

Лабораторија за дигиталну форензику
Факултет техничких наука
Фрушкогорска 1
21102 Нови Сад

5. 6. 2024.

Петар Петровић
Тополска 18
11000 Београд

Дана 9. 3. 2024. године ангажовани смо од стране Петра Петровића из Београда, да извршимо вештачење и сачинимо налаз и мишљење.

Задатак вештачења је да прегледамо и анализирамо електронску опрему која укључује десктоп рачунар Богољуба Гагића, произвођача Acer, модела Aspire E1-571 и серијског броја 589-87VQW389FSF-3FG, десктоп рачунар Душанке Свиларевић, произвођача HP, модела Pavilion G6 и серијског броја HP98-556FRWQ98DFL-258F, десктоп рачунар Павла Пандуровића, произвођача и мобилни телефон произвођача Toshiba, модела Satellite Pro L450, серијског броја 897526, USB стик у власништву Павла Пандуровића, произвођача SanDisk, модела Cruser Force, серијског броја 0xd585e28, мобилног телефона у власништву Душанке Свиларевић, произвођача Google, модел Pixel 5 и серијског броја EMULATOR32X1X11X0, снимци надзорних камера компаније „Муња транс”, преузетих са камера произвођача Reolink Tehnologija IP и модела REO RLC-510A, од директора Богољуба Гагића: snimak_nadzorne_kamere_1.mp4 (у наставку снимак 1) и snimak_nadzorne_kamere_2.mp4 (у наставку снимак 2) а које је Богољуб Гагић, добровољно предао полицијским службеницима МУП РС, приликом извршења наредбе Вишег суда у Београду и:

1. Да ли је рачунар осумњиченог Богољуба Гагића злонамерно употребљен од стране трећих лица и ако да, навести те трагове,
2. Да ли меморија рачунара Павла Пандуровића садржи трагове прикривања његове активности и ако да, навести те трагове,
3. Анализирати мрежни саобраћај приватне мреже предузећа „Муња транс”, и изјаснити се да ли је са рачунара приватне мреже приступано веб-сајту за куповину авионских карата и, ако јесте, са ког рачунара,
4. Потом се изјаснити у погледу приступања веб-сервису хостованом на адреси

<https://munja-trans.surge.sh/> који приказује ажурне информације о поласцима камиона – да ли му је приступано са рачунара који не би требало да имају приступ веб-серверу и ако јесте, навести трагове приступања,

5. Да ли су осумњичени, Павле Пандуровић и Душанка Свиларевић, комуницирали са другим особама, ко су особе са којима је комуникација вршена, преко чега је вршена комуникација, шта је садржина комуникације,
6. Анализирати прикупљене податке са мобилног телефона од Душанке Свиларевић, њене контакте, поруке и позиве. Потребно је приказати све контакте у именику, све SMS поруке и метаподатке о телефонским позивима везане за комуникацију са Павлом Пандуровићем,
7. Да ли се у историји веб-претраге осумњичених, Павла Пандуровића и Душанке Свиларевић, налазе трагови приступања веб-сајтовима авио- компанија, туристичких агенција и дестинација.
8. Изјаснити се да ли је могуће побољшање видео снимака 1 и 2 тако да се на снимку 1 може одредити број особа чија се лица могу препознати, а на снимку 2 да се могу одредити регистарске ознаке возила,
9. Такође, задатак вештака је да пруже одговоре и свој налаз и мишљење дају и у погледу других чињеница и околности које уоче током вештачења, а које су од значаја за сагледавање предмета вештачења и околности под којима је предметно кривично дело извршенено,

На основу задатка вештачења, дајемо следећи

Н а л а з

Дана 16. 3. 2024. године у 9.00 часова, приступили смо вештачењу у просторијама Лабораторије за дигиталну форензику. Из десктоп рачунара Богољуба Гагића, произвођача Acer, модела Aspire E1-571 и серијског броја 589-87VQW389FSF-3FG, извадили смо чврсти диск производа Seagate, модела ST1000DM010 и серијског броја 3660619402182 (у наставку чврсти диск Богољуба Гагића).

Направили смо форензичку копију чврстог диска Богољуба Гагића помоћу алата FTK Imager верзије 3.1.1.8.

Форензичка копија је копија складишта података идентична оригиналу, а алат FTK Imager служи за креирање форензичке копије складишта података.

Помоћу алата RegRipper над кошницом System утврдили смо да је на десктоп рачунару Богољуба Гагића била маунтована USB флеш меморија Павла Пандуровића под именом Generic Flash Disk USB Device. У прилогу 1 се налази команда коју смо користили како би дошли до закључка.

RegRipper је алат који се користи за анализу Windows регистра ради екстракције информације из њега. Овај алат омогућава форензичарима да прегледају, анализирају и интерпретирају регистарске записи ради проналажења доказа о активностима корисника, инсталираним програмима, променама у систему и другим важним подацима.

Помоћу алата Foremost анализом чврстог диска Павла Пандуровића пронашли смо обрисане датотеке у jpg формату.

Foremost је форензички програм за опоравак изгубљених датотека на основу њихових заглавља, подножја и интерних структура података. Може да ради на датотекама слика, као што су оне које генерише dd, Safeback, Encase или директно на диску.

Помоћу Volatiliy Foundation алата анализом форензичке слике радне меморије прикупљене са десктоп рачунара Павла Пандуровића пронашли смо команде које је корисник уносио у терминал-емулатор, а које указују на коришћење стеганографских алата и алат за криптоирање фајлова, партиција, дискова. У прилогу 2 се налазе команде које је Павле Пандуровић користио за прикривање своје активности.

Volatiliy Foundation је софтверски алат отвореног извornог кода за прегледање и анализу радне меморије.

Стеганографија је техника скивања порука унутар других неупадљивих медија како би се порука сакрила од неовлашћених посматрача.

Помоћу алата mrezaR смо анализирали мрежни саобраћај и рутирање у мрежи. Јавна IP адреса предузећа „Муња Транс“ је 192.168.36.100. Приватна адреса рачунара са кога је приступано веб сайту wizzair.com је 10.10.10.3. Приватне адресе рачунара са којих је приступано Apache2 HTTP веб серверу су 10.10.10.1 и 10.10.10.2. Веб претраживач који је користио малициозни запослени приликом приступања Apache2 HTTP веб серверу је Mozilla/5.0.

MrezaR је апликација коју је развила студент докторских студија факултета техничких наука у Новом Саду, ради лакше анализе мреже, мрежних уређаја и мрежног саобраћаја.

Користећи Hash Lookup алат одређен је софтвер помоћу којег је запослени дошао до креденцијала помоћу којих је неовлашћено приступио сајту <https://munja-trans.surge.sh/>.

Hash Lookup је алат који проверава да ли се у бази података са hash вредностима малициозних датотека налази нека од датотека из извornог медијума. Могуће је додатно исконфигурисати овај модул и проширити базу са hash вредностима.

Користећи Autopsy алат утврдили смо да су Палве Пандуровић и Душанка Свиларевић вршили комуникацију са другим особама. Користили смо ingest модуле recent activity (издава корисничку активност у последњих 7 дана коју чувају веб претраживачи, инсталирани програми и оперативни системи), email parser (идентификује Thunderrbird MBOX датотеке и PST формате датотека на основу потписа датотека, издава е-поруке из њих, додаје прилоге као изведене датотеке), extension mismatch (пореди заглавље фајла и екstenзију и проверава да ли је одговарајући тип фајла) , embedded file extractor(отвара архиве датотека ZIP, RAR и друге форате као што су .doc, docx, ppt, xls, xlsx како би омогућио анализу ових датотека тј. Претпрагу кључних речи).

У прилогу 3 су приказане све SMS поруке и метаподаци о телефонским позивима везане за комуникацију са Павлом Пандуровићем, као и email комуникација за куповину авионских карата.

Утврдили смо да се у историји веб-претраге осумњичених, Павла Пандуровића и Душанке Свиларевић, налазе трагови приступа веб-сајтовима авио-компанија, туристичких агенција и дестинација користећи претходно наведене ingest модуле. У прилогу 4 се налазе информације о историји претраге као и информације о претраживачу.

Користећи Video Cleaner алат утврдили смо да је могуће побољшање видео снимака 1 и 2 тако да се на снимку 1 могу одредити број особа чија се лица могу препознати, а на снимку 2 да се могу одредити регистарске ознаке возила.

У прилогу 5 се налазе параметри које смо подесили како би дошли до закључка.

Video Cleaner је бесплатан алат отвореног кода за оперативни систем Windows. Служи за форензичку анализу дигиталних слика и видео записа различитих формата.

М и ш л ѕ е њ є

Десктоп рачунар Богољуба Гагића је злонамерно употребљен од стране трећих лица. Установљено је да се на његовом рачунару налазио USB диск Павла Пандуровића.

Меморија десктоп рачунара Павла Пандуровића садржи трагове прикривања активности. Пронађено је коришћење стеганографских алата и алата за криптовање фајлова, партиција, дискова као и обрисане датотеке у .jpg формату.

Одређен је софтвер помоћу којег је запослени дошао до креденцијала помоћу којих је неовлашћено приступиој сајту <https://munja-trans.surge.sh/>. Закључено је да му је приступљено са рачунара који не би требало да има приступ веб серверу.

На основу анализе SMS порука и email порука закључено је да су Душанка Свиларевић и Павле Пандуровић комуницирали са другим особама. Конверзација се може видети у прилогу.

На основу анализе историје претраге осумљичених Павла Пандуровића и Душанке Свиларевић утврђено је да се налазе трагови приступања веб сајтовима авио компанија, туристичких агенција и дестинација.

Побољшање видео снимака је успешно извршено помоћу одговарајућег алата и одговарајућих параметара који се могу видети у прилогу.

Судски вештак за информационе технологије

Нови Сад, 6. 6. 2024.

Немања Малиновић, маст. инж.

Прилози:

1. Прилог 1: RegRipper команда
2. Прилог 2: Команде за прикривање активности
3. Прилог 3: Размењене SMS и EMAIL поруке , позиви и контакти, авионске карте
4. Прилог 4: Информације о историји претраге као и информације о претраживачу
5. Прилог 5: Video Cleaner параметри

Прилог 1: RegRipper команда

```
perl rip.pl.linux -r /home/kali/LDF/radni_direktorijum/E2-45 2023/Zadatak3/104833-SYSTEM -  
p usbstor >> /home/kali/LDF/radni_direktorijum/E2-45-2023/Zadatak3/usbstor.txt
```

```
perl rip.pl.linux -r /home/kali/LDF/radni_direktorijum/E2-45-2023/Zadatak3/104827-  
SOFTWARE -p run >> /home/kali/LDF/radni_direktorijum/E2-45-2023/Zadatak3/run.txt
```

Прилог 2: Команде за прикривање активности

Errors occurred while ingesting image

1. Encryption detected (LUKS) (Sector offset: 0)

На USB-у откриена је енкрипција путем LUKS. Потребно је изврсити декрипцију.

Користи се foremost алат како бисмо из диска експортовали слике одређене величине.

Команда: foremost -t jpg -i pavle.img -o pavleJpgs -q [velicina]

```
sudo python2 vol.py -f  
/home/kali/Documents/Forenzicke_slike/Pavle_Pandurovic/FS_operativna_memorija/paja_ram.r  
aw --profile=LinuxLinux_4_4_0-142-genericx64 linux_bash
```

Излистани су сви уноси у терминал, затим су у фајлу bash.txt пронађене команде везане за криптографију и стеганографију.

Прилог 3: Разменење SMS и EMAIL поруке, позиви и контакти, авионске карте

KONTAKTI

vnd.android.cursor.item/email_v2 pajapandurovic60@gmail.com	pajapandurovic60@gmail.com	Paja
vnd.android.cursor.item/phone_v2 +381 64 5956081	+381 64 5956081	Danilo Jezerkic Jeza
vnd.android.cursor.item/phone_v2 +381645956081	+381645956081	Danilo Jezerkic Jeza
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 874852	+381 65 874852	Nikolina +381 65
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

POZIVI

+381643814567 Paja	2023-02-23 10:01:55	2023-02-23 10:01:55	Outgoing
+381643814567 Paja	2023-02-22 12:03:37	2023-02-22 12:03:37	Outgoing
+381643814567 Paja	2023-02-22 12:03:52	2023-02-22 12:03:52	Incoming
+381643814567 Paja	2023-02-22 12:03:46	2023-02-22 12:03:46	Incoming

from_id	to_id	start_date	end_date	direction	name
---------	-------	------------	----------	-----------	------

PORUKE

2023-02-22 11:04:07 11:04:07	1	Received	+381643814567 Ej sta je bilo	1 0	2023-02-22
2023-02-22 11:04:49 Sent	12	5	+381 64 3814567 Ma Nikolina me zove do grada, pa da proverim da li tece	1	
dogovor nas sa Jezom?	0				
2023-02-22 11:05:00 11:05:00	13	5	+381643814567 E pa treba ti da mu se javis	1	2023-02-22
2023-02-22 11:05:21 11:05:21	14	5	+381643814567 Tj. da mu javis informacije	1	2023-02-22
2023-02-22 11:05:47 11:05:47	15	5	+381643814567 Ja cu brzo zavrsiti sa ovim, pa ti	1	2023-02-22
saljem sta da mu posaljes	0				
2023-02-23 08:54:47 08:54:47	20	5	+381643814567 Prebacio sam ti jedan fajl na komp, to	1	2023-02-23
probaj da posaljes Jezi. Tu se sve nalazi	0				
2023-02-23 08:54:48 08:54:48	21	5	+381643814567 Prebacio sam ti jedan fajl na komp, to	1	2023-02-23
probaj da posaljes Jezi. Tu se sve nalazi	0				
2023-02-23 08:55:02 Sent	22	5	+381 64 3814567 E vazi. Saljem mu odmah	0	1
2023-02-23 09:02:28 Sent	23	5	+381 64 3814567 Samo da ti javim da je reseno sve. Bice veceras zavrseno sve	0	1

2023-02-23 14:02:45 24 5 +381 64 3814567 1
 Sent Jeza mi javio da su njegovi momci uhvaci. Sta cemo sada?
 0
 2023-02-23 14:03:23 25 5 +381643814567 1 2023-02-23
 14:03:23 1 Received Ajao 0
 2023-02-23 14:03:36 26 5 +381643814567 1 2023-02-23
 14:03:36 1 Received Cekaj smislicemo nesto 0
 2023-02-25 13:17:21 27 5 +381643814567 1 2023-02-25
 13:17:21 1 Received Spremaj se Dudo. Idemo za Maroko
 0

0	0	1677065380000	1677064200551	-1	0	Cao	0	0
0	7							
0	0	1677064210730	0	1677065391000	0	Cao Jezo		
0	0	0	8					
0	0	1677064249651	0	1677065429000	0	Sta se		
radi?	0	0	9					
we punom parom	0	0	1677065457000	1677064277475	-1	0	Evo radi	
	0	0	1677065493000	1677064313101	-1	0	Ti	0
	0	0	11					
	0	0	1677064314477	0	1677065494000	0	Ahha,	
lepo lepo	0	0	0	12				
	0	0	1677064342761	0	1677065523000	0	Pa I ja	
isto, evo sa Pajom dogovaram oko naseg posla zajednickog					0	0		
	13							
	0	0	1677065536000	1677064356182	-1	0	O lepe	
vesti	0	0	0	14				
	0	0	1677065565000	1677064385057	-1	0	Zna li se	
kakva informacija?	0	0	0	15				
	0	0	1677064405030	0	1677065585000	0	E bice,	
kaze Paja da je saznao nesto oko polazaka ove ture pa ti javlja detalje					0			
	0	0	16					
	0	0	1677064419927	0	1677065600000	0	Naravno	
mislim da ce to on na svoj specijalan nacin					0	0	17	
	0	0	1677064430006	0	1677065610000	0	Pa ti ja	
saljem te dokumente uskoro	0	0	0	18				
	0	0	1677065637000	1677064457762	-1	0	Super	
💰 💰	0	0	0	19				
	0	0	1677065697000	1677064517266	-1	0	Bez brige	
moj roki ce to protumaciti	0	0	0	20				
	0	0	1677064544877	0	1677065725000	0	E super	
😊	0	0	0	21				
	0	0	1677064600717	0	1677065781000	0	Nista	
javim ti ja cim saznam vise	0	0	0	22				
	0	0	1677064607082	0	1677065787000	0	Budi u	
pripravnosti	0	0	0	23				
	0	0	1677065794000	1677064614247	-1	0	Vazi	0
	0	0	24					
	0	0	1677064892609	0	1677142698000	0	Cao Jezo,	
evo saljem ti informacije po dogovoru. Valjda cete uspeti da se snadjete.					0			
	0	0	25					
	0	0	1677064897484	1677065069167	1677142860000	9		
knjiga.txt	0	0	0	26				

0	0	1677064916351	0	1677142707000	0	Paja je
primenjivao	ono	standard	kao	I	do	sad
0	0	1677064934298	0	1677142725000	0	Ti mozes
isto	uraditi	I	za	povratak	0	28
0	0	1677064941244	0	1677142732000	0	Cist
racun	duga	ljubav	0	0	29	
0	0	1677142766000	1677064975559	-1	0	OO super
0	0	0	30			
0	0	1677142784000	1677064993383	-1	0	Sada ce
to	moj	Roki	da	resi	0	31
0	0	1677142801000	1677065010888	-1	0	Javljam
kako	je	proslo	0	0	32	
0	0	1677065015314	0	1677142806000	0	Vazi 0
0	0	33				
0	0	1677142895000	1677065104339	-1	0	E
pronasli	sмо	sve	informaicje.	Ocekujte	lovu	veceras
34						\$ 0 0
0	0	1677065117270	0	1677142908000	0	Super 😊
0	0	0	35			
0	0	1677160874000	1677065349784	-1	0	Dudo
imamo	problem					
Moj	momci	su	pali	0	0	36

8	1758531046816034069	1758437231447652639	"Pavle Pandurovic"
<pajapandurovic60@gmail.com>	"Dusanka Svilarevic"		
<dudasvilarevic60@gmail.com>			
"Bogoljub Gagic" <cercilgagic60@gmail.com>			
1677065890000	1677065894053	Re: Sastanak	Pozdrav, Odgovara i
meni.	Paja	1	1
0	0	0	0
		0	-1
			0

<https://mail.google.com/mail/?extsrc=sync&client=g&plid=ACUX6DOoJjU-LvBBRU7PLtbXeOhXDVsLjHYnbLM> 0 0 0 0

Pajo evo moje karte. Istampaj i skinji.

----- Forwarded message -----
Од: <rdc01z+8wu62vn3pz8tc@guerrillamail.com>
Date: пет, 24. феб 2023. у 13:31
Subject: Online tickets
To: dudasvilarevic60@gmail.com <dudasvilarevic60@gmail.com>

Dear Dušanka,

We are sending you tickets for the destination Belgrade - Casablanca.

Please do not reply to this email, as it is automatically generated.

Have a nice trip,
Air Serbia

Sent using Guerrillamail.com
Block or report abuse:
<https://www.guerrillamail.com//abuse/?a=RVRwBB4WSrgUmgui%2BX1JIjTAQMuz3p1TyKk%3D>

Evo i tvoje karte.

----- Forwarded message -----
Od: <rdc01z+8wu62vn3pz8tc@guerrillamail.com>
Date: пет, 24. феб 2023. у 13:33
Subject: Online ticket
To: dudasvilarevic60@gmail.com <dudasvilarevic60@gmail.com>

Dear Dušanka,

We are sending you tickets for the destination Belgrade - Casablanca.

Please do not reply to this email, as it is automatically generated.

Have a nice trip,
Air Serbia

3.

Naziv dokumenta: PavleKarta.pdf i DudaKarta.pdf
Kompanija: AirSERBIA
Na cije ime glasi karta: Pavle Pandurovic i Dusanka Svilarevic
Destinacija: Beograd RS - Casablanca MA
Datum i vrijeme: 27.02.2023 11:30 - 27.02.2023 14:30
Format dokumenta: application/pdf

4.

air serbia
letovi za kazablanku
letovi za kazablanku air serbia

https://www.airserbia.com/sr_latin/

<https://www.google.com/search?client=opera&hs=7mF&sxsrf=AJOqlzUcVHbN4tMinK5Cd5nvqdMKSTR39w%3A1677238354301&q=letovi+za+kazablanku+air+serbia&oq=letovi+za+kazablanku+air+serbia&aqs=heirloom-srp..>

Program name: Opera

Авионска карта Павла Пандуровића:

IME / FIRST NAME	PREZIME / LAST NAME	LET IZ – LET ZA / FLIGHT FROM – FLIGHT TO	AirSERBIA
Pavle	Pandurović	Beograd RS – Casablanca MA	
POLAZAK / DEPARTURE	DATUM / DATE	VРЕМЕ / TIME	
BEG	27.02.2023.	11:30	
DOLAZAK / ARRIVAL	DATUM / DATE	VРЕМЕ / TIME	
CMN	27.02.2023.	14:30	
MEĐUSLETANJA / INTERMEDIATE LANDINGS			
AERODROMI / AIRPORTS	BEG – Nikola Tesla Aerodrom (Beograd, Srbija) / Nikola Tesla Airport (Belgrade, Serbia)		
	CMN – Mohamed V International Airport (Casablanca, Maroko) / Mohamed V International Airport (Casablanca, Marokan)		
PROLAZ / GATE	B-15	VРЕМЕ / UVRCAVANJA / BOARDING TIME	10:50
SEDIŠTE / SEAT	18 F	USLUGE / SERVICES	Odrasli, Ekonomski klasa / Adults, Economy class
REG. BROJ / RE. NUMBER	2548-7856-9846		
CENA / PRICE	35100,00 RSD / 300 EUR		
KOD / CODE			
MANIFESTA / Manifest	Manifestačna karata sačinjena na osnovu 1. marta 2023.		

Прилог 4: Информације о историји претраге као и информације о претраживачу

hotel caxablana
 ADDRESS Hotel Casablanca
 ADDRESS Hotel Casablanca booking
 Turisticka agencija kazablanka
 kazablanka maroko google maps

https://www.booking.com/hotel/ma/address-casablanca.en-gb.html?account_created=1#map_closed

program: Firefox
 domain: google.com

24.02.2023. i 25.02.2023.

Прилог 5: Video Cleaner параметри и слике

TOOLS (Denoise is SLOW)			
Apply TOOLS settings (0=no)	0	1	1
UnSharpen Strength (0=off)	0	50	17
Sharpening Strength (0=off)	-25	50	0
Video Contrast Strength (0=off)	-10	20	7
Color Contrast Strength (0=off)	-10	20	0
Color Saturation Strength (0=off)	-10	20	0
Suppress HotSpot Strength (0=off)	-5	9	0
Shift Overall Hue (0=off)	-99	99	3
Equalizer Strength (0=off)	-15	15	0
Backlight / Off / Histogram (0)	-1	1	1
Deblur / Off / Denoise (0=Off)	-1	3	1
Stabilize Strength (0=off)	0	3	0
Focus Correction Strength (0=off)	0	20	0
Deblock Model (0=off)	0	9	0
Deblock Strength (0=lowest)	0	30	0

Видео 1:

Slika 1 (Frame 168) :

- Tools 1
- Histogram 1

Slika 2 (Frame 168) :

- Color Contrast 15

Видљиве таблице су BG 407 965.



Видео 2:

Slika 1 (Frame 40):

- Tools 1
- Equalizer 15

Slika 2 (Frame 72):

- Tools 1
- Equalizer 15

Слика са другог снимка на којој се могу видети препознатљива лица:

