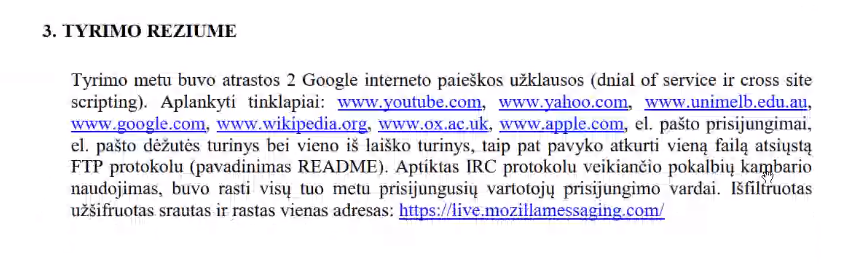
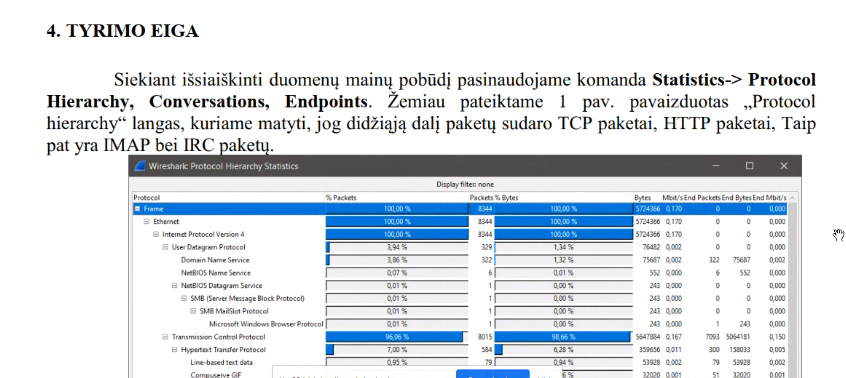
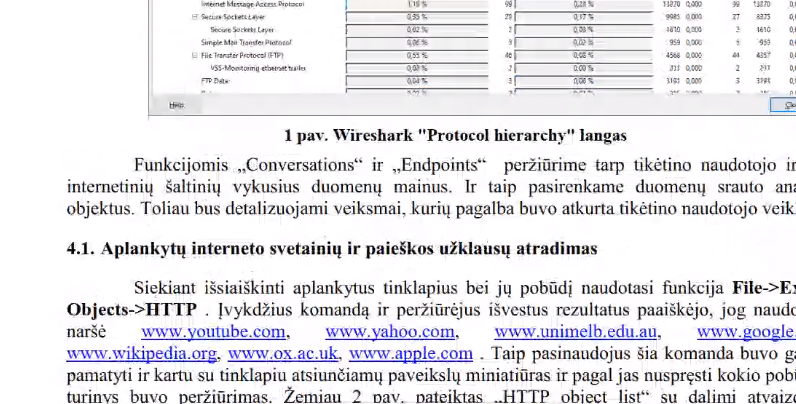


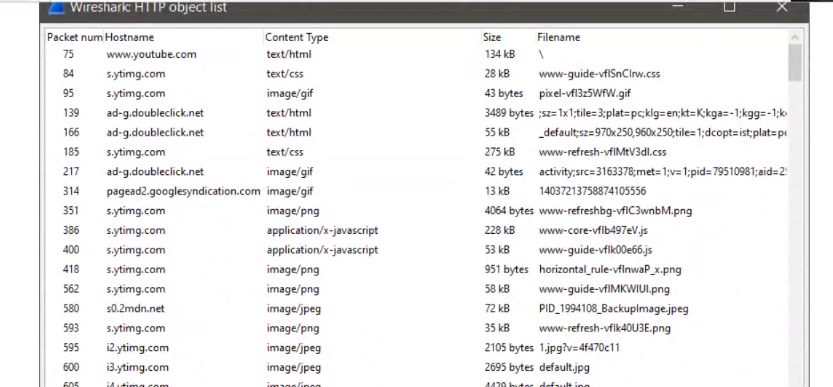
1.1. Ataskaitoje pateikti 
I. Varianto nr, jraöo dat4 ir laik4, trukmg. 
2. Tikétino esminio vartotojo , MAC adresus, OS, naudotas klientines programas. 
3. Tyrimo reziume (trumpai a Syti srauto tyrimo rezultatus). 
4. Tyrimo apragymq. Tyrimo seka (praleid>iant nerezultatyvius veiksmus), nurodant raktiniq kadrq 
numerius, filtrus ir iliustruojant ekrano kopijomis, taip kad skaitantysis galétu atkartoti rezultatyvius 
tyrimo veiksmus. 
5. Kvados (pateikti savo nuomonq apie rezultatu pilnumq, dar pastebéjote, bet nepilnai 
Äsiaiüinote). 
6. Priedai. Pateikti i"ifruotus dokumentus, u}pildyttl formu ar laiSkq turini. 
1.2. Varianto numeris, data ir laikas, trukmé 
Varianto numeris: 12a 
JraQ) data ir laikas: 2012-04-12 00:48: 15 
Iraso trukmé: 269,755436 

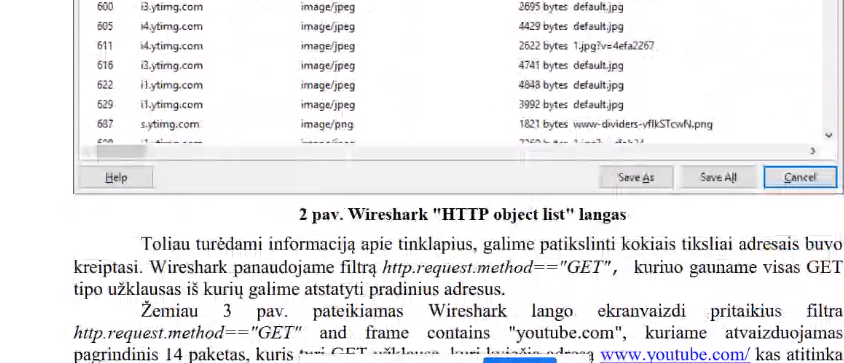
2. TIKÉTINO ESMINIO VARTOTOJO IP, MAC ADRESAI, OS, NAUDOTOS 
KLIENTINÉS PROGRAMOS 
Tikétino naudotojo IP adresas: 10.0.2.15 
Tikétino naudotojo MAC adresas: 
Tikétino naudotojo naudojama operaciné sistema: Windows XP 
Tikétino naudotojo naudotos klientinés programos: interneto narWklé Safari, el. paSt0 
klientas Thunderbird 11.0. I 

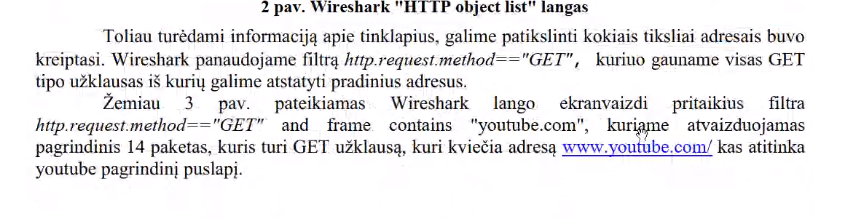


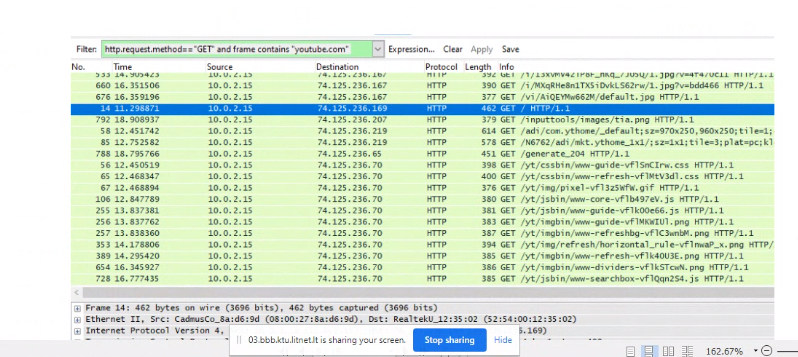




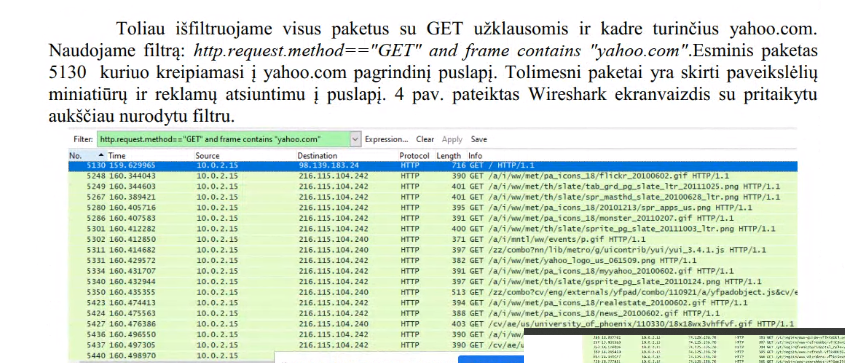




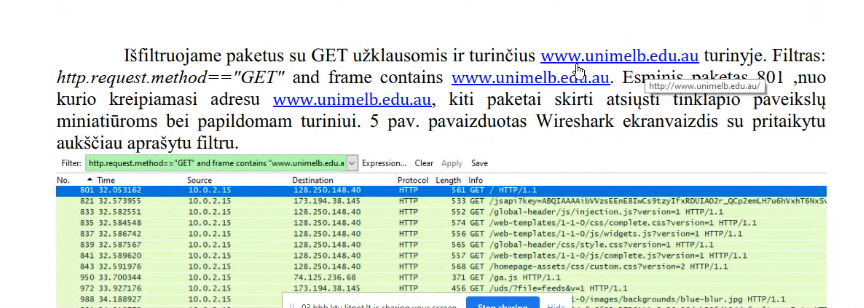


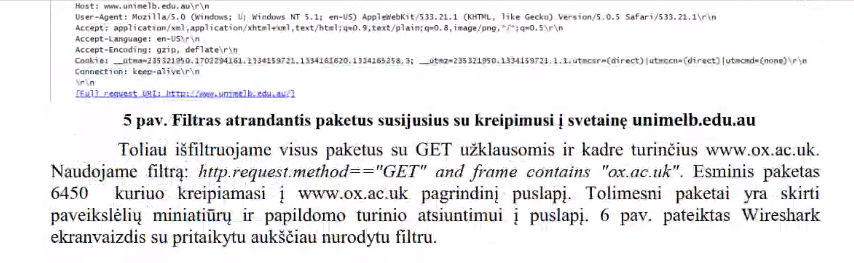


10.0... us 
in.n.2.i5 
20.0. 
N. 70 
236. 
byte 009' 
GET 
BS GET 
"6 GET 
GET 
Sec: 
00.0,2.15J. u.1_25.2J6.16• 
GET 
a,5.o 5. L: G«kaj 
3 pava Filtras atrandantis paketus susijusius Su kreipimusi i svetainq youtube.com 
Toliau ißfiltruojame visus paketus su GET u2klausomis ir kadre turinöius yahoo.com. 



Machine generated alternative text:
'424 
•sa GET 
a". 0.2. IS 
Ito. a'S' '-o 
is an 
4 pav. Filtras atrandantis paketus susijusius su kreipimusi i svetainq yahoo.com 





9 pav. Filtras atrandantis paketus susijusius su kreipimusi i svetainç apple.com 
4.2. El. pasto prisijungimq bei turinio atradimas 
Toliau buvo ieSkoma paketu susijusiu su elektroniniu pastu. Pritaikius filtra imap and frame 
contains "login"buvo rasta prisijungimo prie el. pa<to informacija (10 pav.). Esminiai paketai: 1969, 
2022, 2054, 2222. Prisijungimo vardas prie el. pasto kliento yra: „frederickflinstone", slapta>odis 
„1234abcd". Taip pat atkurto el. lai<ko (Zr. 
frederickflinstone@aol.com 
F itter: imap and frame contains • Ioyin• 
1 priede) pavyko atkurti, jog naudotojo el pa<tas yra: 
Apply Save 
2022 
2054 
2222 
68. 928601 
70.230017 
71.281443 
10. o. 2.15 
10.0.2.15 
10.0.2.15 
Dest i naticn 
64.12.143.164 
64.12.143.164 
64.12.143.164 
64.12.143.164 
P rotOCOl Info 
9 Requet: 
96 Request: 
96 Request. 
3 1 Ogin 
3 login 
"frederickflintstone" 
"frederickflintstone- "1234abcd 
10 pav. Filtras atrandantis el. pasto prisijungimo duomenis 
Pasinaudojus filtru imap and frame contains "STATUS" randame 
"1234abcd" 
elektroninio pasto 
kataloguose saugomu lai<ku kiek) (II pav.). Esminiai paketai: 2030, 2034, 2040, 2046, 2140, 2213. 

frederickflinstone@aol.com 
Filter: imap and frame contains • login• 
1969 s 3.726789 
2022 
68.928601 
2054 
70.2 30017 
2222 
71.281443 
10. o. 2.15 
10. o. 2.15 
10.0.2.15 
10.0.2.15 
64.12. 143.164 
64.12.143.164 
64.12.143.164 
64.12.143.164 
Clear Apply Save 
P rot OCOI Info 
96 Requet: login 
3 login 
96 R«west: 
96 Request 3 login 
96 Request. 
10 pav. Filtras atrandantis el. pa;to prisijungimo duomenis 
Pasinaudojus filtru imap and frame contains "STATUS" randame 
"frederi 
"1234abcd" 
-1234abcd" 
"frederickflintstone- -1234abcd" 
elektroninio 
kataloguose saugonuæ laiüu kieki (Il pav.). Esminiai paketai: 2030, 2034, 2040, 2046, 2140, 2213. 
Buvo nustatyta, jog 7 laßkai saugomi drafts kataloge, 17 laßkq saugoma saved messages, taip pat 

paragytos 259 1M Zinutés, 294 i*siqsti laiüai, 5 laßle,ii 
yra spam kataloge ir 301 lai"as perkeltas j 
ST*Tt'S ÉCtST) 
• STATUS 
69.0S78n 
69.2.04" 
69-7330." 
69."7837 
2140 70.5708" 
137 
CuessåG_s o o 7 O) 
6-4. 
• STATUS 
'0.0. 2. 15 
11 pav. Filtras atrandantis el. paQo déiutéje saugolnl! laikku kiekius 
Norint atvaizduoti atrastu el. laiSku tunni pritaikome filtrq: imap and frame 
"Message". Esminis paketas 4447 (12 pav.). 
contains 

11 pav. Filtras atrandantis el. pa{to déiutéje saugomu laßkq kiekius kataloguose 
Norint atvaizduoti atrastu el. laiSku turini pritaikome filtrq: imap and frame contains 
"Message". Esminis paketas 4447 (12 pav.). 
ength Into 
12 pav. Filtras atrandantis naudotojo el. paqo iinutes 
Detaliau laiÅko turinj randame pasinaud0Jus jrankiu ,„Network miner". Korteléje 
„Conversations" randame naudotojo siust4 laiÅkq su prisijungimo informacija. Kaip matome 13 pav. 
siuntéjo adresas yra frederickflinstone@aol.com, gavéjas yra h138869@rppkn.com , laiüo tema: 
„User Information". 
1 

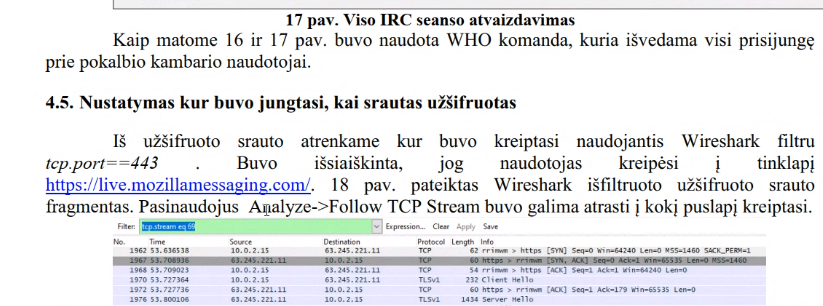
'00215 
a•47S 
NT 1 
257 
13 pav. Network miner langas su Nsiqsto la"ko turiniu 
4.3. FTP protokolu atsiqstu failu atradimas 
Sioje dalyje apraSoma ftp pakettl analize. Pirmiausia bandoma s 
prrsljun 
informacij4. Naudojarnas filtras ftp and frame contains "USER". Esminis pake as 4486. Kai 
matome 14 pav., naudojamas anoniminis prisijungimas, o serverio adresas prie kurio jungiamasi 
208.118.235.20. 
Filter: ftp and frame contains • USER" 
Source 
Destination 
v Clear Apply 
Protocol Length Info 

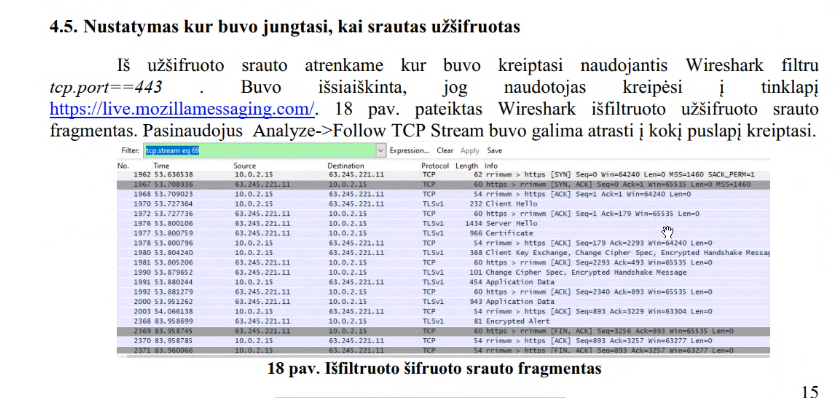
Parsiunéiamas failas Nskaidytas i tris paketus. Pilnq README 
NetworkMiner. Korteléie „Files" surandame README fai14pgr±iürime jc 
4529 119.401843 
4571 349869 
4572 126.350393 
208.118. 235 . 
208.118.25.20 
Expression. , 
DestinAtion 
10.0.2.15 
o. 2.15 
15 pav- Filtras FTP protokoku siunéiamy fail" turiniu 
4.4. Veiksmai IRC protokolu veikianéiame pokalbiq kambaryje 

Parsiunéiamas failas ßskaidytas i tris paketus. Pilnq README failq gauname naudojantis 
NetworkMiner. „Files" surandame README fail Füiürime jo turinj (tr. ?7priede). 
Filter. 
4529 119.401843 
4571 126. 149869 
208.118.235.20 
208.118. us. 20 
208.11*.235.20 
Destination 
10.0.2.15 
10.0.2-15 
u.o.z.15 
v Clear Sove 
protocol Length Info 
FTP-OAT: FTP Data: bytes 
1434 FTP Data: 1380 bytes 
449 FTP 385 bytes 
15 pav. Filtras FTP protokoku siunéiamt! fail" turiniui rasti 
4.4. Veiksmai IRC protokolu veikiandiame pokalbiq kambaryje 
Pritaike Wireshark filtrq irc randame paketus skirtus iinuéiu siuntimui IRC protokolu. 16 
pav. vaizduojami iSfiltruoti IRC aketai. 

Follow 
Stream C 
PING 
; 1 eouin.fre 
PING 133418 
l: leguin. fre 
PINC 
: leguin. 
JOIN *pytho 
:frederick_ 
: leguin. fre 
been 
"We inform 
eguin. fre 
: leguin.fre 
chdertom 
akosch 

—koşch 'tarenkez BrianE şivy siliver lükeqb rhdoenqes 
rnnyc.racle sğbr_ treyka cdh473 joe_obijv 
net 3?) frederick_fJint5 z ğpython—ünrewst 
petter•hj m•4i7h TopRamen men t4bz kjellskl skrite joar 
XheSh•qg Conradknight50ck •orrr_ proton_ andreypopp 
(y rüşe "10 
: leguın,freenode.nez 353 
iri Yon crazydiamond jack%boo forbyN. Inqel• 'i rrqre•y 
]jcrza üuffer alshain rageous 
Çoxbor•on Idiannnd Cakh qzl joepie9L yb•it kanzure 
]janur2 sunzup estel*5tec r 
: i 353 Şrederşck_flinğs 'pythnn—unreoist 
gtr-ak schn•odIe5 abchirk_ abchırk_ rothant 
karavanjok Pİ )ackBeePee Kuukunen kj•cka bdhuser 
n2dğy fovoler • Tsha'n_ crescendo •eor BicnrD_ 
RoozterJuice Rafusek joepa I i mn_d.•• 
tez 
: 1 353 Frederick_flints • •gython-unre9is 
ISupreme— mai ack%on cqtdk Yr-haz Aragon chendo_ GGSE akujın Muzer 
fOO 
Matrixium 5erqSerçıu 
: leçuın, freenode.ner 3" tvvthon-unreqıstered 
ardon "ibate '3v3 yandhi jee_ pior di 
ing Prpçster sataker44 yumaob.•o rayyne B ueLaquna 





5. IŠVADOS 
Darbo metu atliktas srauto tyrimas. Išsiaiškinta,jog naudotojo darbinëje stotyje naudojama 
operacinë sistema yra Windows XP bei naudojama internâ naršyklë Safari ir el. pašto klientas 
Thunderbird 11.0.1. Atlikus srauto analizę buvo atrastos 2 užklausos Google ir aplankyti du 
Wikipedia straipsniai, susiję su paieškos kriterijais. Analizës metu pavyko atkurti vieną naudotojo 
siqstą elektronini laišką, kuriame buvo siunčiama prłsijungimo infOrmacija. Taip pat, pavyko atkurti 
vieną naudotojo FTP protokolu atsisiqstą failą ir jo turinj. Buvo aptikta, jog naudotojas naudojosi 
IRC protokolu paremtu pokalbiq kambariu, tačiau nepavyko atkurti tikslaus pokalbio. Iš užšifruoto 
srauto pavyko iŠgauti vieną aplankytą adresą. Analizës metu nepavyko nustatyti užpildytq formq 
duomemł bei rasti užsakymL1 bei ju informacijos. 