemote.net frederick_flints H :0 frederick_flintstone
:leguin.freemote.net 352 frederick_flints #python-unregistered ~wa 50.45.207.133 wright.freemote.net wa H :0 ~
:leguin.freemote.net 352 frederick_flints #python-unregistered 45e4ab28 gateway/web/freemote/ip.69.228.171.40 rowling.freemote.net _mineral H :0 69.228.171.40 - http://webchat.freemote.net
:leguin.freemote.net 352 frederick_flints #python-unregistered ~Joachim cm-84.210.106.182.getinternet.no adams.freemote.net Joachim H :0 Joachim
:leguin.freemote.net 352 frederick_flints #python-unregistered ~enmand sydnns8109w-099192038023.dhcp-dynamic.FibreOp.ns.bellalliant.net adams.freemote.net enmand H :0 Daniel Enman
:leguin.freemote.net 352 frederick_flints #python-unregistered ~adum 8x5da3b8b5.cpe.ge-1-1-0-1104.oelnuq1.customer.tele.dk verne.freemote.net jantzen05 H :0 Adium User
:leguin.freemote.net 352 frederick_flints #python-unregistered ~andrejpan tesla.chaoflow.net adams.freemote.net andrejpan H :0 andrejpan
:leguin.freemote.net 352 frederick_flints #python-unregistered ~jpuderer 69-165-165-142.dsl.teksavvy.com card.freemote.net jpuderer_ H :0 James Puderer
:leguin.freemote.net 352 frederick_flints #python-unregistered ~juliohm unaffiliated/juliohm adams.freemote.net juliohm H :0 J.llo Hoffmann Mendes
:leguin.freemote.net 352 frederick_flints #python-unregistered ~textual 173-30-31-241.client.mchsi.com zelazny.freemote.net lyddonb H :0 Textual User
:leguin.freemote.net 352 frederick_flints #python-unregistered ~zacharypc c-69-143-215-162.hsd1.dc.comcast.net adams.freemote.net zacharypc H :0 zakp
:leguin.freemote.net 352 frederick_flints #python-unregistered ~andrew 69.31.123.122.holmes.freemote.net andrewwatts H :0 Andrew Watts
:leguin.freemote.net 352 frederick_flints #python-unregistered ~necavi c-67-180-112-130.hsd1.ca.comcast.net cameron.freemote.net necavi H :0 necavi_nocui
:leguin.freemote.net 352 frederick_flints #python-unregistered ~ichdertom p5C774A0.dip.t-dialin.net holmes.freemote.net ichdertom H :0 Thomas Kagerer
:leguin.freemote.net 352 frederick_flints #python-unregistered ~parham pool-74-96-96-110.washdc.fios.verizon.net asimov.freemote.net Goopyo H :0 Parham
:leguin.freemote.net 352 frederick_flints #python-unregistered ~mgeneral pool-71-186-174-82.bflony.east.verizon.net adams.freemote.net mgeneral H :0 Matthew General
:leguin.freemote.net 352 frederick_flints #python-unregistered ~Jonbo123 97.67.110.15 adams.freemote.net Jonbo H :0 Jonbo
:leguin.freemote.net 352 frederick_flints #python-unregistered ~tkiddle cpc4-hari15-2-0-cust505.20-2.cable.virginmedia.com adams.freemote.net tkiddle H :0 New Now Know How
:leguin.freemote.net 352 frederick_flints #python-unregistered ~Grimmur vr2t-dw014.rhi.hi.is moorcock.freemote.net Grimmer H :0 Anonymous User
:leguin.freemote.net 352 frederick_flints #python-unregistered ~yassine unaffiliated/yassine asimov.freemote.net yassine H :0 Yassine Elasad
:leguin.freemote.net 352 frederick_flints #python-unregistered ~daniel HSI-KBW-078-043-203-037.hsi4.kabel-badenwerttemberg.de wright.freemote.net schlaftier H :0 Computational Linguist
:leguin.freemote.net 352 frederick_flints #python-unregistered ~marcink unaffiliated/marcinkuzminski adams.freemote.net marcinkuzminski H :0 Marcin Kuzminski
:leguin.freemote.net 352 frederick_flints #python-unregistered ~machine4 pool-74-111-197-200.lsanca.fios.verizon.net wright.freemote.net machine2 H :0 machine2
:leguin.freemote.net 352 frederick_flints #python-unregistered ~akosch catv-80-99-193-104.catv.broadband.hu wright.freemote.net akosch H :0 akosch
:leguin.freemote.net 352 frederick_flints #python-unregistered ~starenka ip-62-245-81-157.net.upcbroadband.cz adams.freemote.net starenka H :0 starenka
:leguin.freemote.net 352 frederick_flints #python-unregistered ~dagnachew 70.48.137.170.wolfe.freemote.net dagnachew H :0 dagnachew
:leguin.freemote.net 352 frederick_flints #python-unregistered ~brian 188-220-10-235.zone11.bethere.co.uk pratchett.freemote.net BrianE H :0 Brian
:leguin.freemote.net 352 frederick_flints #python-unregistered ~sivy ip98-167-222-209.ph.ph.cox.net asimov.freemote.net sivy H :0 sivy
:leguin.freemote.net 352 frederick_flints #python-unregistered ~rob nat-out.akwd1-gw.webhost.co.nz calvino.freemote.net shiver H :0 rob
:leguin.freemote.net 352 frederick_flints #python-unregistered ~lukegb static.230.106.9.176.clients.your-server.de adams.freemote.net lukegb H :0 lukegb
:leguin.freemote.net 352 frederick_flints #python-unregistered ~ryan c-71-197-153-41.hsd1.wa.comcast.net leguin.freemote.net rhoenges H :0 Ryan Doenges
:leguin.freemote.net 352 frederick_flints #python-unregistered ~u214 pdpc/supporter/professional/magn3ts lindholm.freemote.net magn3ts H :0 magn3ts
:leguin.freemote.net 352 frederick_flints #python-unregistered ~quassel unaffiliated/mrpps adams.freemote.net MrPPS G :0 MrPPS
:leguin.freemote.net 352 frederick_flints #python-unregistered ~PhilK 50-56-190-233.static.cloud-ips.com card.freemote.net PhilK H :0 Phil Kates
:leguin.freemote.net 352 frederick_flints #python-unregistered ~lux ppp-236-182-25-151.libero.it adams.freemote.net lux H :0 lux
:leguin.freemote.net 352 frederick_flints #python-unregistered ~kvirc p4CFDF09.dip.t-dialin.net kornbluth.freemote.net rref H :0 KVirc 4.1.1 Equilibrium http://kvirc.net/
:leguin.freemote.net 352 frederick_flints #python-unregistered ~tonyorac1 115.246.190.179 asimov.freemote.net tonyoracle H :0 ...
:leguin.freemote.net 352 frederick_flints #python-unregistered ~scorchsab python/site-packages/ssbr card.freemote.net ssbr_ H :0 Devin Jeanpierre
:leguin.freemote.net 352 frederick_flints #python-unregistered ~Hussein 93-96-200-255.zone4.bethere.co.uk adams.freemote.net ElGoof H :0 Hussein
:leguin.freemote.net 352 frederick_flints #python-unregistered ~treyka 85.234.199.185 niven.freemote.net treyka H :0 treyka
:leguin.freemote.net 352 frederick_flints #python-unregistered ~textual lCaen-156-54-32-101.w80-11.abo.wanadoo.fr zelazny.freemote.net craigkerstiens H :0 Textual User
:leguin.freemote.net 352 frederick_flints #python-unregistered ~cdh473 h43.114.40.69.dynamic.ip.windstream.net moorcock.freemote.net cdh473 H :0 cdh473
:leguin.freemote.net 352 frederick_flints #python-unregistered ~joe dynamic-adsl-94-37-167-39.clienti.tiscali.it calvino.freemote.net joe_oblivian H :0 Joe
:leguin.freemote.net 352 frederick_flints #python-unregistered ~x unaffiliated/jrua niven.freemote.net jrua H :0 x
:leguin.freemote.net 352 frederick_flints #python-unregistered ~mhooker 50-0-80-160.dsl.static.sonic.net niven.freemote.net mhooker H :0 Matthew Hooker

```

Pav. 27 „WHO“ komandos rezultatai

2.1. Užkuoduotų paketų analizė

Pritaikius *ts/* filtrą pavyko atfiltruoti 29 paketus. Atfiltravus paketus buvo surasti trys du IP adresai, kurie gražino aplikacijos duomenis (pav. 28). Kadangi duomenys yra užšifruoti, bandysime bent jau surasti kur naudotojas kreipėsi.

12a.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1991	53.880244	10.0.2.15	63.245.221.11	TLSv1	454	Application Data
2000	53.951262	63.245.221.11	10.0.2.15	TLSv1	943	Application Data
4415	104.298503	64.12.175.136	10.0.2.15	TLSv1	283	Application Data

pav. 28 „TLS“ paketų filtravimo daliniai rezultatai

Pasirinkus antrąjį paketą numeriu: 2000, galime atsekti kur naudotojas kreipėsi kai gavo šį paketą. Pasinaudojus „Follow TCP Stream“, buvo galima atsekti į kokį puslapį naudotojas kreipėsi (pav. 29). Sekant pavyko aptikti puslapį kuriame naudotojas lankėsi. Surastas puslapis yra: <http://live.mozillamessaging.com>.

12a.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 69

No.	Time	Source	Destination	Protocol	Length	Info
1968	53.709023	10.0.2.15	63.245.221.11	TCP	54	1694 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1978	53.800796	10.0.2.15	63.245.221.11	TCP	54	1694 → 443 [ACK] Seq=179 Ack=2293 Win=64240 Len=0
2003	54.066138	10.0.2.15	63.245.221.11	TCP	54	1694 → 443 [ACK] Seq=893 Ack=3229 Win=63304 Len=0
2370	83.958785	10.0.2.15	63.245.221.11	TCP	54	1694 → 443 [ACK] Seq=893 Ack=3257 Win=63277 Len=0
2371	83.960066	10.0.2.15	63.245.221.11	TCP	54	1694 → 443 [FIN, ACK] Seq=893 Ack=3257 Win=63277 Len=0
1962	53.636538	10.0.2.15	63.245.221.11	TCP	62	1694 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1972	53.727736	63.245.221.11	10.0.2.15	TCP	60	443 → 1694 [ACK] Seq=1 Ack=179 Win=65535 Len=0
1981	53.805206	63.245.221.11	10.0.2.15	TCP	60	443 → 1694 [ACK] Seq=2293 Ack=493 Win=65535 Len=0
1992	53.881279	63.245.221.11	10.0.2.15	TCP	60	443 → 1694 [ACK] Seq=2340 Ack=893 Win=65535 Len=0
2372	83.962307	63.245.221.11	10.0.2.15	TCP	60	443 → 1694 [ACK] Seq=3257 Ack=894 Win=65535 Len=0
2369	83.958745	63.245.221.11	10.0.2.15	TCP	60	443 → 1694 [FIN, ACK] Seq=3256 Ack=893 Win=65535 Len=0
1967	53.708936	63.245.221.11	10.0.2.15	TCP	60	443 → 1694 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1991	53.880244	10.0.2.15	63.245.221.11	TLSv1	454	Application Data
2000	53.951262	63.245.221.11	10.0.2.15	TLSv1	943	Application Data
1977	53.800759	63.245.221.11	10.0.2.15	TLSv1	966	Certificate, Server Hello Done
1990	53.879652	63.245.221.11	10.0.2.15	TLSv1	101	Change Cipher Spec, Encrypted Handshake Message
1970	53.727364	10.0.2.15	63.245.221.11	TLSv1	232	Client Hello
1980	53.804240	10.0.2.15	63.245.221.11	TLSv1	368	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2368	83.958699	63.245.221.11	10.0.2.15	TLSv1	81	Encrypted Alert
1976	53.800106	63.245.221.11	10.0.2.15	TLSv1	1434	Server Hello

Type: server_name (0)
Length: 30

Server Name Indication extension
Server Name list length: 28
Server Name Type: host_name (0)
Server Name length: 25
Server Name: live.mozillamessaging.com

pav. 29 Paketo sekimo rezultatas

Pasirinkus paketą kurio numeris yra: 4415, galime sekti kaip sekėme ir praėjusi paketą. Sekant paketą buvo aptiktas serveris į kurį kreipėsi naudotojas (pav. 30). Serverio pavadinimas: smtp.aol.com.

12a.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 75

No.	Time	Source	Destination	Protocol	Length	Info
4415	104.298503	64.12.175.136	10.0.2.15	TLSv1	283	Application Data
4418	104.370768	64.12.175.136	10.0.2.15	TLSv1	123	Application Data
4422	104.401025	64.12.175.136	10.0.2.15	TLSv1	107	Application Data
4425	104.587451	64.12.175.136	10.0.2.15	TLSv1	107	Application Data
4428	104.613685	64.12.175.136	10.0.2.15	TLSv1	123	Application Data
4433	104.857709	64.12.175.136	10.0.2.15	TLSv1	123	Application Data
4436	104.891599	64.12.175.136	10.0.2.15	TLSv1	107	Application Data
4413	104.273596	10.0.2.15	64.12.175.136	TLSv1	144	Application Data, Application Data
4416	104.332407	10.0.2.15	64.12.175.136	TLSv1	176	Application Data, Application Data
4419	104.373257	10.0.2.15	64.12.175.136	TLSv1	176	Application Data, Application Data
4423	104.401628	10.0.2.15	64.12.175.136	TLSv1	160	Application Data, Application Data
4426	104.590229	10.0.2.15	64.12.175.136	TLSv1	128	Application Data, Application Data
4429	104.620758	10.0.2.15	64.12.175.136	TLSv1	640	Application Data, Application Data
4430	104.621478	10.0.2.15	64.12.175.136	TLSv1	128	Application Data, Application Data
4434	104.863044	10.0.2.15	64.12.175.136	TLSv1	128	Application Data, Application Data
4387	103.910284	10.0.2.15	64.12.175.136	SMTP	72	C: EHLO [10.0.2.15]
4390	103.942737	10.0.2.15	64.12.175.136	SMTP	64	C: STARTTLS
4398	104.078983	64.12.175.136	10.0.2.15	TLSv1	644	Certificate, Server Key Exchange, Server Hello Done
4401	104.141012	64.12.175.136	10.0.2.15	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
4393	103.976233	10.0.2.15	64.12.175.136	TLSv1	219	Client Hello
4399	104.100180	10.0.2.15	64.12.175.136	TLSv1	352	Client Key Exchange, Change Cipher Spec, Encrypted

Extensions Length: 43

Extension: server_name (len=17)
Type: server_name (0)
Length: 17

Server Name Indication extension
Server Name list length: 15
Server Name Type: host_name (0)
Server Name length: 12
Server Name: smtp.aol.com

pav. 30 Paketo sekimo rezultatas

3. Išvados

Darbo metu atliktas srauto tyrimas. Buvo išsiaiškinta, jog naudotojas naudotojo Windows XP operacinę sistemą bei naudojo Safari naršyklę ir Thunderbird 11.0.1 el. pašto klientą. Atlikus interneto srauto filtravimą buvo atrasta, kad naudotojas lankėsi google.com puslapyje iš kurio ėjo du kartus į wikipedia.org puslapį. Taip pat pavyko aptikti su „FTP“ protokolu susijusį failą, kurio turinys buvo peržiūrėtas naudojant „Follow TCP Stream“ funkciją. Išanalizavus „IRC“ protokolą pavyko aptikti, kad naudotojas naudojosi pokalbių kambariu, kuriame panaudojo komandas, kaip „WHO“. Atkurti pranešimą pavyko tik vieną, kitų pranešimų atkurti nepavyko, kadangi jie buvo užšifruoti. Iš užšifruoto srauto pavyko aptikti aplankytą adresą. Puslapių analizės metu, nepavyko aptikti užpildytu formų informacijos. Atlikus analizę buvo išanalizuota ir aptikta, daugiau duomenų negu tikėtasi. Buvo pagilintos žinios naudojantis filtrais.