Лабораторија за дигиталну форензику
Факултет техничких наука

Фрушкогорска 1
21102 Нови Сад

17.6.2023.

Невена Атић

Тополска 18, 11000 Београд

ОПИС СЛУЧАЈА

Дана 1. 3. 2023. године, ангажовани смо од стране Богољуба Гагића из Београда, директора фирме „Мања транс“, да извршимо вештачење и сачинимо налаз и мишљење за случај тешког кривичног дела које обухвата шверц дроге. Недозвољене супстанце су заплењене у транспортном камиону регистарских ознака BG584XX, који припада фирми на чијем се челу налази Гагић. Фирма се изворно бави шпедицијом и транспортом робе и Богољуб Гагић тврди да лично није повезан са недозвољеним активностима, као и да је превоз дроге подметнут у сарадњи са неким од запослених.

Задатак вештачења је да прегледамо и анализирамо електронску опрему која укључује следеће уређаје:

− Десктоп рачунар произвођача Acer, модела Aspire E1-571 и серијског броја 589-87VQW389FSF-3FG преузет од директора Богољуба Гагића.

− Десктоп рачунар произвођача HP, модела Pavilion G6 и серијског броја HP98-556FRWQ98DFL-258F преузет од запослене Душанке Свиларевић.

− Десктоп рачунар произвођача Toshiba, модела Satellite Pro L450 и серијског броја 897526 преузет од запосленог Павла Пандуровића.

− USB флеш меморија произвођача SanDisk, модела Cruser Force и серијског броја 0xd585e28 преузета од запосленог Павла Пандуровића.

− Мобилни телефон произвођача Google, модел Pixel 5 и серијског броја EMULATOR32X1X11X0 преузет од запослене Душанке Свиларевић.

као и мрежни саобраћај уређаја настао у периоду од 23.2.2023. до 26.2.2023. године (access.log) и снимке надзорних камера (snimak_nadzorne_kamere_1.mp4 и snimak_nadzorne_kamere_2.mp4) без знања запослених. Сходно томе, у циљу разрешења случаја:

1. утврдити да ли је злонамерни запослени могао да дође до креденцијала за приступ веб сервису за вођење евиденције о поласцима камиона, да ли су постојале датотеке сумњивог садржаја или, пак, обрисане датотеке релевантне за истрагу

2. утврдити да ли је постојао малициозни софтвер на рачунару Богољуба Гагића путем ког је неко од запослених могао доћи у посед креденцијалима и на који начин, као и да ли је неко од неовлашћено приступао веб сервису за вођење евиденције о поласцима камиона и, уколико јесте, са чијег рачунара је вршен приступ
3. анализом радне меморије прикупљене са рачунара запослених пронаћи да ли је присутно коришћење стеганографских алата и алата за криптовање фајлова, партиција, дискова и доћи до датотека којима је руковао током спровођења команди. Уколико постоје енкриптовани фајлови, и уколико је могуће, доћи до изворних информација које су скривене
4. увидом у датотеку access.log издвојити јавне IP адресе фирме „Муња транс" (и одговарајуће портове) са којих је приступано веб сервису за евидентирање полазака камиона, такође одредити и приватне приватне IP адресе са којих је приступано веб сервису и којим запосленима те адресе припадају
5. документовати резултате претраге запослених, изјаснити се да ли је у периоду од 23.2.2023. до дана 26.2.2023. постојала интеракција електронском поштом између запослених. Извршити детаљну анализу како те преписке тако и других сумњивих преписки и листе позива уколико постоје на мобилном телефону запослене Душанке Свиларевић
6. над пронађеним видео снимцима надзорне камере пронађеним међу доказима, применити одговарајуће операције тако да се може одредити да ли је забележена нека сумњива активност релевантна за истрагу, и ко су њени учесници уколико јесте

На основу задатака вештачења, дајемо следећи

Н а л а з

Дана 6. 3. 2022. године у 10.30 часова, приступили смо вештачењу у просторијама Лабораторије за дигиталну форензику. Из рачунара Acer, модела Aspire E1-571 и серијског броја 589-87VQW389FSF-3FG, извадили смо чврсти диск произвођача Seagate, модела ST1000DM010 и серијског броја 3660619402182 (у наставку чврсти диск Богољуба Гагића). Из рачунара Toshiba, модела Satellite Pro L450 и серијског броја 897526, извадили смо чбрсти диск произвођача SYNOLOGY, модела HAT5300-12T и серијског броја 4711174724130 (у наставку чврсти диск Павла Пандуровића). Из рачунара HP, модела Pavilion G6 и серијског броја HP98-556FRWQ98DFL-258F, извађен је чврсти диск произвођача Western Digital, модела WD10SPZX и серијског броја 718037845319 (у наставку чврсти диск Душанке Свиларевић).

Направили смо форензичку копију чврстих дискова помоћу алата FTK Imager верзије 3.1.2.0. Форензичка копија је копија складишта података идентична оригиналу, а алат FTK Imager служи за креирање форензичке копије складишта података.

Помоћу алата Autopsy 4.19.2 извршили смо прегледање и анализу форензичких копија чврстог диска Богољуба Гагића, Павла Пандуровића и интерног складишта

Душанкиног мобилног телефона. Алат Autopsy служи за прегледање и анализу форензичких копија складишта података.

Анализом чврстог диска Богољуба Гагића, применом алата Autopsy и ingest модула Hash Lookup установљено је да постоје два малициозна софтвера под називом logview.exe и emsvc.exe (Прилог 1) помоћу којих је злонамеран запослени могао да дође до креденцијала за приступ веб сервису за вођење евиденције о поласцима камиона.

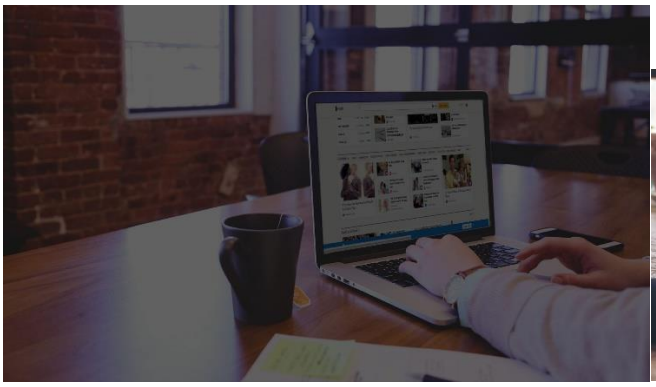
Source Name	S	C	O	MD5 Hash	Comment	
logview.exe			0	53b1de4f61d4716ea0c8b2f4d439c1e2		/img_bogoljub-disk.E01/vol_vol3/Program Files (x86)/FKL/logview.exe
emsvc.exe			0	c7f66f845d33f8e8e9746badf8447810		/img_bogoljub-disk.E01/vol_vol3/Program Files (x86)/FKL/emsvc.exe

Прилог 1- малициозни софтвери

Анализом чврстог диска Павла Пандуровића, пронађене су сумњиве датотеке у application/pdf формату чија екстензија не одговара датом формату, а то су фотографије под називима dddd.jpg и ssss.jpg. Фотографије заправо представљају једносмерне авионске карте на име Душанке Свиларевић и Павла Пандуровића са поласком истог датума 27.2.2023. у 11:30 на релацији BEG-CMN наведене у Прилогу 2. За овај проналазак коришћен је модул под називом Extension Mismatch Detector.

Прилог 2 – датотеке dddd.jpg и ssss.jpg којима је формат промењен

Користећи програм Foremost који представља форензички програм за опоравак изгубљених датотека на основу њихових заглавља, подножја и интерних структура података, пронађене су обрисане датотеке сумњивог садржаја у jpg формату од 100 до 150 KiB са чврстог диска извађеног из кућишта Павла Пандуровића које су дате у Прилогу 3.



Прилог 3 – обрисане фотографије

Рам меморија са рачунара запосленог Павла Пандуровића на ком је подигнут Ubuntu 14.04 оперативни систем, прикупљена је помоћу AVML алата. AVML је X86_64 кориснички алат за прикупљање радне меморије. AVML се може користити за прикупљање меморије без неопходног познавања циљне ОС дистрибуције или кернела.

Помоћу алата Volatility Foundation 2.6 извршили смо прегледање радне меморије Павла Пандуровића. Volatility Foundation представља софтверски алат отвореног изворног кода за прегледање и анализу радне меморије који је развила независна и непрофитна организација The Volatility Foundation.

Како је подигнут Ubuntu оперативни систем на његовом рачунару, било је неопходно укључити предложени профил као LinuxLinux_4_4_0-142-genericx64. Прегледањем форензичке слике и након примењеног linux_pslist плагина, анализом добијених резултата откривено је да су постојале две апликације за директну комуникацију које су инсталиране и то су Thunder bird и whatsApp. Такође, применом linux_bash плагина сазнали смо списак команди које су уношене. Детаљном анализом свих команди које су уношене преко терминала, издвојиле су се као сумњиве **инсталације steghide** алата која омогућава сакривање поверљивих података у слици или аудио фајлу и може да врши компресију, шифровање, екстраховање података, **cryptsetup** алата за енкриптовање података на Линуксу, као и **ccrypt** алат командне линије за енкрипцију и декрипцију података који је врло једноставан за коришћење. Пронађене су и команде које су извршене над датотекама како би се сакрили одређени подаци применом стеганографских метода. Датотеке којима је руковано током спровођења комади су *porodicnoblago.png* и *knjiga.jpeg* у које је сакривена идентична информација.

Декриптовањем ових датотека установљено је да информација коју скрива представља план са описом, локацијом утовара и истовара, време поласка и време трајања вожње, као и име возача. Такође, на чврстом диску Павла Пандуровића пронађена је и криптована датотека под називом **adresa.cpt** у којој је скривена информација о адреси хотела у Мароку. Адреса је Hôtel Casablanca, 02 Blvd Mohamed Diouri, Sidi Belyout, 20250 Casablanca, Morocco.

За прављење копије података са USB флеш меморија произвођача SanDisk, модела Cruser Force и серијског броја 0xd585e28 (у наставку USB флеш меморија) коришћен је FTK Imager.

Алат који се најчешће користи за анализу артифаката оперативног система Windows је RegRipper. Алат RegRipper 3.0 представља парсер датотека са кошницама регистра. Типови датотека са кошницама које може да парсира су SAM (Security Accounts Manager), SECURITY, SYSTEM, SOFTWARE и NTUSER.DAT. Помоћу категорија скрипти алата RegRipper смо били у могућности да прикажемо информације о инсталираним програмима, мрежној конфигурацији, екстерним складиштима, периферним уређајима и информацијама о извршеним програмима.

Анализом USB флеш меморије установљено је да је постојао софтвер **fk_install.exe** за снимање уноса са тастатуре – keylogger. Поред тога, применом алата RegRipper над кошницом System извезеном са чврстог диска Богољуба Гагића, пронађен је доказ да је

USB флеш меморија, која припада Павлу Пандуровићу, била маунтована на рачунару Богољуба Гагића, а такође пронађено је и да се малициозни софтвер покреће аутоматски након покретања рачунара (Прилог 4 и 5).

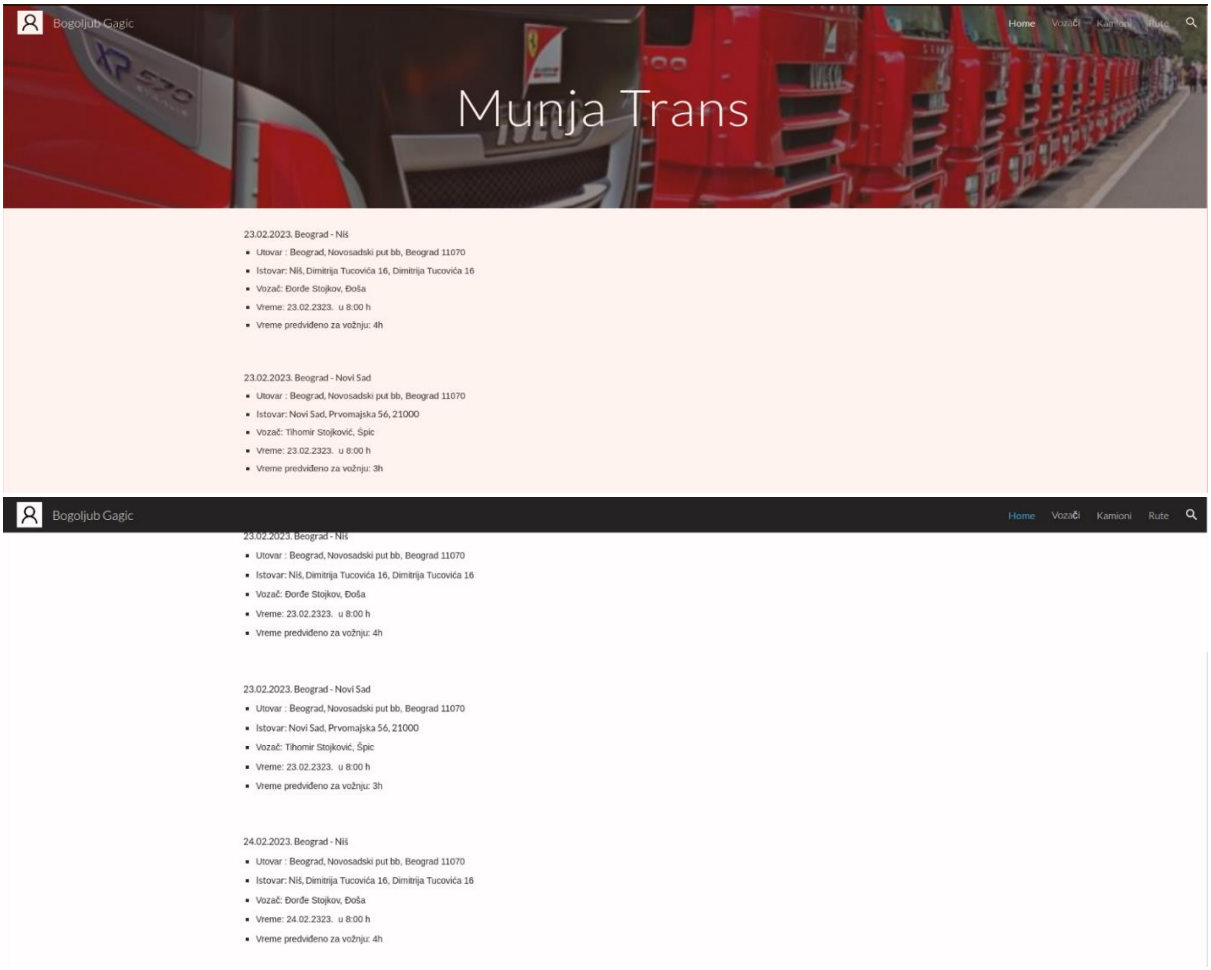
```
PortDev
Microsoft\Windows Portable Devices\Devices

Device    : DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07
SN        : 11711396&0
Drive     : pajausb


      E: - LastWrite time: 2023-02-22 22:27:33Z
      DriveType: Fixed
      VolumeLabel: pajausb

      G: - LastWrite time: 2023-02-22 22:27:33Z
      DriveType: Fixed
      VolumeLabel: Primer3

      H: - LastWrite time: 2023-02-22 22:28:25Z
      DriveType: Fixed
      VolumeLabel: Ceca
```

Прилог 4 – флеш меморија

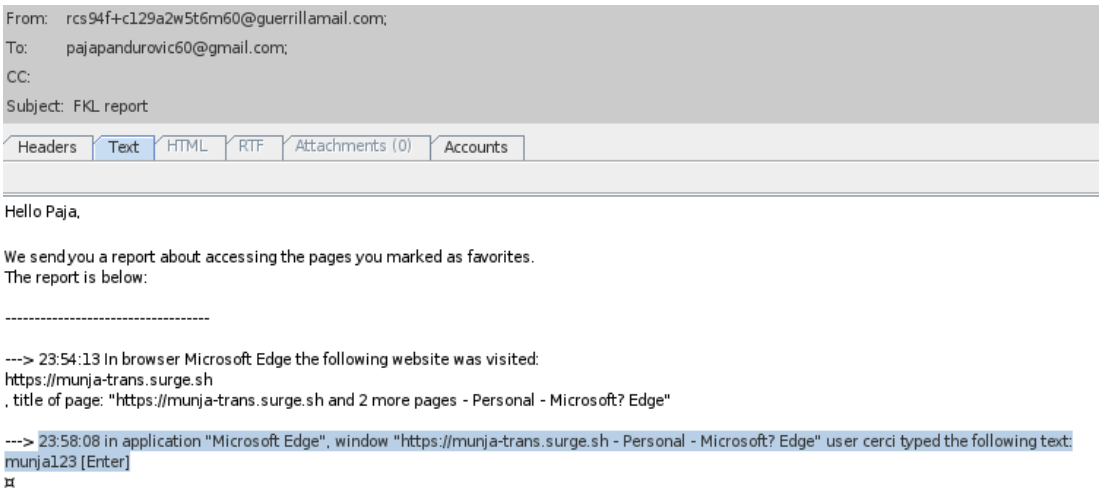
```
Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2023-02-23 07:52:04Z
  emsvc - C:\Program Files (x86)\FKL\emsvc.exe


Key path: Microsoft\Windows Defender\Exclusions\Extensions

Key path: Microsoft\Windows Defender\Exclusions\Processes
Exclusions\Processes key LastWrite time: 2023-02-26 00:28:09Z
  logview.exe                                          0
  emsvc.exe                                            0
```

Прилог 5 – аутоматско покретање малициозног софтвера

Анализом форензичке слике масовне меморије Павла Пандуровића и уз помоћ Exiftool алата командне линије, који омогућава екстракцију и измену метаподатака датотека различитих формата, пронашли смо све датотеке са графичким садржајем настале као снимак екрана путем gnome-screenshot апликације и издвојили две најрелевантније слике за истрагу и њихове метаподатке. Овим су експлицитно забележени редови вожње камиона, као и да се до те информације дошло преко профила Богољуба Гагића, што је могуће једино познавањем његових креденцијала за пријаву (Прилог 6). Такође, анализом масовне меморије Павла Пандуровића пронађена је електронска пошта чији садржај представља извештај малициозног програма keylogger (Прилог 7)



Прилог 6 – снимци екрана



Прилог 7 – садржај мејла малициозног софтвера

Анализом масовне меморије Павла Пандуровића, откривена је претрага везана за туристичке агенције и дестинације, где се издваја Казабланка која одговара и горепоменутој карти купљеној на његово име. Такође, иста анализа је извршена и над масовном меморијом Дубравке Свиларевић, где су добијени подударни резултати претраге (Прилог 8). Утврђено је да је Павле Пандуровић користио Firefox веб претраживач, а Душанка Свиларевић Opera веб претраживач.

places.sqlite,"google.com","ADDRESS Hôtel Casablanca","FireFox","2023-02-24 23:12:19 CET","pavle.img"
places.sqlite,"google.com","ADDRESS Hôtel Casablanca booking","FireFox","2023-02-24 23:12:29 CET","pavle.img"
places.sqlite,"google.com","hotel caxablana","FireFox","2023-02-24 23:18:10 CET","pavle.img"
places.sqlite,"google.com","turisticka agencija kazablanka","FireFox","2023-02-25 13:48:39 CET","pavle.img"
places.sqlite,"google.com","kazablanka maroko google maps","FireFox","2023-02-25 13:49:01 CET","pavle.img"
places.sqlite,"google.com","volatilityfondation.github","FireFox","2023-01-12 22:26:11 CET","pavle.img"

History,"google.com","zakon o prevozu robe","Opera","2023-02-21 11:32:38 CET","duda-disk.E01"
History,"google.si","https://mail.google.com/mail/","Opera","2023-02-21 10:23:40 CET","duda-disk.E01"
History,"google.si","https://mail.google.com/mail/","Opera","2023-02-21 10:21:18 CET","duda-disk.E01"
History,"google.si","gmail","Opera","2023-02-21 10:21:10 CET","duda-disk.E01"
History,"google.com","youtube","Opera","2023-02-24 12:32:11 CET","duda-disk.E01"
History,"google.com","air serbia","Opera","2023-02-24 12:32:21 CET","duda-disk.E01"
History,"google.com","letovi za kazablanku","Opera","2023-02-24 12:32:34 CET","duda-disk.E01"
History,"google.com","letovi za kazablanku air serbia","Opera","2023-02-24 12:32:49 CET","duda-disk.E01"

Прилог 8 – резултати претраге

Утврђено је да је постојала и преписка 24.2.2023. путем мејла у контексту путовања између њих, приликом које су разменили авионске карте купљене за путовање у Казабланку преко агенције AirSerbia, на датум 27.2.2023. са поласком у 11:30 са аеродрома у Београду. Преписка, приказ карата који је изворно у pdf формату и њихови метаподаци дати су у Прилогу 9.

```
"Source Name","E-Mail From","E-Mail To","Subject","Date Received","Message
(Plaintext)","Message ID","Path","Thread ID","Data Source"
"INBOX","dudasvilarevic60@gmail.com;","pajapandurovic60@gmail.com;","Fwd: Online
ticket","2023-02-24 13:36:23 CET","Evo i tvoje karte.

---------- Forwarded message ---------
ĐžĐ´: <rdc01z+8wu62vn3pz8tc@guerrillamail.com>
Date: Đ¿ĐµÑ‚, 24. Ñ„ĐµĐ± 2023. Ñƒ 13:33
Subject: Online ticket
...","Not available","/imap.gmail.com/INBOX","0fcc575b-67df-43ee-
aa9c-1f11d1d51561","pavle.img"
"INBOX","dudasvilarevic60@gmail.com;","pajapandurovic60@gmail.com;","Fwd: Online
tickets","2023-02-24 13:36:04 CET","Pajo evo moje karte. Istampaj i skini.


---------- Forwarded message ---------
ĐžĐ´: <rdc01z+8wu62vn3pz8tc@guerrillamail.com>
Date: Đ¿ĐµÑ‚, 24. Ñ„ĐµĐ± 2023. Ñƒ 13:31
Su...","Not
available","/imap.gmail.com/INBOX","a55bcba7-543d-46d7-8ec5-411fcbe8b759","pavle.img"
```

AirSERBIA

IME / FIRST NAME	PREZIME / LAST NAME	LET IZ – LET ZA / FLIGHT FROM – FLIGHT TO		AirSERBIA	
Dušanka	Svilarević	Beograd RS – Casablanca MA		IME / FIRST NAME	Dušanka
POLAZAK / DEPARTURE	DATUM / DATE	VREME / TIME		PREZIME / LAST NAME	Svilarević
BEG	27.02.2023.	11:30		LET IZ – LET ZA / FLIGHT FROM – FLIGHT TO	Beograd RS – Casablanca MA
DOLAZAK / ARRIVAL	DATUM / DATE	VREME / TIME		POLAZAK / DEPARTURE	BEG
CMN	27.02.2023.	14:30		DATUM / DATE	VREME / TIME
MEĐUSLETANJA / INTERMEDIATE LANDINGS				27.02.2023.	11:30
AERODROMI / AIRPORTS	BEG – Nikola Tesla Aerodrom (Beograd, Srbija) / Nikola Tesla Airport (Belgrade, Serbia)			DOLAZAK / ARRIVAL	CMN
	CMN – Mohamed V International Airport (Kazablanka, Maroko) / Mohamed V International Airport (Casablanca, Maroko)			DATUM / DATE	VREME / TIME
PROLAZ / GATE	B-15	VREME UKRCAVANJA / BOARDING TIME	10:50	27.02.2023.	14:30
SEDIŠTE / SEAT	19 F	USLUGE / SERVICES	Odrasli, Ekonomska klasa / Adults, Economy class	PROLAZ / GATE	B-15
REG. BROJ / RE. NUMBER	2548-7668-9887			VREME UKRCAVANJA / BOARDING TIME	10:50
CENA / PRICE	35100,00 RSD / 300 EUR			SEDIŠTE / SEAT	19 F
KOD / CODE	2548-7668-9887-beg-cas			USLUGE / SERVICES	Odrasli, Ekonomska klasa / Adults, Economy class
NAPOMENA / NOTE	Elektronska karta važi bez pečata i potpisa. / The electronic card is valid without a stamp and signature.			REG. BROJ / RE. NUMBER	2548-7668-9887

AirSERBIA

IME / FIRST NAME	PREZIME / LAST NAME	LET IZ – LET ZA / FLIGHT FROM – FLIGHT TO		AirSERBIA	
Pavle	Pandurović	Beograd RS – Casablanca MA		IME / FIRST NAME	Pavle
POLAZAK / DEPARTURE	DATUM / DATE	VREME / TIME		PREZIME / LAST NAME	Pandurović
BEG	27.02.2023.	11:30		LET IZ – LET ZA / FLIGHT FROM – FLIGHT TO	Beograd RS – Casablanca MA
DOLAZAK / ARRIVAL	DATUM / DATE	VREME / TIME		POLAZAK / DEPARTURE	BEG
CMN	27.02.2023.	14:30		DATUM / DATE	VREME / TIME
MEĐUSLETANJA / INTERMEDIATE LANDINGS				27.02.2023.	11:30
AERODROMI / AIRPORTS	BEG – Nikola Tesla Aerodrom (Beograd, Srbija) / Nikola Tesla Airport (Belgrade, Serbia)			DOLAZAK / ARRIVAL	CMN
	CMN – Mohamed V International Airport (Kazablanka, Maroko) / Mohamed V International Airport (Casablanca, Maroko)			DATUM / DATE	VREME / TIME
PROLAZ / GATE	B-15	VREME UKRCAVANJA / BOARDING TIME	10:50	27.02.2023.	14:30
SEDIŠTE / SEAT	18 F	USLUGE / SERVICES	Odrasli, Ekonomska klasa / Adults, Economy class	PROLAZ / GATE	B-15
REG. BROJ / RE. NUMBER	2548-7856-9846			VREME UKRCAVANJA / BOARDING TIME	10:50
CENA / PRICE	35100,00 RSD / 300 EUR			SEDIŠTE / SEAT	18 F
KOD / CODE	2548-7856-9846-beg-cas			USLUGE / SERVICES	Odrasli, Ekonomska klasa / Adults, Economy class
NAPOMENA / NOTE	Elektronska karta važi bez pečata i potpisa. / The electronic card is valid without a stamp and signature.			REG. BROJ / RE. NUMBER	2548-7856-9846

```
ExifTool Version Number         : 12.40
File Name                       : PavleKarta.pdf
Directory                       : .
File Size                       : 69 KiB
File Modification Date/Time     : 2023:04:19 12:04:43+02:00
File Access Date/Time           : 2023:04:19 12:04:43+02:00
File Inode Change Date/Time     : 2023:04:19 12:04:43+02:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.6
Linearized                      : No
Page Count                      : 1
Language                        : sr-RS
Author                          : Svetlana Antesevic
Creator                         : Writer
Producer                        : LibreOffice 7.3
Create Date                     : 2023:02:24 13:23:03+01:00
```

```
ExifTool Version Number         : 12.40
File Name                       : PavleKarta.pdf
Directory                       : .
File Size                       : 69 KiB
File Modification Date/Time     : 2023:04:19 12:04:43+02:00
File Access Date/Time           : 2023:04:19 12:04:43+02:00
File Inode Change Date/Time     : 2023:04:19 12:04:43+02:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.6
Linearized                      : No
Page Count                      : 1
Language                        : sr-RS
Author                          : Svetlana Antesevic
Creator                         : Writer
Producer                        : LibreOffice 7.3
Create Date                     : 2023:02:24 13:23:03+01:00
```

Прилог 9 – преписка, приказ карата и њихових метаподатака

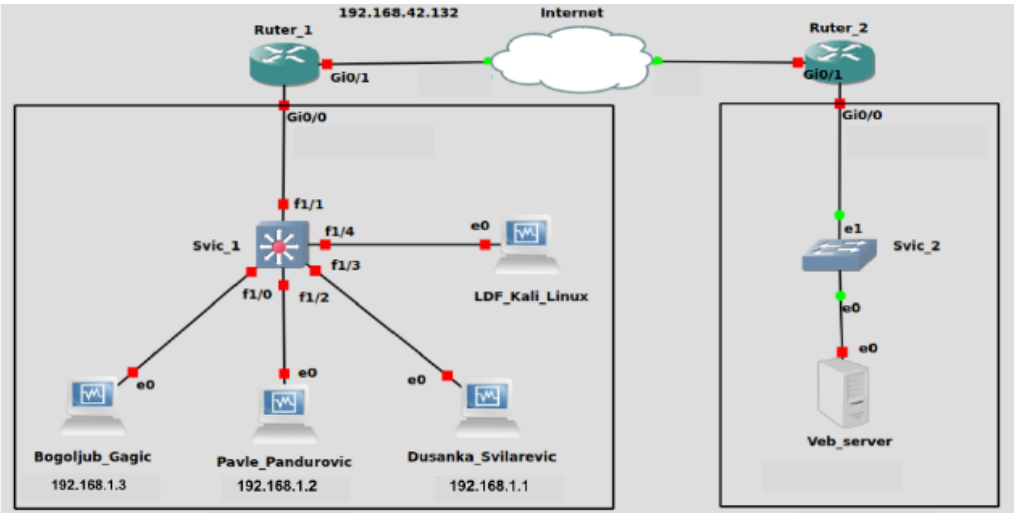
Алат FTK Imager коришћен је и за прикупљање рам меморије са рачунара Душанке Свиларевић на ком је подигнут WindowsXP оперативни систем.

Анализом радне меморије прикупљене са рачунара Душане Свиларевић пронађени су и документовани процесе који су покренути, а који нису системски (Прилог 10). То је одрађено коришћењем Volatility софтверског алата и pslist плагина. С обзиром да је оперативни систем на рачунару Душанке Свиларевић WindowsXP, било је неопходно поставити профил на WinXPSP1x64.

```
Offset(V)          Name                    PID   PPID   Thds
Hnds   Sess  Wow64 Start                          Exit
------------------ ---------------------- ------ ------ ------ -
------- ------ ------ ------------------------------ ---------
---------------------
0xfffffadfce8d9c20 System                    4      0     61
402 ------      0
0xfffffadfcdfe4040 smss.exe                548      4      3
18 ------      0 2023-02-26 00:02:33 UTC+0000
0xfffffadfce0e3040 csrss.exe                604    548     11
441      0      0 2023-02-26 00:02:33 UTC+0000
0xfffffadfce0dd040 winlogon.exe             628    548     27
599      0      0 2023-02-26 00:02:33 UTC+0000
0xfffffadfce0e9040 services.exe             672    628     17
287      0      0 2023-02-26 00:02:33 UTC+0000
0xfffffadfce0e8040 lsass.exe                700    628     28
495      0      0 2023-02-26 00:02:33 UTC+0000
0xfffffadfce0aa440 VBoxService.exe          876    672      9
131      0      0 2023-02-26 00:02:34 UTC+0000
0xfffffadfce3a98d0 svchost.exe              944    672      7
83       0      0 2023-02-26 00:02:34 UTC+0000
0xfffffadfce0e1040 svchost.exe              120    672     10
245      0      0 2023-02-26 00:02:34 UTC+0000
0xfffffadfce284040 svchost.exe              184    672     95
1365      0      0 2023-02-26 00:02:34 UTC+0000
0xfffffadfcdf12040 svchost.exe              264    672     11
138      0      0 2023-02-26 00:02:34 UTC+0000
0xfffffadfce04a640 svchost.exe              376    672     24
281      0      0 2023-02-26 00:02:34 UTC+0000
0xfffffadfce0e1c20 spoolsv.exe              580    672     15
122      0      0 2023-02-26 00:02:34 UTC+0000
0xfffffadfce060780 explorer.exe            1552   1488     13
323      0      0 2023-02-26 00:02:43 UTC+0000
**************************
0xfffffadfce209b10 svchost.exe             1784    672      2
56       0      0 2023-02-26 00:02:43 UTC+0000
0xfffffadfce2bb8d0 IPROSetMonitor.         1856    672      2
42       0      0 2023-02-26 00:02:43 UTC+0000
0xfffffadfce4a0c20 VBoxTray.exe            1864   1552     12

0xfffffadfce0f7a90 msmsgs.exe              1908   1552      3
147      0      1 2023-02-26 00:02:43 UTC+0000
0xfffffadfce11b8b0 svchost.exe             2024    672      7
93       0      0 2023-02-26 00:02:43 UTC+0000
0xfffffadfce120670 wmiprvse.exe             820    944      7
176      0      0 2023-02-26 00:02:43 UTC+0000
0xfffffadfce4b6c20 alg.exe                  276    672      6
75       0      0 2023-02-26 00:02:47 UTC+0000
0xfffffadfcded1780 msiexec.exe             2276    672      6
105      0      0 2023-02-26 00:04:37 UTC+0000
0xfffffadfce2325b0 FTK Imager.exe          2520   2252     11
267      0      1 2023-02-26 00:05:13 UTC+0000
**************************
0xfffffadfce2708d0 wmiadap.exe             2972    184      3
18 ------      0 2023-02-26 00:06:44 UTC+0000
```

Прилог 10 – Несистемски процеси на рачунару Душанке Свиларевић

Анализом лог датотека веб сервера који хостује сервис за евидентирање полазака камиона и NAT сервиса конфигурисаног на рутеру фирме „Мућа транс“, издвојене су како јавне тако и приватне IP адресе са којих је приступано веб сервису за евидентирање полазака камиона. Утврђено је да оне припадају директору Богољубу Гагићу и запосленом Павлу Пандуровићу (Прилог 11 и 12).




```
192.168.42.132 "57333" - - [14/Feb/2023:12:55:45] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.75 Safari/537.36 Edg/100.0.1185.39"
192.168.42.132 "41036" - - [19/Feb/2023:16:05:46] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:65.0) Gecko/20100101 Firefox/65.0"
192.168.42.132 "57355" - - [20/Feb/2023:08:01:13] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.75 Safari/537.36 Edg/100.0.1185.39"
192.168.42.132 "57358" - - [20/Feb/2023:12:05:39] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.75 Safari/537.36 Edg/100.0.1185.39"
192.168.42.132 "41038" - - [21/Feb/2023:11:05:17] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:65.0) Gecko/20100101 Firefox/65.0"
192.168.42.132 "41034" - - [15/Feb/2023:12:57:33] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:65.0) Gecko/20100101 Firefox/65.0"
192.168.42.132 "57341" - - [15/Feb/2023:12:58:17] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.75 Safari/537.36 Edg/100.0.1185.39"
192.168.42.132 "57346" - - [16/Feb/2023:12:59:01] "GET /
HTTP/1.1" 200 490 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.75 Safari/537.36 Edg/100.0.1185.39"
```

Прилог 11 – шема рачунарске мреже, јавне ИП адресе и портови

```
tcp 192.168.42.132:57358 192.168.1.3:57358 10.10.10.1:80
10.10.10.1:80 <- Bogoljub Gagic

tcp 192.168.42.132:41038 192.168.1.2:41038 10.10.10.1:80
10.10.10.1:80 <- Pavle Pandurovic

tcp 192.168.42.132:41034 192.168.1.2:41034 10.10.10.1:80
10.10.10.1:80 <- Pavle Pandurovic
```

Прилог 12 – приватна адреса која припада Павлу Пандуровићу

Поред овога, увидом у снимак мрежног саобраћаја Душанке Свиларевић, утвдили смо да је дана 23.2.2023. године успостављена безбедна комуникација са сервером чије име домена је airserbia.com (екстерни Прилог 13)

Помоћу алата adb, направили смо форензичку копију података ускладиштених у интерном складишту података мобилног телефона произвођача Google, модел Pixel 5 и серијског броја EMULATOR32X1X11X0 (у наставку мобилни телефон). Алат adb, између осталог, служи за преузимање података из складишта података мобилног телефона.

Анализирали смо интерно складиште мобилног телефона помоћу модула aLEAPP алата Autopsy. aLEAPP служи за прегледање и анализу података преузетих из складишта података мобилног телефона.

Анализом података са мобилног телефона утврђено је да је Душанка размењивала поруке и позиве са Павлом Пандуровићем 22.2.2023. и 23.2.2023. За исти период пронађена је листа позива и SMS порука између ово двоје запослених у којима се помиње извесни Језа – Данило Језеркић и план за одлазак у Мароко. Пронађена је и WhatsApp преписка са претходно поменутим Данилом Језеркићем за дане 22.2.2023. и 23.2.2023. у којој је размењена и једна сумњива датотека (Прилог 13 и 14)

mimetype	data1	display_name	phone_number	email address
vnd.android.cursor.item/email_v2	pajapandurovic60@gmail.com	Paja		pajapandurovic60@gmail.com
vnd.android.cursor.item/phone_v2	+381 64 5956081	Danilo Jezerkic Jeza	+381 64 5956081	
vnd.android.cursor.item/phone_v2	+381645956081	Danilo Jezerkic Jeza	+381645956081	
vnd.android.cursor.item/phone_v2	+381 69 587875	Dragan	+381 69 587875	
vnd.android.cursor.item/phone_v2	+381 65 854745	Mama	+381 65 854745	
vnd.android.cursor.item/phone_v2	+381 65 874852	Nikolina	+381 65 874852	
vnd.android.cursor.item/phone_v2	+381 64 3814567	Paja	+381 64 3814567	
vnd.android.cursor.item/phone_v2	+381 64 558589	Tata	+381 64 558589	

from_id	to_id	start_date	end_date	direction	name
	+381643814567	2023-02-23 10:01:55	2023-02-23 10:01:55	Outgoing	
	+381643814567	2023-02-22 12:03:37	2023-02-22 12:03:37	Outgoing	Paja
+381643814567		2023-02-22 12:03:52	2023-02-22 12:03:52	Incoming	Paja
+381643814567		2023-02-22 12:03:46	2023-02-22 12:03:46	Incoming	Paja
from_id	to_id	start_date	end_date	direction	name

Прилог 13 – Контакти и позиви

2023-02-22 11:10:00		Danilo Jezerkic Jeza		Outgoing	System Message				
2023-02-22 11:10:10		Danilo Jezerkic Jeza		Outgoing	Text	Cao Jezo			
2023-02-22 11:10:49		Danilo Jezerkic Jeza		Outgoing	Text	Sta se radi?			
2023-02-22 11:11:54		Danilo Jezerkic Jeza		Outgoing	Text	Ahha, lepo lepo			
2023-02-22 11:12:22		Danilo Jezerkic Jeza		Outgoing	Text	Pa I ja isto, evo sa Pajom dogovaram oko naseg posla zajednickog			
2023-02-22 11:13:25		Danilo Jezerkic Jeza		Outgoing	Text	E bice, kaze Paja da je saznao nesto oko polazaka ove ture pa ti javlja detalje			
2023-02-22 11:13:39		Danilo Jezerkic Jeza		Outgoing	Text	Naravno mislim da ce to on na svoj specijalan nacin			
2023-02-22 11:13:50		Danilo Jezerkic Jeza		Outgoing	Text	Pa ti ja saljem te dokumente uskoro			
2023-02-22 11:15:44		Danilo Jezerkic Jeza		Outgoing	Text	E super 😊			
2023-02-22 11:16:40		Danilo Jezerkic Jeza		Outgoing	Text	Nista javim ti ja cim saznam vise			
2023-02-22 11:16:47		Danilo Jezerkic Jeza		Outgoing	Text	Budi u pripravnosti			

2023-02-22 11:21:37	2023-02-22 11:24:29	Danilo Jezerkic Jeza		Outgoing	Document	knjiga.txt	DOC-20230223-WA0000.	Media/WhatsApp Documents/Sent /DOC-20230223-WA0000.	142583
2023-02-22 11:21:56		Danilo Jezerkic Jeza		Outgoing	Text	Paja je primenjivao ono standard kao I do sad			
2023-02-22 11:22:14		Danilo Jezerkic Jeza		Outgoing	Text	Ti mozes isto uraditi I za povratak			
2023-02-22 11:22:21		Danilo Jezerkic Jeza		Outgoing	Text	Cist racun duga ljubav			
2023-02-22 11:23:35		Danilo Jezerkic Jeza		Outgoing	Text	Vazi			
2023-02-22 11:25:17		Danilo Jezerkic Jeza		Outgoing	Text	Super 😊			
2023-02-22 11:29:40	2023-02-22 11:10:00	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Cao			
2023-02-22 11:30:57	2023-02-22 11:11:17	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Evo radi we punom parom			
2023-02-22 11:31:33	2023-02-22 11:11:53	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Ti			
2023-02-22 11:32:16	2023-02-22 11:12:36	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	O lepe vesti			
2023-02-22 11:32:45	2023-02-22 11:13:05	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Zna li se kakva informacija?			
2023-02-22 11:33:57	2023-02-22 11:14:17	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Super 👌👌			
2023-02-22 11:34:57	2023-02-22 11:15:17	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Bez brige moj roki ce to protumaciti			
2023-02-22 11:36:34	2023-02-22 11:16:54	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Vazi			

2023-02-23 08:59:26	2023-02-22 11:22:55	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	OO super
2023-02-23 08:59:44	2023-02-22 11:23:13	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Sada ce to moj Roki da resi
2023-02-23 09:00:01	2023-02-22 11:23:30	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Javljam kako je proslo
2023-02-23 09:01:35	2023-02-22 11:25:04	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	E pronasli smo sve informaicje. Ocekujte lovu veceras 💰
2023-02-23 14:01:14	2023-02-22 11:29:09	Danilo Jezerkic Jeza	381645956081@s.whatsapp.net	Incoming	Text	Dudo imamo problem Moj momci su pali
Message Timestamp	Received Timestamp	Other Participant WA User Name	Sending Party JID	Message Direction	Message Type	Message

Прилог 14 – поруке

Обрада слика и видеа рађена је коришћењем VideoCleaner 5.8 софтвера, уз помоћ кога се може побољшати квалитет слика, аудио и видео записа, који даје изузетно добре резултате на екстремно тамним/светлим сликама, уз помоћ ког се могу издвојити и изоштрити детаљи као и уклонити шум.

Увидом у снимке надзорних камера утврђено је да се на њима појављују три особе од којих једна стоји ослоњена на ауто са возачеве стране, друга је возач, док се трећа особа, највероватније мушког пола, на сувозачевом месту не види добро. За обраду фотографије примењени су следећи параметри: unSharpen Strength = 26, Sharpening Strength =8, Video Contrast strength -5, Histogram=1, Stabilize strength=1, Deblock strength=12.

На другој издвојеној фотографији из видео снимка надзорне камере уочен је и један аутомобил регистарских таблица BG407964 или BG407965. За обраду ове фотографије примењени су следећи параметри: Histogram=1, unSharpen Strength = 15, Sharpening Strength =19,Color Contrast Strength = 9, Stabilize Strength = 2, Focus Correction Strength =19. Фотографије пре и после обраде дате су у Прилогу 15, редом.

Прилог 15- издвојене фотографије кадрова надзорне камере пре и после обраде

На основу изнетог налаза, дајемо следеће

М и ш љ е њ е

Детаљном анализом свих прикупљених доказа и вештачењем утврђено је да је постојао малициозни софтвер на рачунару Богољуба Гагића путем ког су се могли сазнати креденцијали за приступ веб сервису за вођење евиденције о поласцима камиона. Инсталациону датотеку тог истог софтвера поседовао је запослени Павле Пандуровић на USB флеш меморији која је маунтована на рачунар Богољуба Гагића. Такође, анализом мрежног саобраћаја фирме „Муња транс“ и чврстих дискова преузетих из рачунара Богољуба Гагића и Павла Пандуровића, утврђено је да је Павле приступао веб сервису за вођење евиденције о поласцима камиона, којем, по правилу, имају право само директор фирме и возачи камиона, што имплицира да је он малициозним софтвером дошао до креденцијала за пријаву и искористио их. Ту чињеницу поткрепљује и имејл малициозног софтвера са креденцијалима који је пронађен у његовом имејл сандучету. На чврстом диску његовог рачунара су пронађене и фотографије које експлицитно представљају снимке екрана на ком су приказане информације о поласцима камиона.

У периоду од 23.2.2023. до 26.2.2023. пронађени су докази да је постојала комуникација у виду телефонских позива и размене електронске поште између Душанке Свиларевић и Павла Пандуровића приликом које су договарали путовање у Казабланку. Електронском поштом су размењене авионске карте на њихово име за 27.3.2023. путем авио компаније AirSerbia. Пронађен је доказ анализом мрежног саобраћаја да је Душанка Свиларевић приступала сајту авио компаније.

За исти период пронађена је листа SMS порука између Павла и Душанке у којима се помиње дотични Језа – Данило Језеркић и план за одлазак у Мароко. У телефону Душанке Свиларевић пронађена је и WhatsApp преписка са претходно поменутим Данилом Језеркићем за дане 22.2.2023. и 23.2.2023. у којој је размењена и једна сумњива датотека.

Увидом у снимке надзорних камера утврђено је да се на њима појављују три мушке особе, од којих је једна неидентификована, а за друга два мушкарца се претпоставља се да су то Павле Пандуровић и Данило Језеркић, а уочен је и један аутомобил регистарских таблица BG407964 или BG407965.

Декриптовањем датотеке пронађене на чврстом диску Павла Пандуровића, добијена је информација о адреси хотела у Мароку што оправдава сумњу да су запослени умешани у овај злочин, као и претпоставку да су желели да побегну након извршеног плана. На основу команди које је Павле Пандуровић извршавао у терминалу, пронађена је и фотографија унутар које је сакривен текст који представља план недозвољених активности. Он обухвата опис, локацију утовара и истовара, време поласка и трајање вожње и име возача.

Судски вештак за информационе технологије

Невена Атић, дипл. инж.

Нови Сад, 21. 6. 2023.

Прилози:

1. Прилог 13