

**Univerzita sv. Cyrila a Metoda v Trnave**

## **Hacking študenta**

Denis Németh

# Obsah

|                                                                |    |
|----------------------------------------------------------------|----|
| Obsah .....                                                    | 1  |
| Odborný príspevok .....                                        | 2  |
| Prípad.....                                                    | 9  |
| Prezentácia .....                                              | 9  |
| .....                                                          | 9  |
| 5WH(6) .....                                                   | 9  |
| Hypotézy + výsledky hypotéz + softvérové nástroje .....        | 10 |
| Analýza a overenie, vysvetlenie hypotéz .....                  | 11 |
| Bezpečnostné opatrenia .....                                   | 22 |
| Zaistenie dôkazov z USB zariadení Kingston DTR30G2 .....       | 22 |
| Chain of custody .....                                         | 22 |
| Dáta .....                                                     | 22 |
| Analýza log reportov, artefaktov z image RAM, VirtualBox ..... | 22 |
| Prečo .....                                                    | 22 |
| Image VirtualBox zariadení .....                               | 22 |

# Odborný príspevok

Zdroj: [https://www.youtube.com/watch?v=x\\_LVxSkHMTI](https://www.youtube.com/watch?v=x_LVxSkHMTI)

Používateľ “**SeanLikesTech**” na YouTube zamaskoval edukačné video na propagáciu škodlivého open source software **FTK Imager 3.1.2.0**. Edukačné video by malo poskytnúť informáciu, ako používatelia môžu porovnávať **MD5** a **SHA5** hash hodnoty dvoch USB kľúčov, avšak všetko cez **User Account Control: Unknown publisher** softvér. Softvér má prístup k pevnému disku počítaču a nemá podpisovací hashovací algoritmus **sha256RSA**, taktiež nemá **verejný kľúč RSA(4096 bits)** s parametrom **0500** a nemá vydavateľa **DigiCert Trusted G4 Code Signing RSA 4096 SHA384 2021 CA 1** s platnosťou od **9.6.2021** do **14.6.2024**. Nebola uvedená validná verzia softvéru **V3** a ani držiteľ **Exterro, Inc (CN), Exterro, Inc (O), L=Beaverton, S=Oregon, C=US**. “SeanLikesTech” uviedol konkrétne postupy porovnávaní dvoch hash hodnôt USB kľúčov: **Add Evidence Item ... > Logical Drive > C:\-[NTFS], E:\-USB-1[FAT] > [unallocated space] , [root]>C4Pri04>Hashtest.txt>Export File hash**

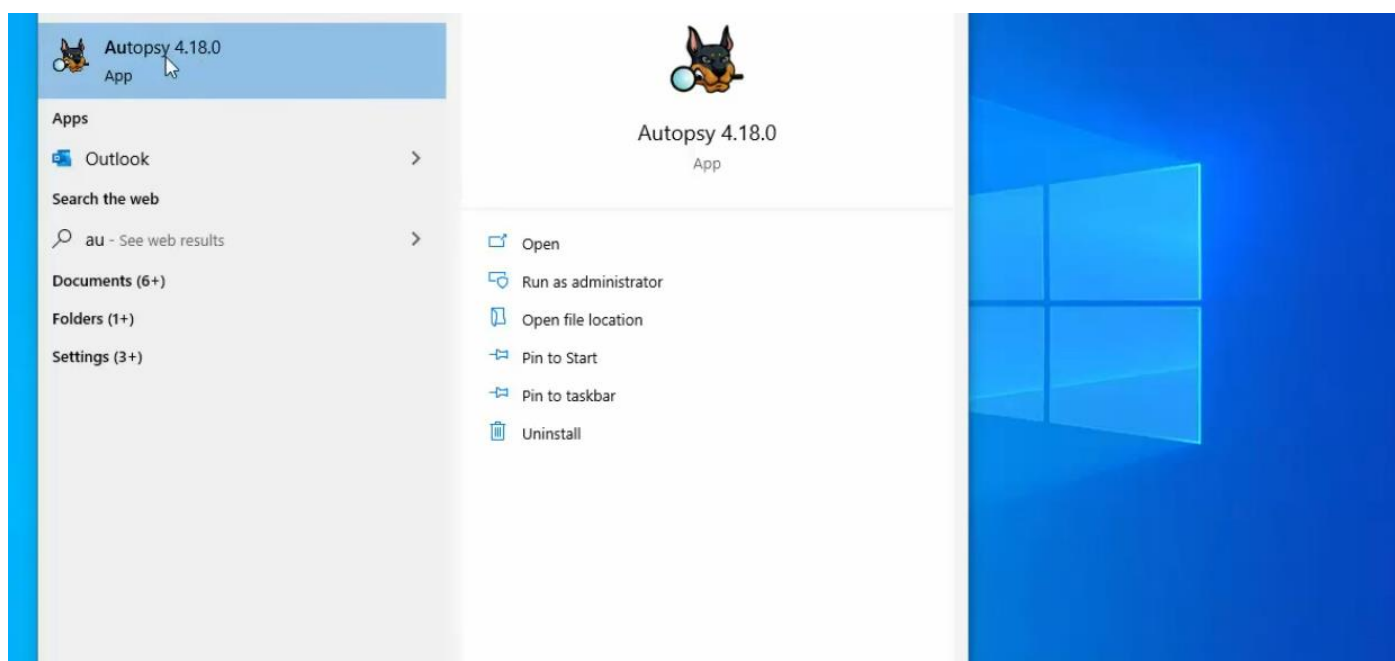
Pointa spočívala v tom, že YouTube používateľ chcel nabádať edukačným videom používateľov na stiahnutie škodlivého softvéru, čo má prístup k súborovému systému **C:\-NTFS** a k **pevnému disku** počítaču. Všetko **bez verejného kľúča , bez digitálneho podpisu, bez digitálneho certifikátu, bez sha256RSA**. Softvér **FTK Imager 3.1.2.0** je zdrojom na **SSH port forwarding** so **synchronizáciou** a na únik údajov, napriek tomu, že edukačné video by mal slúžiť na poskytnutie informácii sľedovateľom ako predísť takýmto útokom.

(používateľ video následne aj **zmazal..**)

Vyriešime *identifikáciu útokov na zariadenie* pomocou *kompromitovaných zariadení a sieťových nastavení*, identifikujeme *sociálne inžinierstvo v sociálnych mediách*, *zaistíme všetky dôkazy* a *identifikujeme útoky aj počas zaistenia dôkazov na útoky*:

Na kontrolu prístupu k pevnému disku sa použije softvér ako napr.

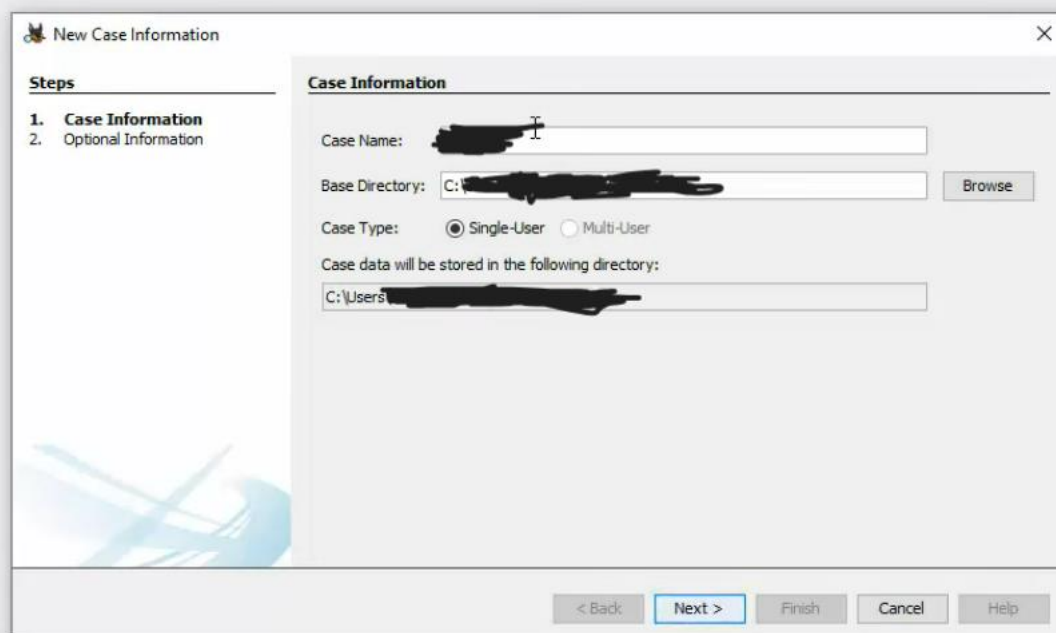
### *Autopsy 4.18.0.*



Analýza bude realizovaná na lokálnom *pevnom disku*. Uvedieme kroky:



Vytvoríme *image súbor* pevného disku a analýza dát sa vykonáva na *kópii*.



*Next >*

**New Case Information**

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number: [Redacted]

Examiner

Name: [Redacted]

Phone: [Redacted]

Email: [Redacted]

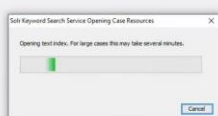
Notes: [Redacted]

Organization

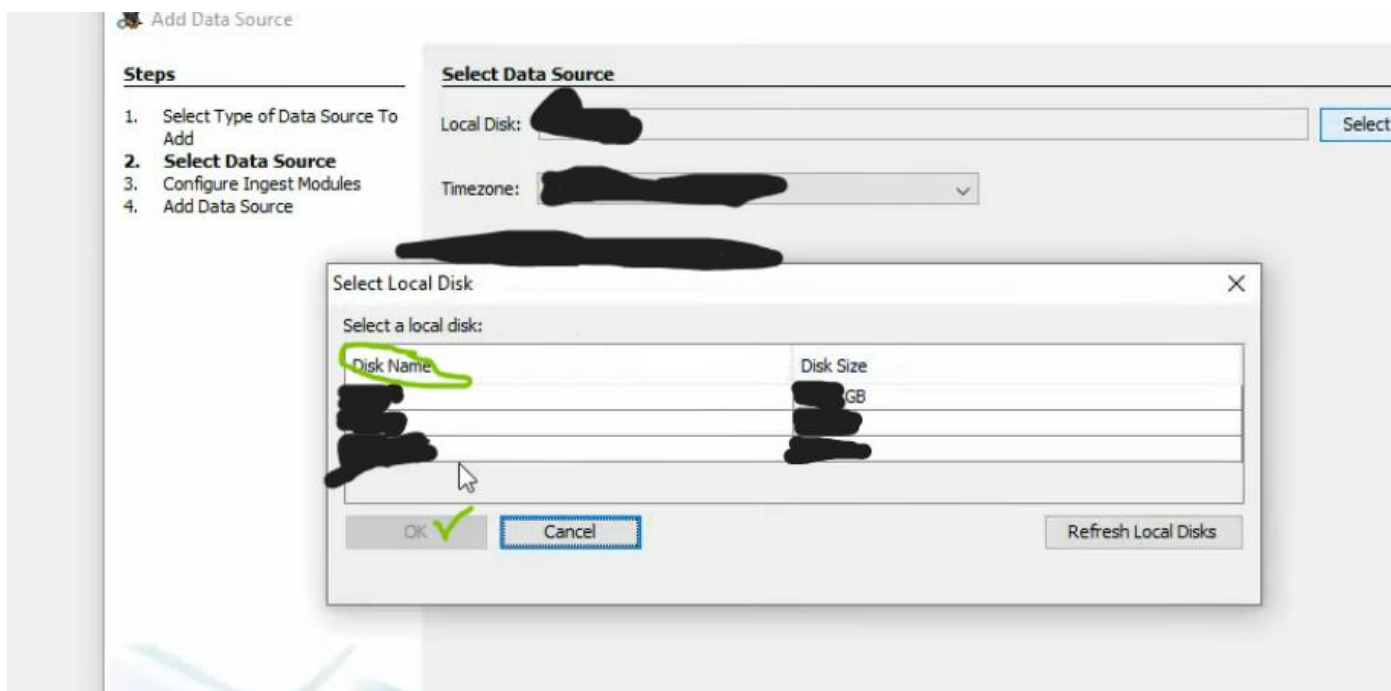
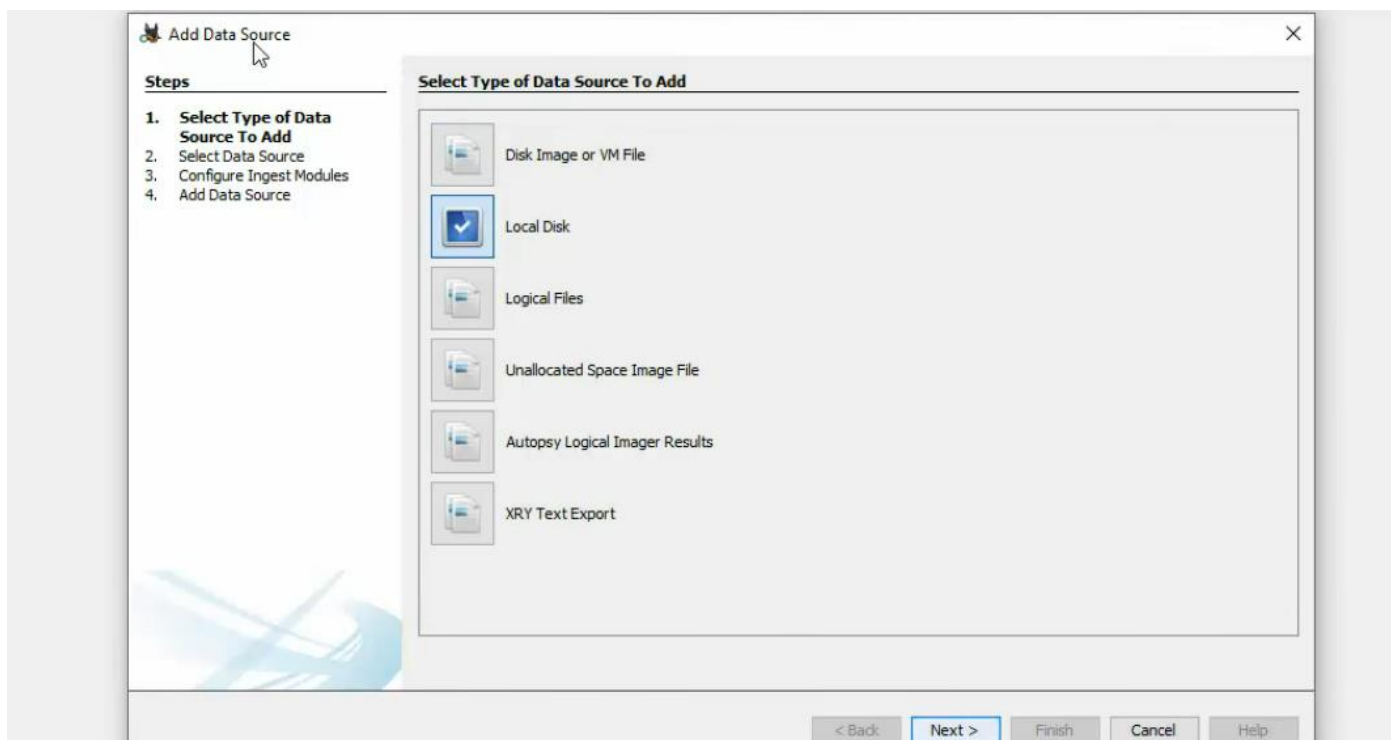
Organization analysis is being done for: [Redacted] [Redacted]

< Back Next > **Finish** Cancel Help

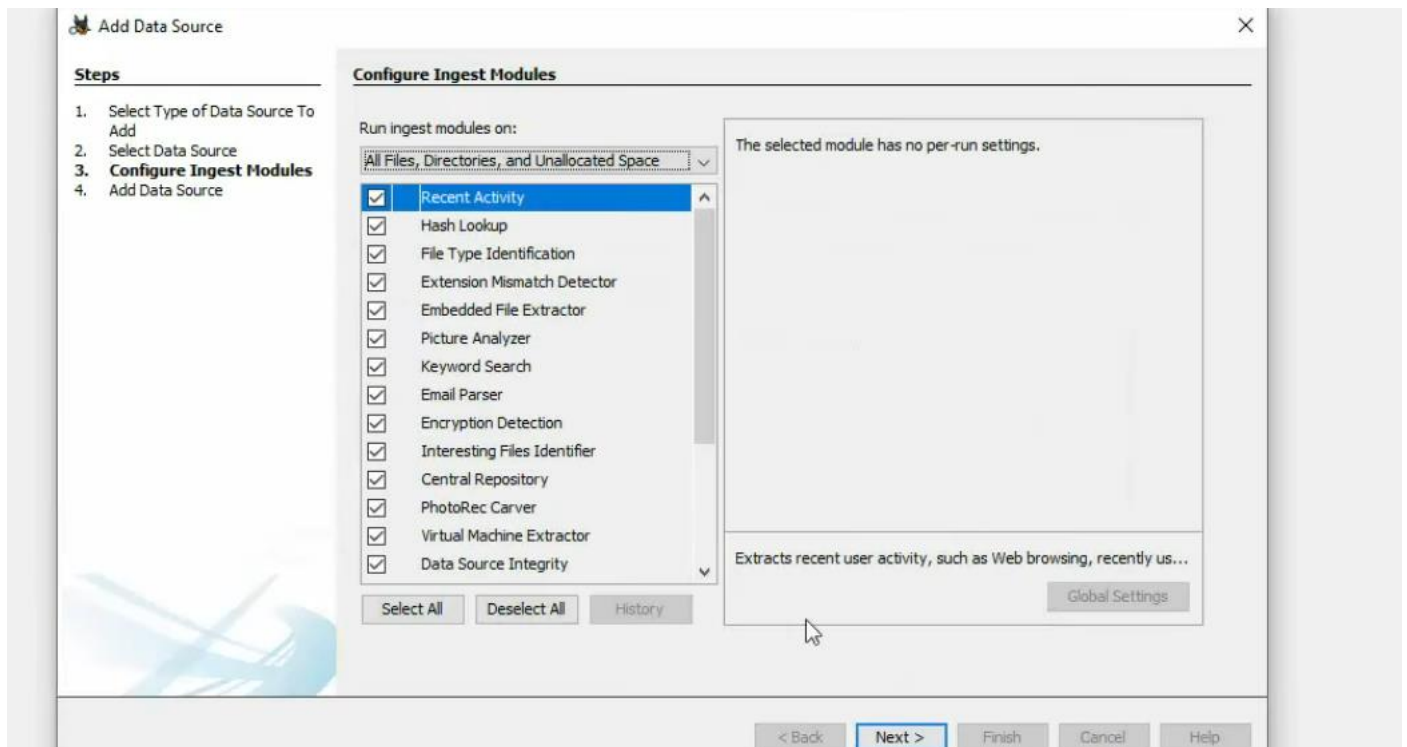
Treba zadať **Case Number** a **Name**. *Phone, Email, Notes, Organization* sú **nepovinné**.



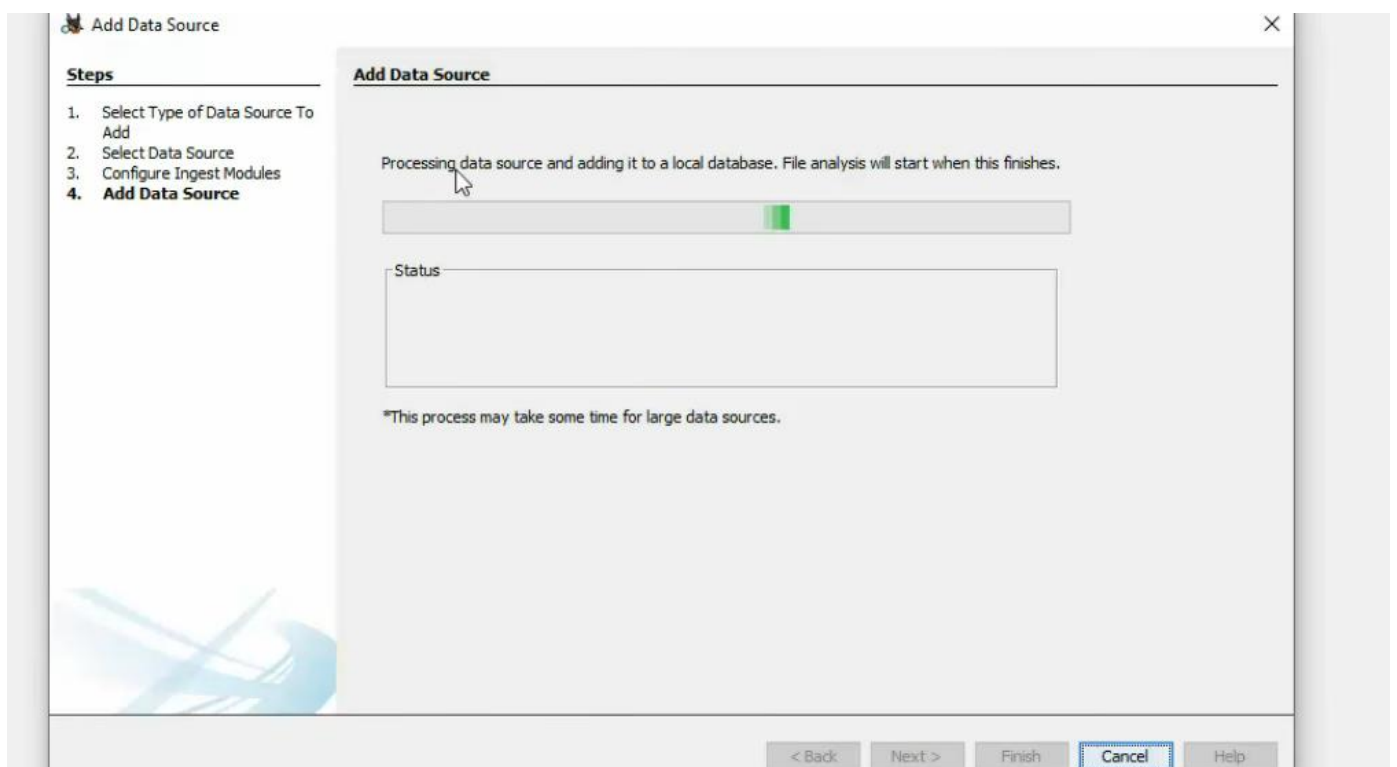
Po vytváraní Case prípadu sa zobrazí **Add Data Source** dialogBox, čo môže byť napr. **Image File** alebo **Local Hard Disk Drive**. Klikneme **Next>**

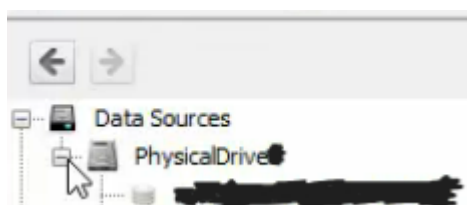
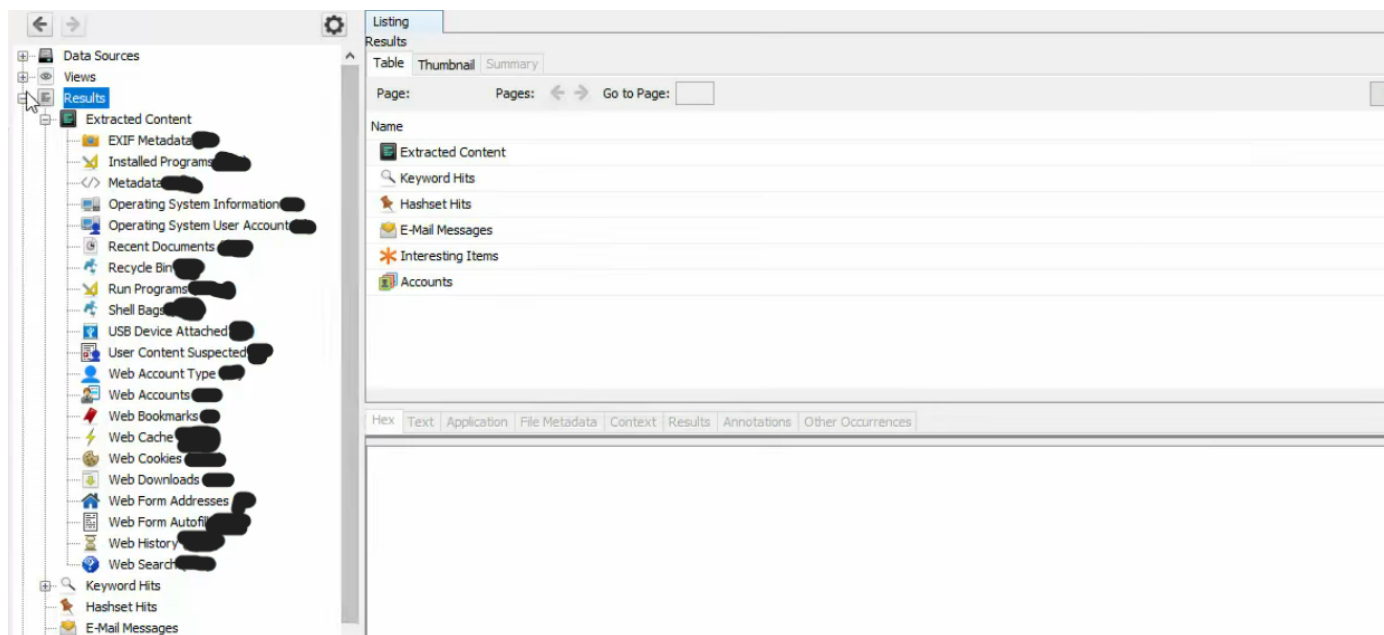


Vyberieme disk. Klikneme Ok.



*Next>*





Vyberieme si **disk**, pretože veľa útokov zničí výdrž **batérie** zariadenia napr., a každý softvér má prístup k **pevnému disku** počítaču, teda napr. **exploit útoky na port forwardingy** musíme hľadať tam. Nehľadáme cez **Installed Programs!** pretože škodlivé softvéry práve chcú **zbierať informácie** o tom, čo máme my na zariadení a to není úloha, úloha je identifikovať prístup softvérov na diery, a to ide **cez pevný disk (lokátor pevného disku so zneužitím prístupových pravidiel pomocou SSH)**.

Softvéry **Unknown Publisher**, čo aj zmaže videá chcú **extrahovať** údaje o zariadení ako: **Installed Programs, OS User ACCOUNT, Recent Documents**-kradnutie dokumentov cez **port forwardingy, open port ssh connect, Run Programs** a nainštalované, doinštalované **Shell bagy** a pod. My by sme práve mali **tie údaje držať private a neposkytnúť to softvérom nikdy**. (lebo môže sa stať, že autor videa po identifikovaní útoku video náhle zmaže)

My musíme hľadať **zmeny na pevnom disku**, škodlivé softvéry fungujú skôr ako “**server**” na **zber** čo najviac informácii o zariadení, ako **konkrétny model USB drive-u**, teda **poskytnúť tie údaje priamo útočníkom** je **podľahnutie sociálnemu inžinierstvu**. (NEposkytujem!, ak vidím tam útok, inak defakto súhlasím s tým, že niekto ma snaží hacknúť aj napriek tomu, že viem o tom, teda NESúhlasím.))

Veľa ľudí proste súhlasí, že ju/ho hacknú, preto je dôležité vzdelávať používateľov na **rozpoznanie útokov** ako sme si to robili vyššie a pokračujeme trošku konkrétnejšie, (cases nižšie)

*...Je dôležité vzdelávať používateľov pomocou odborných článkov, alebo zverejnených príspevkov, nesfalšovaných videotutoriálov.*

## Prípad

### Prezentácia

Prezentácia: <https://bcstudent.fpvucm.sk/~nemethdenis/dfa/prezentacia.pdf>

Nastal únik prihlasovacích údajov, neoprávenený prístup cez virtuálny stroj na zariadenie, únik dát, zmanipulovanie sieťových (perzistentných) rozhraní a neoprávený prístup k informácii aj počas samotného zaistovania informácii na USB zariadení pomocou softvéru **MagnetCatcher RAM Capture v1.2.0**.

### 5WH(6)

**Who (Kto)**- neznámy páchatelia, identifikovali sme aj používateľa pod menom “oerdnj” z GitHub fóru s kompromitovanými open source skriptovými aktualizáciami na server [www.ubuntu.com](http://www.ubuntu.com) s IP adresou 185.125.190.20, osobu identifikovanú pri úniku prihlasovacích údajov pod menom “Milada Janigová”, Apacer AS2280P4 1TB diskovú jednotku, páchatel’a man in the middle pri servri s IP adresou cez next hop 10.69.253.127 na server 185.125.190.26

**Where (Kde)** - **Ubuntu Server 16.04.7 LTS** , Kingston DTR30G2 USB Device

**When (Kedy)**- **24.2.2026, (aj hlásený incident)**

**What (Čo)** - neoprávnený prístup k zariadení, man-in-the-middle útoky, kompromitované nastavenia sieťových rozhraní, únik citlivých dát (prihlasovacie údaje, heslá). Poškodenie samotného počítača.

**Why( Prečo)**- odpočúvanie používateľa, získať citlivé údaje, poškodiť a znefunkčniť zariadenie ale aj používateľa (zdroj pod elektrickým vedením a poškodeným káblom)

**How (Ako)**- Pomocou zamaskovaných *perzistentných sieťových konfigurácií* za legítimných, pomocou *IPV6 autokonfigurácií* a presmerovaním sieťovej komunikácie cez *Ubuntu Server 16.04.7 LTS*, pomocou vzdialeného SSH prístupu na zariadenie cez *Debian(64-bit)*, pomocou získanie *prihlasovacích údajov na microsoft365* cloud účet cez

*word.cloud.microsoft/?wdOrigin=OFFICECOM-*

*WEB.APPBAR%2CAPPHOME-WEB.UNAUTH%CAPPHOME-*

*WEB.SHELL.SIGNIN* a pomocou *administratívnych prihlasovacích údajov*

získaných metódou *word.cloud.microsoft/?wdOrigin=OFFICECOM-*

*WEB.APPBAR%2CAPPHOME-WEB.UNAUTH%CAPPHOME-*

*WEB.SHELL.SIGNIN* a pomocou techník *sociálneho inžinierstva* (presvedčiť používateľa na stiahnutie kompromitovaných softvérov, sieťových nastavení)

## **Hypotézy + výsledky hypotéz + softvérové nástroje**

- 1) Používateľ zamaskoval *perzistentnú sieťovú konfiguráciu* za *legitímnu (verejnú adresu zamaskoval na privátnu)* na virtuálnom stroji *Ubuntu Server 16.04.7 LTS* a pomocou *zneužitia prihlasovacích údajov* získaných pomocou *word.cloud.microsoft/?wdOrigin=OFFICECOM-WEB.APPBAR%2CAPPHOME-WEB.UNAUTH%CAPPHOME-WEB.SHELL.SIGNIN* sa posnažil *odpočúvať používateľa (man-in-the-middle útok)* pri servri s IP adresou, ktorý *cez next hop 10.69.253.127* ide na server *185.125.190.26*. - *Potvrdená, aj priamo hlásená.*

2) Používateľ zdefinoval *sfaľované sieťové rozhranie* na USB zariadenie *Kingston DTR30G2 USB Device* pomocou *zneužitia administratívnych prihlasovacích údajov* a *poškodil už zaistené dôkazy na USB zariadení, komprimované súbory* na USB zariadení. - *Potvrdená, Apacer AS2280P4 1TB diskovú jednotku páchateľ priamo podchytená, aj hlásená.*

3) Používateľ pomocou *SuprHardenedWinVerifyCacheInsert* spôsobil *spustenie a únik zvukových súborov (natáčanie používateľa)* na virtuálnom zariadení *Debian(64-bit)*. - *Potvrdená, log súbory naznačujú o skutočný prístup k takýmto údajom cez sieť.*

## **Analýza a overenie, vysvetlenie hypotéz**

Na obrázku vidíme *poškodený kábel*, čo nechal za sebou páchateľ. Počítač bol *pod elektrickým vedením*, zapnutý do elektrického zdroja, čo na jednej strane je *poškodenie pôvodných dôkazov* na PC, na druhej strane je to *nebezpečenstvo pre používateľa*. Taktiež umiestnenie kábla sa podobá na *dial-up port bonding* techniku, čo sa používa *pri odpočúvaní a pri presmerovaní sieťovej komunikácii*. Môže sa jednať o *sociálne inžinierstvo*.

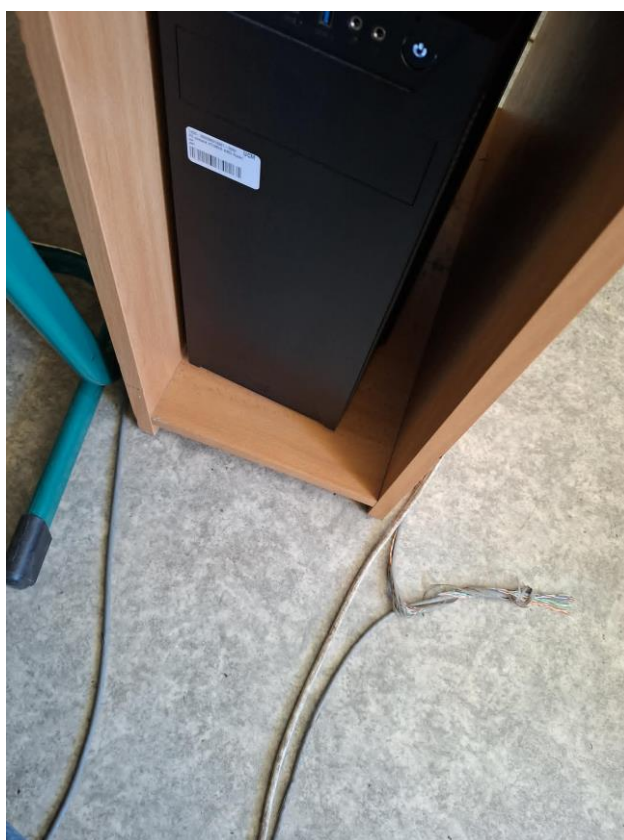


Fotka spravená dňa: **29.5.2026**

PC zostava ***HTONER AMD Ryzen 1000 – 000090010881 – 0000*** pod elektrickým vedením.



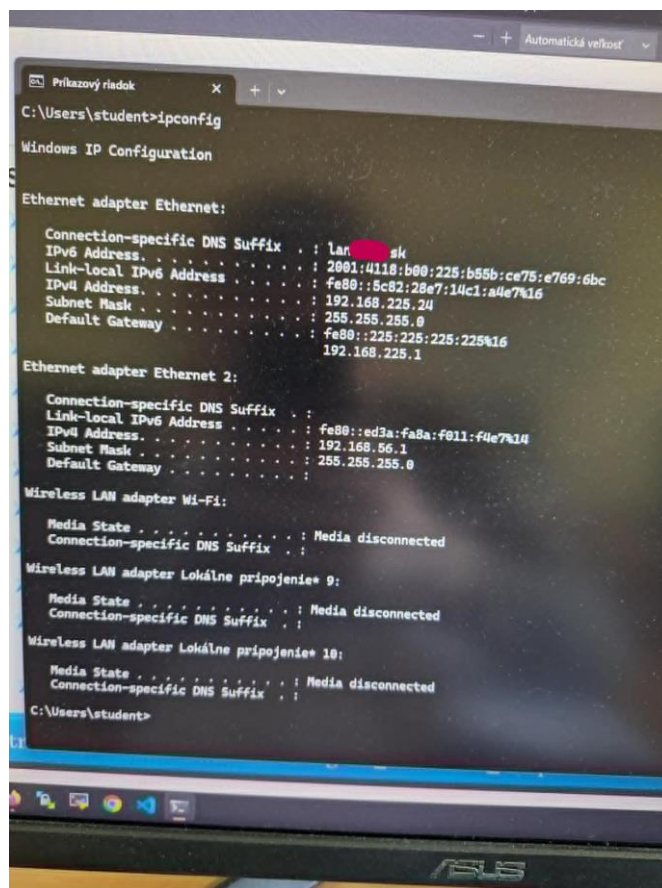
PC zostava **HTONER AMD Ryzen 1000 – 000090010881 – 0000** pod elektrickým vedením, avšak s poškodeným káblom.



Vzhľadom na situáciu, že počítač **HTONER AMD Ryzen 1000 – 000090010881 – 0000** obsahujúce dôkazy bol poškodený, vyskúšali sme vyriešiť dôvody z inej

PC (vid' obrázok) v rámci *chrbticovej siete v miestnosti (backbone sieť)*.

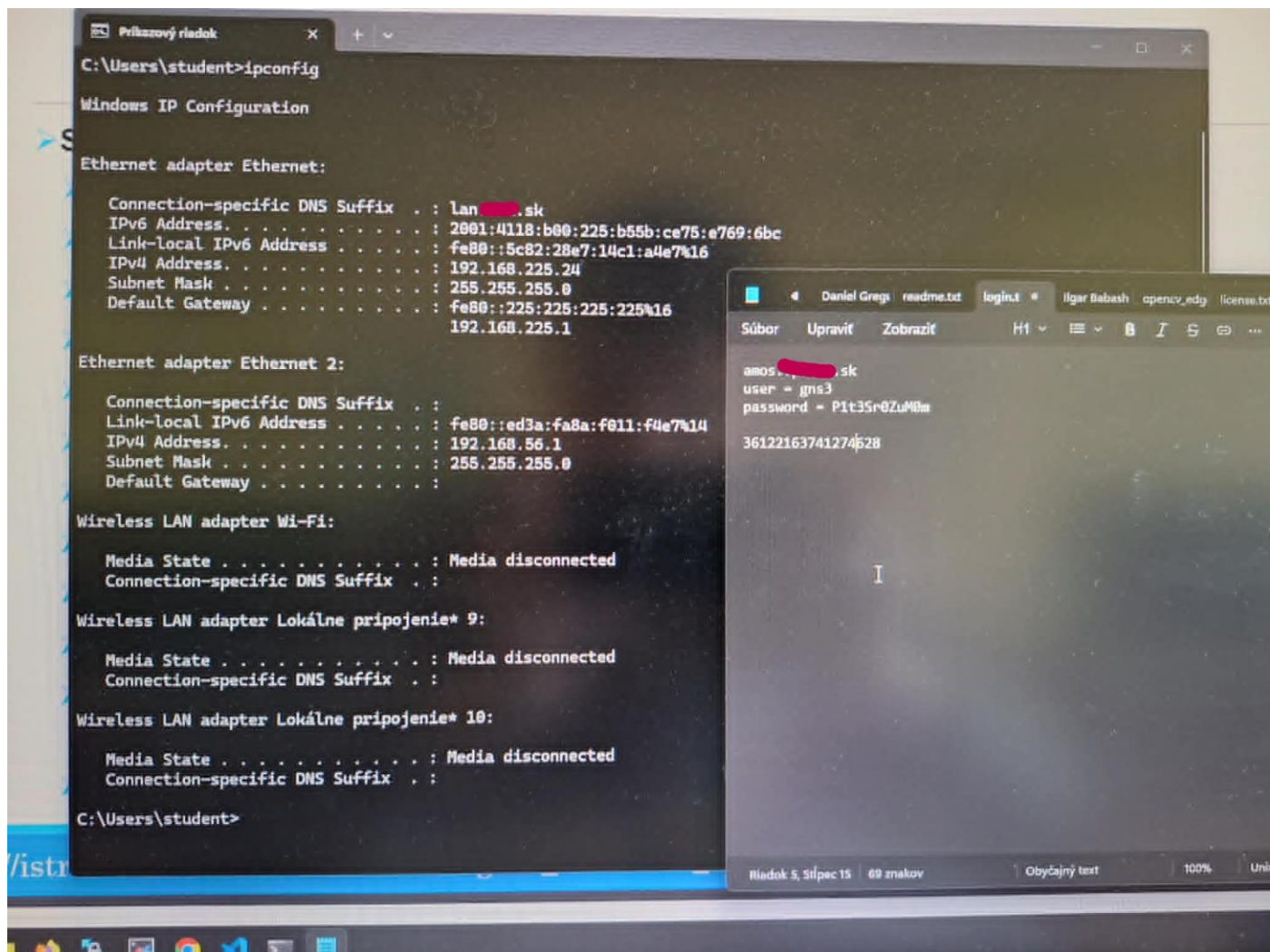
Dôvodom je to, že v rámci *sieťovej infraštruktúry* sa dajú nájsť *stopy útočníka a zdroje útokov*. Taktiež informácie o *sieťovom pripojení Ethernet*.



*Ethernet adapter 2* nemá *DNS Suffix* a *Default Gateway*, nemá konzistentne uvedenú špecifikáciu ako v prípade Ethernet adapter 1. Je to bezpečnostný problém, lebo odchádzanie sieťovej komunikácie z privátnej siete na Internet sa uskutoční cez *Default Gateway*. To znamená to, že sa môže nastať *dial-up sieťová konfigurácia, port bonding a odpočúvanie* najmä v prípadoch, keď máme cez centrálny administrátorský počítač nainštalované *virtuálne stroje (VirtualBox)*.

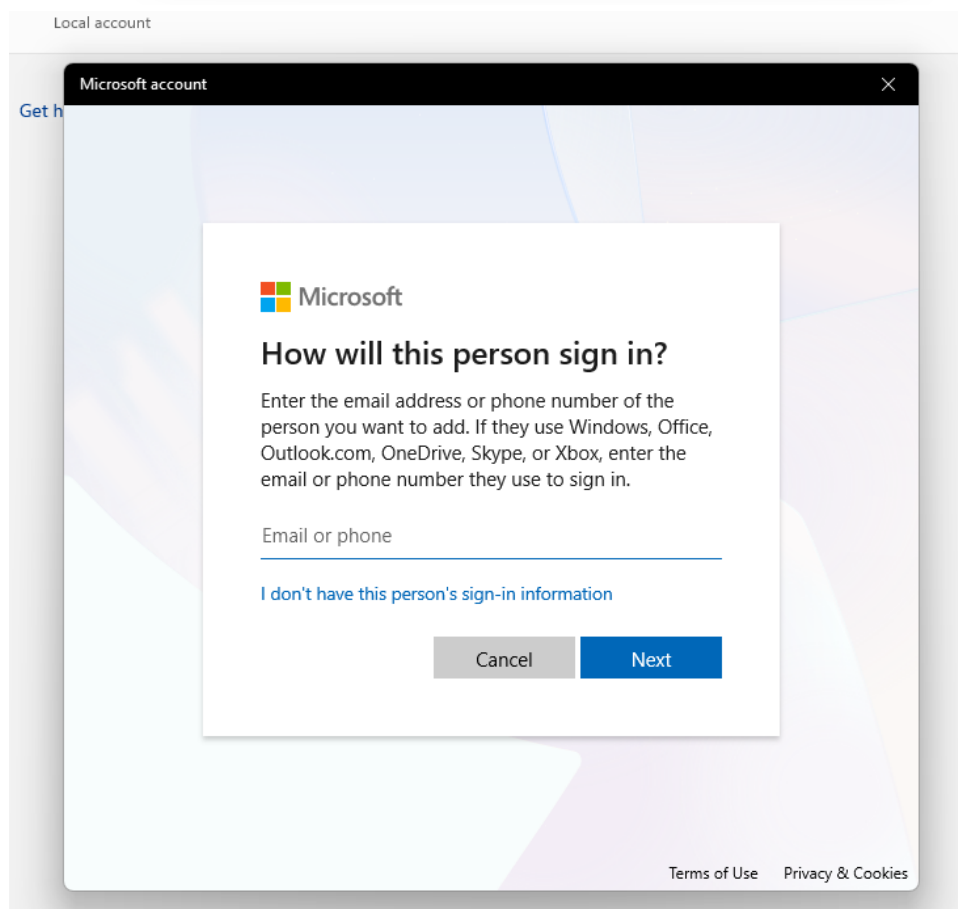
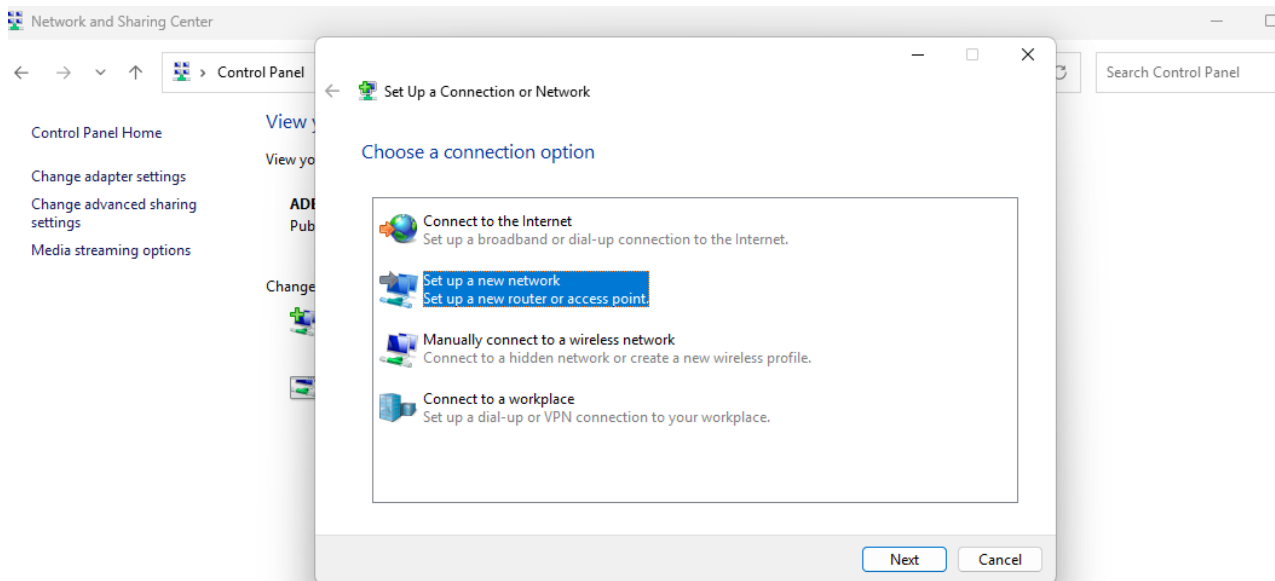
*Interné sociálne inžinierstvo* zahŕňa v sebe únik citlivých dát, ako *prihlasovacie údaje* na *Cloud server účty*, čo slúžia taktiež ako podklad na útoky cez *SSH*

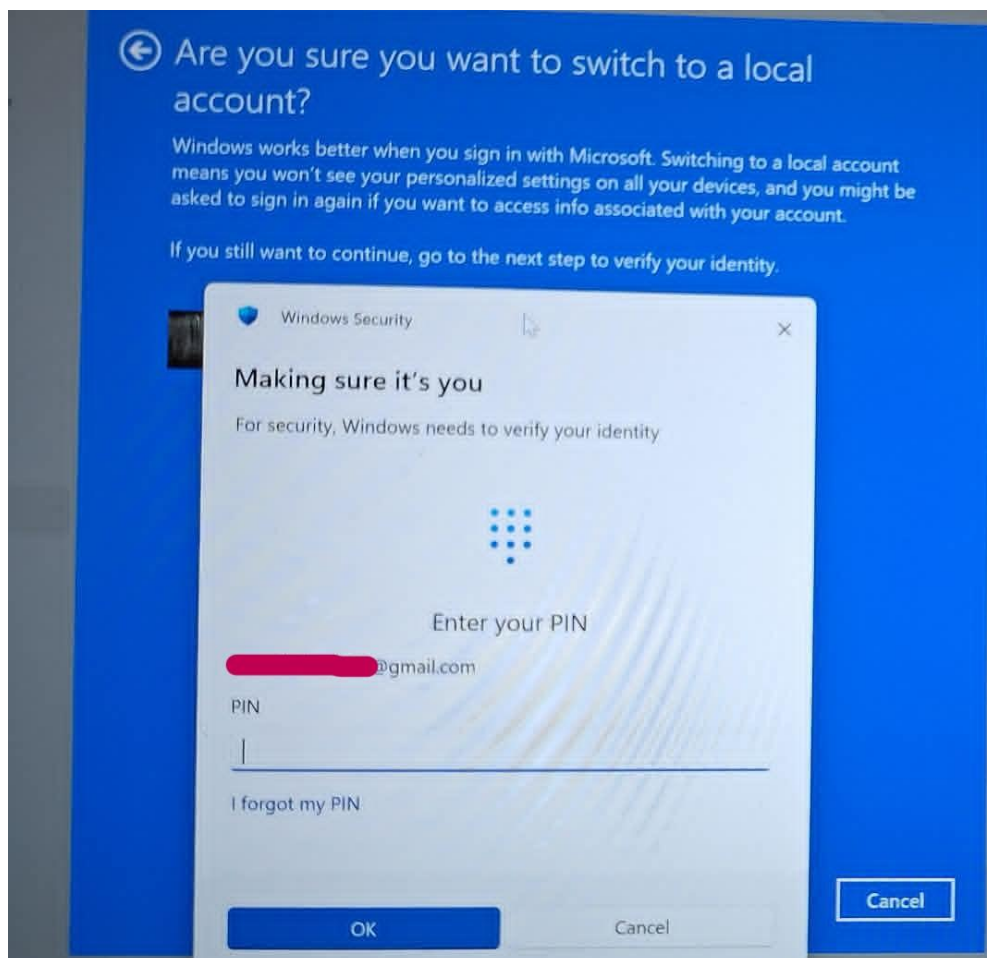
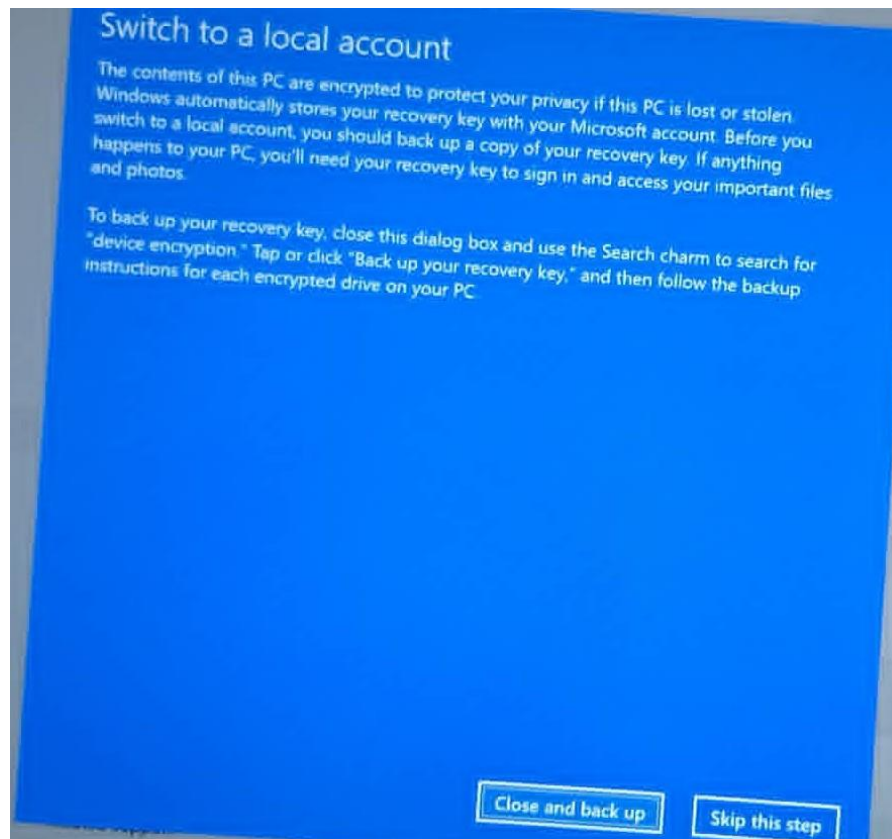
vzdialené prístupy, na *prenos údajov cez sieťové pripojenia VirtualBox*, najmä v prípadoch, keď ide o *Open Source* softvérovú distribúciu, lebo tieto verzie dokážu obísť bezpečnostné kontroly systému *Windows*. VirtualBox má prístup cez *hypervízor* k *HW* počítača Windows, čo už znamená prístup k *administrátorským právam počítača*, totiž spolu s *únikom prihlasovacích údajov a hesiel* (viď obrázok) zdrojové kódy Open Source softvérov vieme zmodifikovať tak, aby mali prístup ku “*Control Panel*”.



*Únik prihlasovacích údajov* sa dá zneužiť pri prihlásení používateľov cez *Control Panel* na server, navyše so *sudo* pravidlami + s nastaveniami takými, čo

spravia z ich **PC router/ server na prihlásenie viacerých používateľov cez synchronizovaný Cloud, SSH, IPV6 a získanými prihlasovacími údajmi.**





← Enter your local account info

Enter the user name and password for your new or existing local account. This is the account you'll use to sign in to Windows from now on.

If you want to continue to sign in to Windows with Windows Hello, you'll need to set up a password.

User name

New password

Confirm password

Password hint

Next Cancel

## Change sign-in settings

You can have assistive technologies start automatically when you sign in, after you sign in, or both. Select the check boxes for each option you'd like to use.

| Assistive Technology                                                         | At sign-in               | After sign-in            |
|------------------------------------------------------------------------------|--------------------------|--------------------------|
| Type without the keyboard (On-Screen Keyboard)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| Press keyboard shortcuts one key at a time ( <u>Sticky Keys</u> )            | <input type="checkbox"/> | <input type="checkbox"/> |
| If I press keys repeatedly, ignore extra presses (Filter Keys)               | <input type="checkbox"/> | <input type="checkbox"/> |
| Use the numeric keypad to move the mouse around the screen (Mouse Keys)      | <input type="checkbox"/> | <input type="checkbox"/> |
| Hear a tone when you press CAPS LOCK, NUM LOCK, or SCROLL LOCK (Toggle Keys) | <input type="checkbox"/> | <input type="checkbox"/> |
| Color Filtering (Settings)                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| Cursor indicator (Narrator)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| Live Captions (livecaptions)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| Speech Recognition (speechreco)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| Voice Access (Voice Access)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

### Touch and tablets

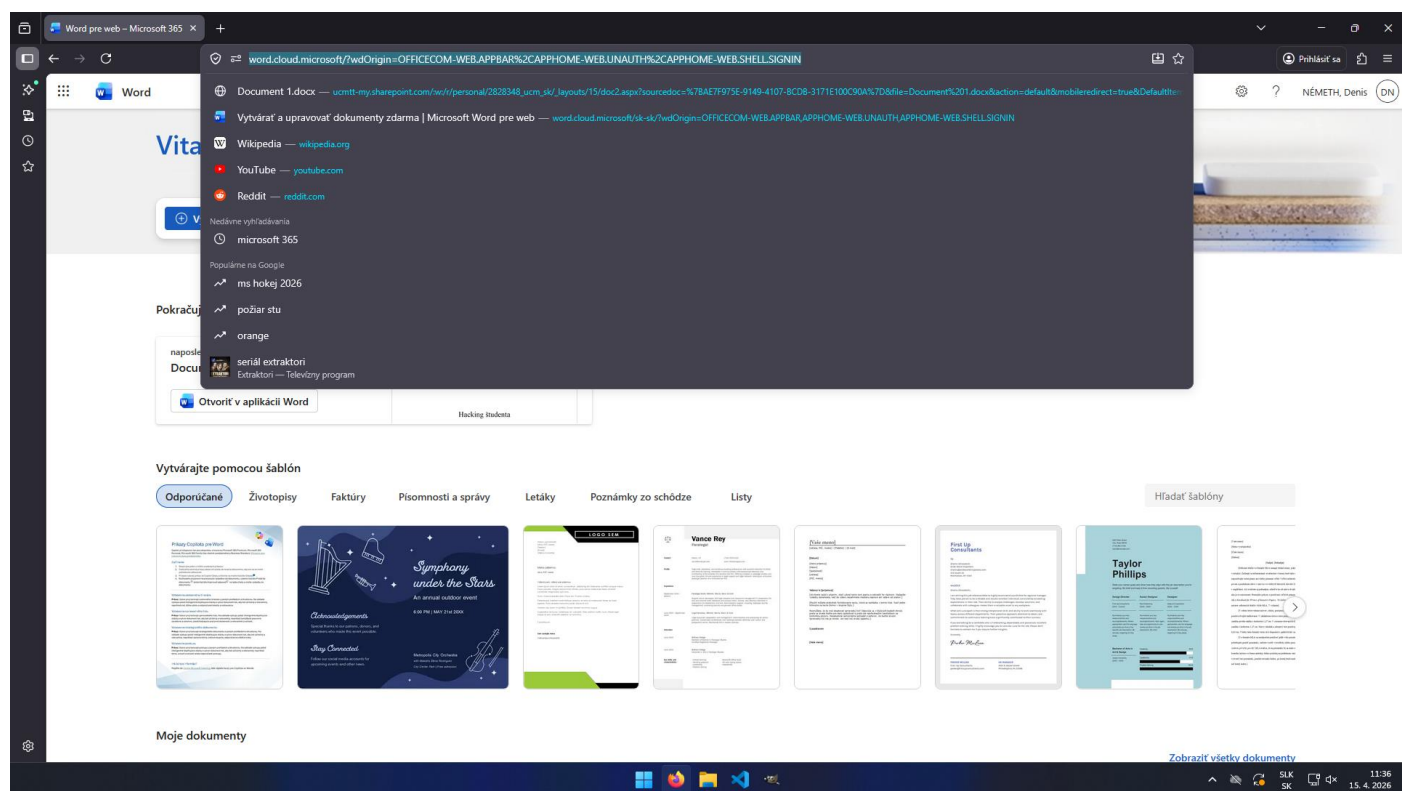
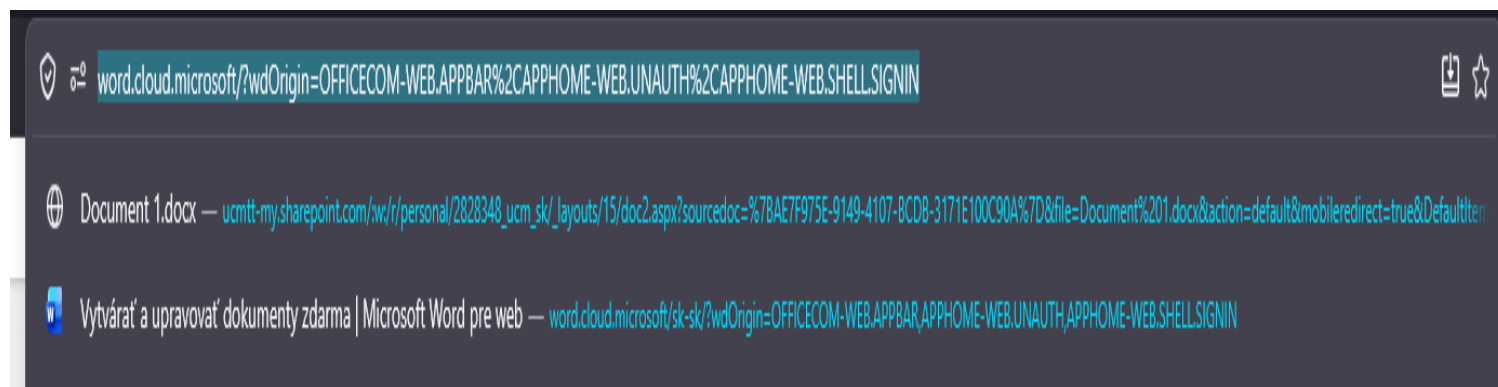
Pressing the Windows button and Volume Up button together on your tablet can start an accessibility tool. To change which tool launches when you press these buttons after you've signed in, go to the Make touch and tablets easier to use page.

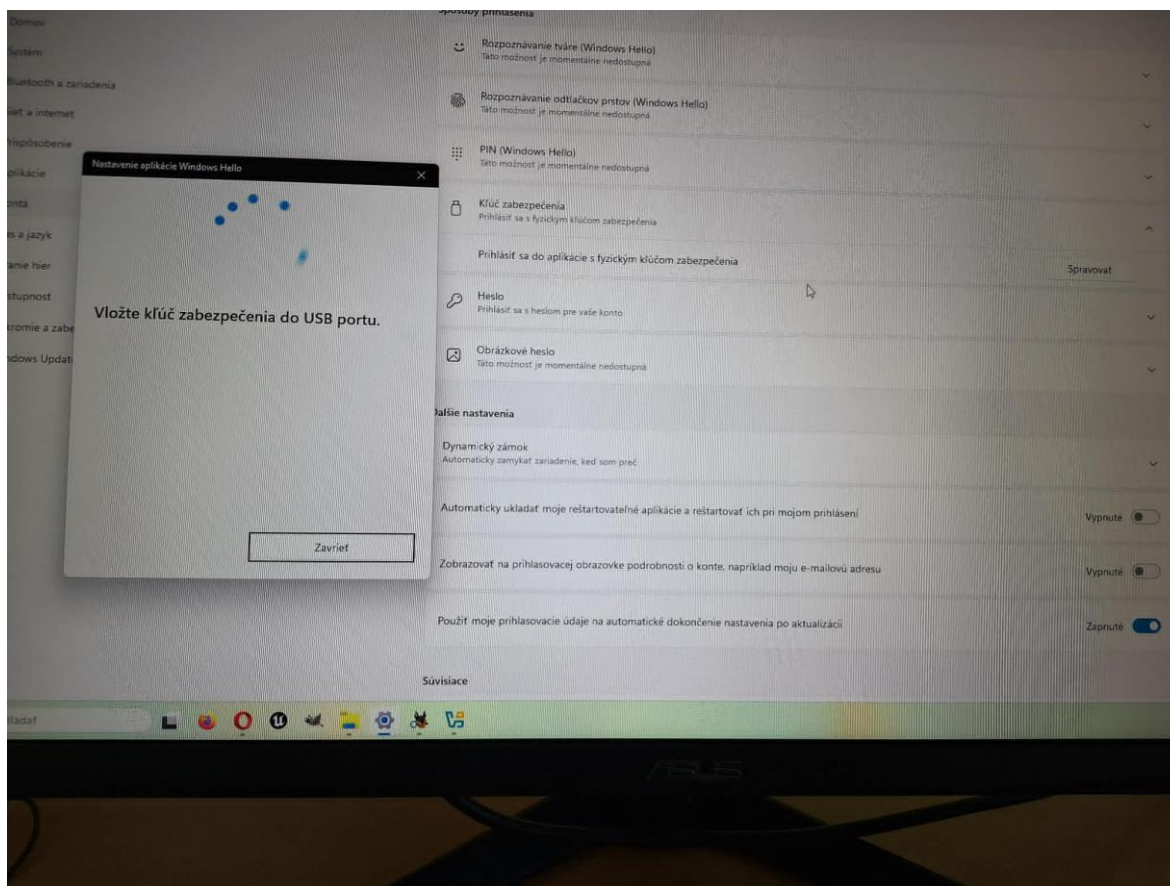
☐ Launch this tool from the sign-in screen

### See also

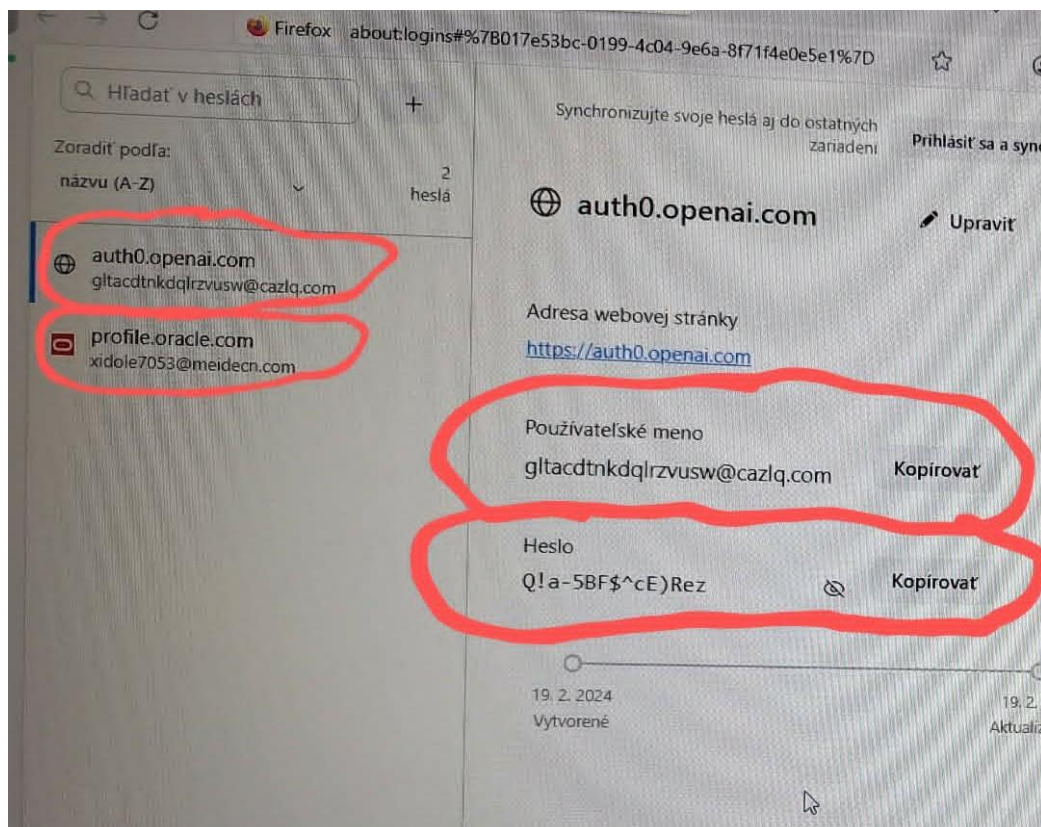
 [Create a restore point for backup](#)

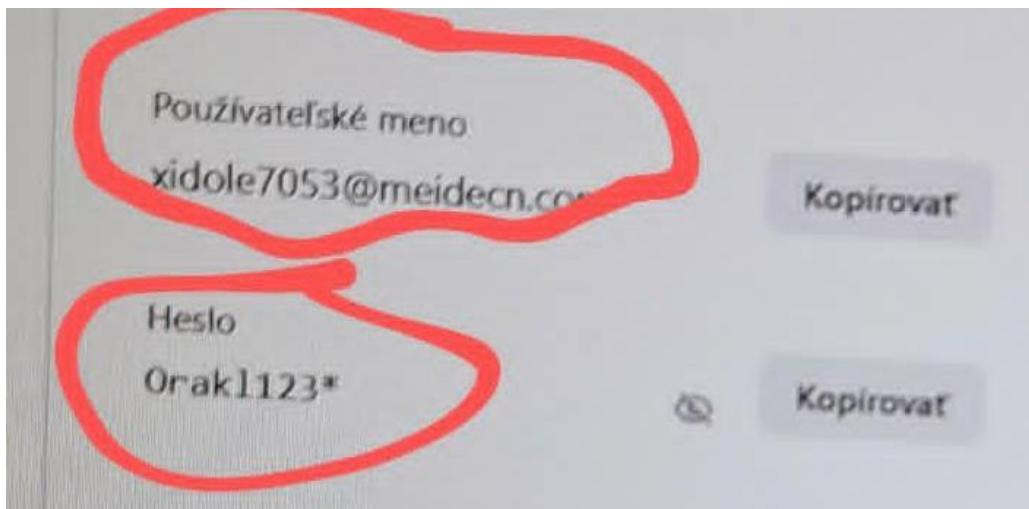
Presne tu na obrázku vidno **únik** a **útok** na **prihlasovacie údaje používateľ'a**, kde aj **po odhlásení z Microsoft365 účtu** je **celý účet aj d'alej prístupný** cez **word.cloud.microsoft/?wdOrigin=OFFICECOM-WEB.APPBAR%2CAPPHOME-WEB.UNAUTH%2CAPPHOME-WEB.SHELL.SIGNIN**. Ide o 100%-ný dôkaz, kde všetky prihlasovacie údaje na **Cloud server unikli**. Samozrejme cez “WEB.SHELL.SIGNIN” (obrázok)



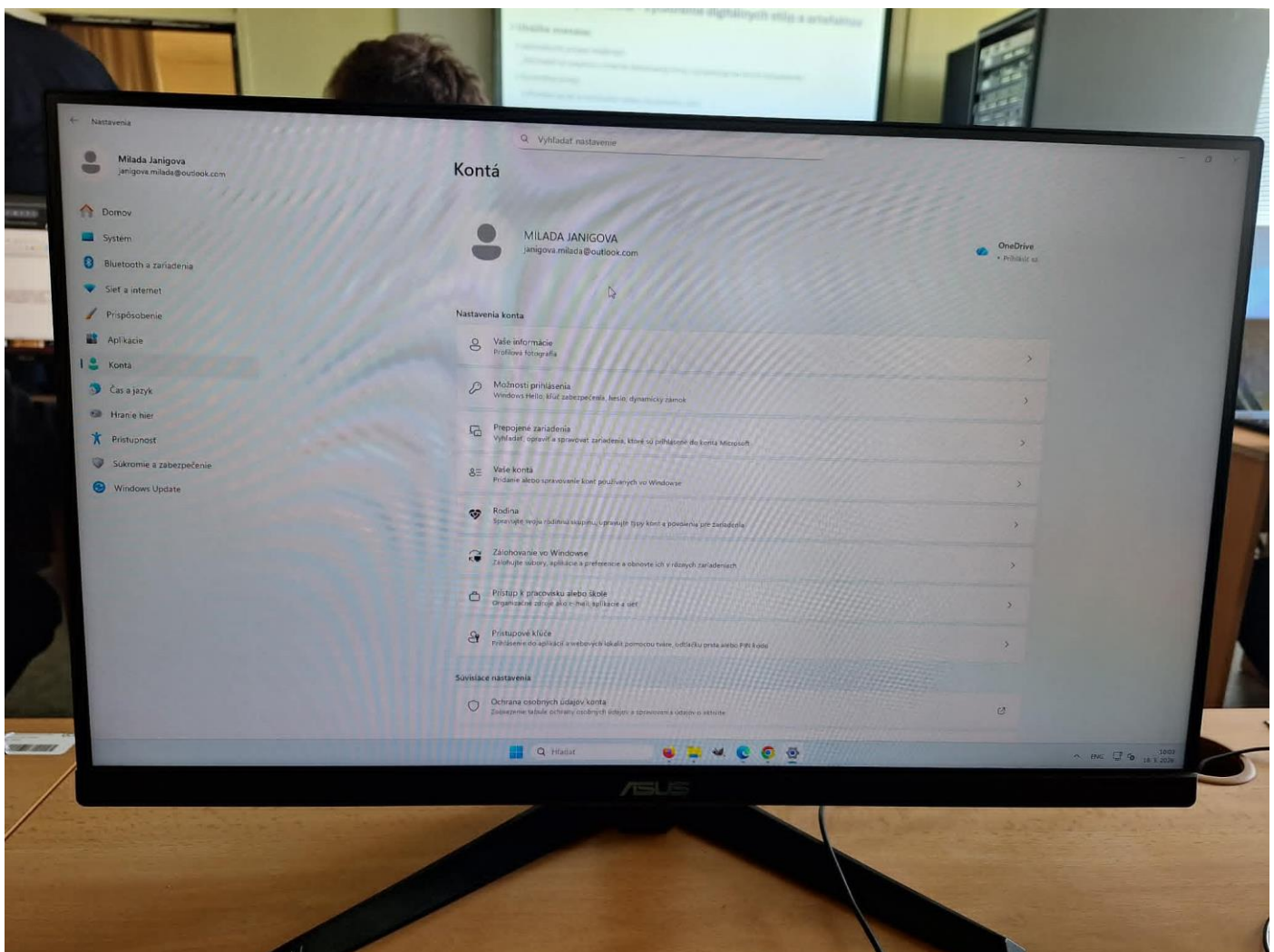


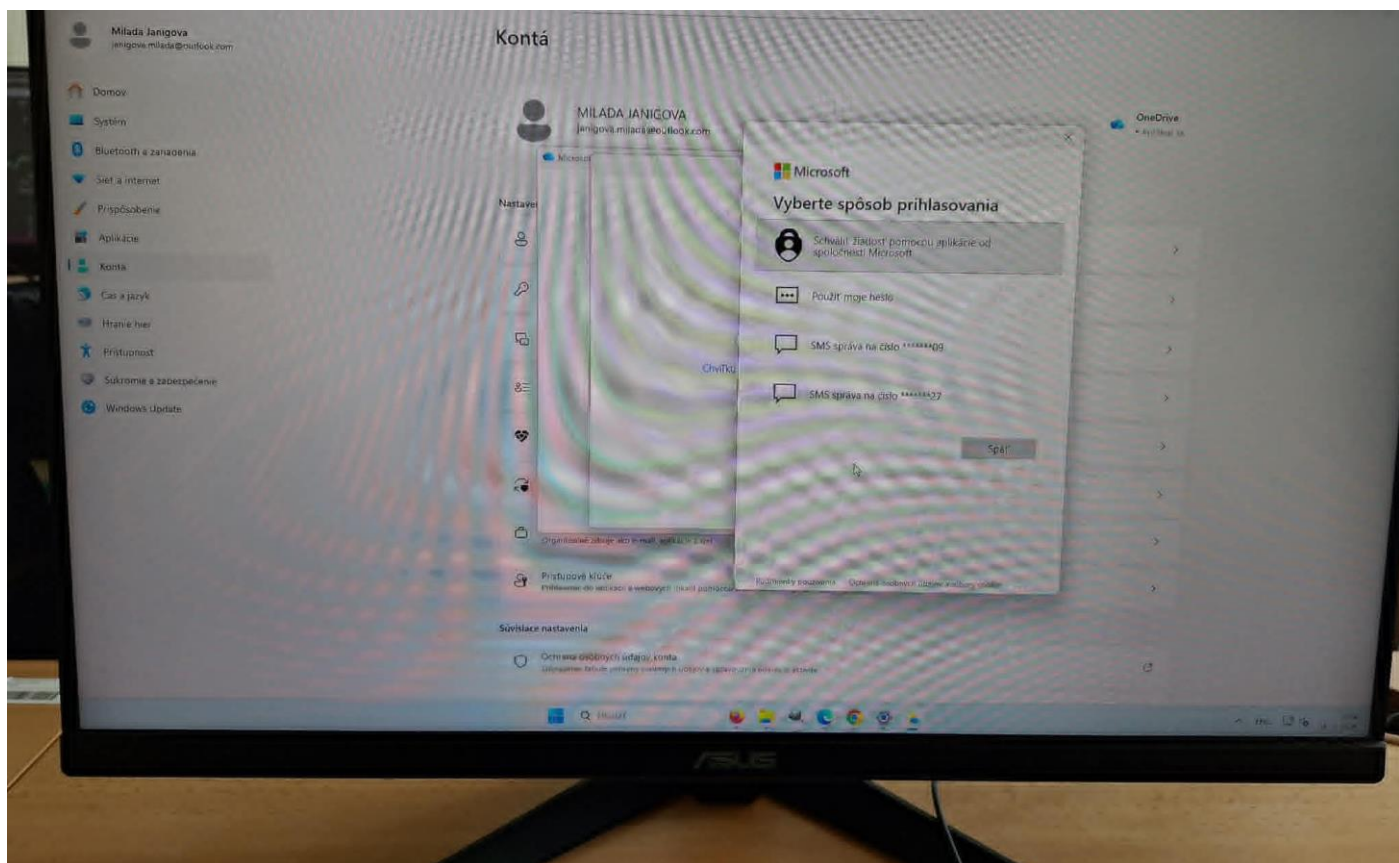
## Únik prihlasovacích údajov:

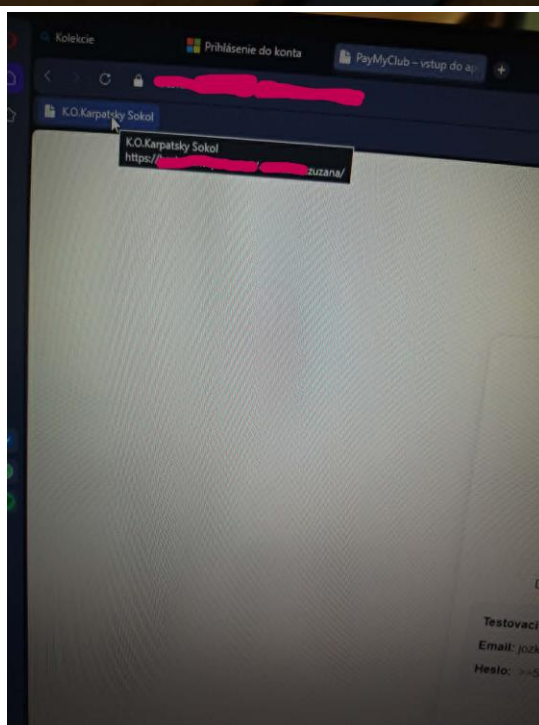
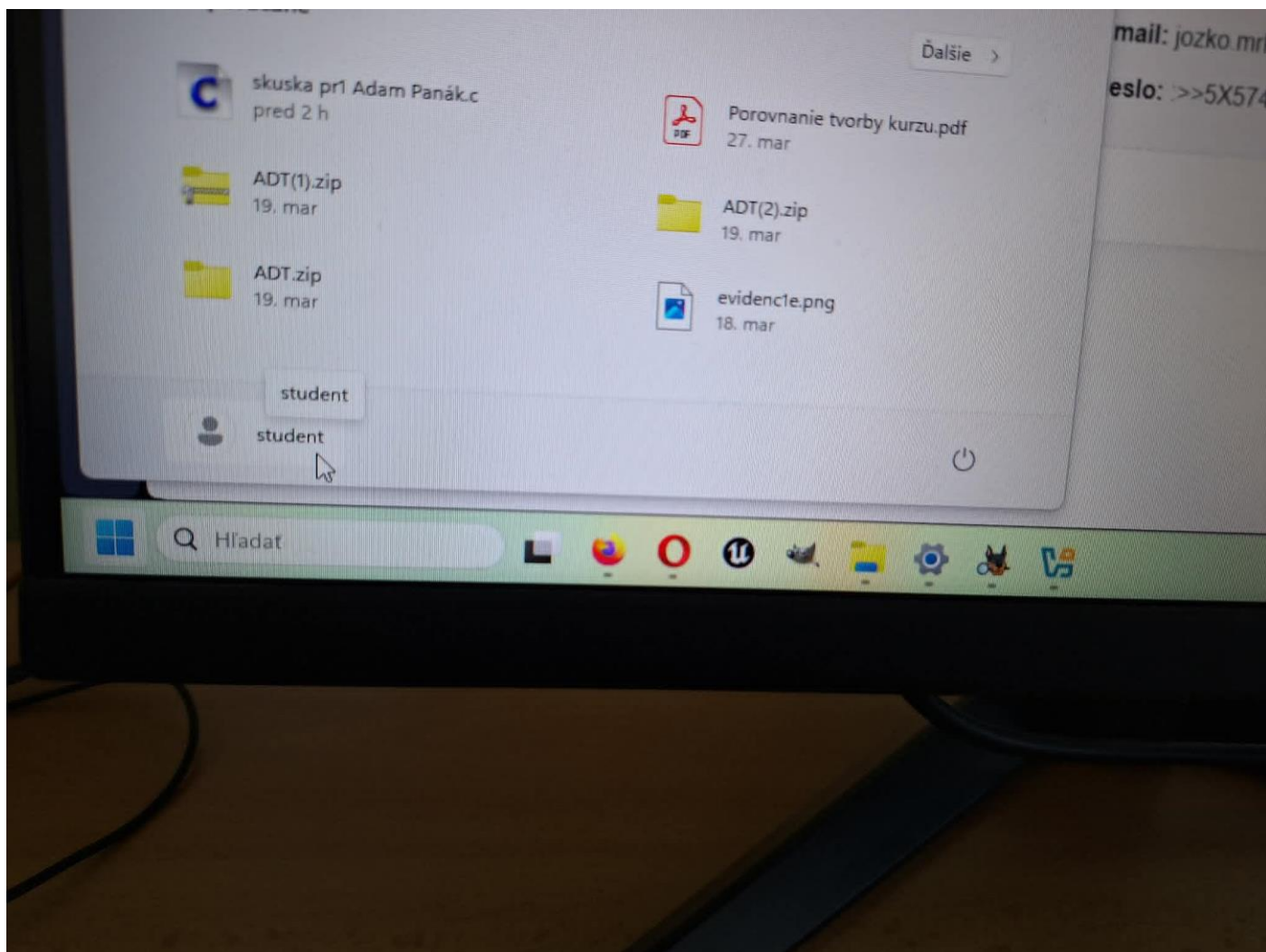




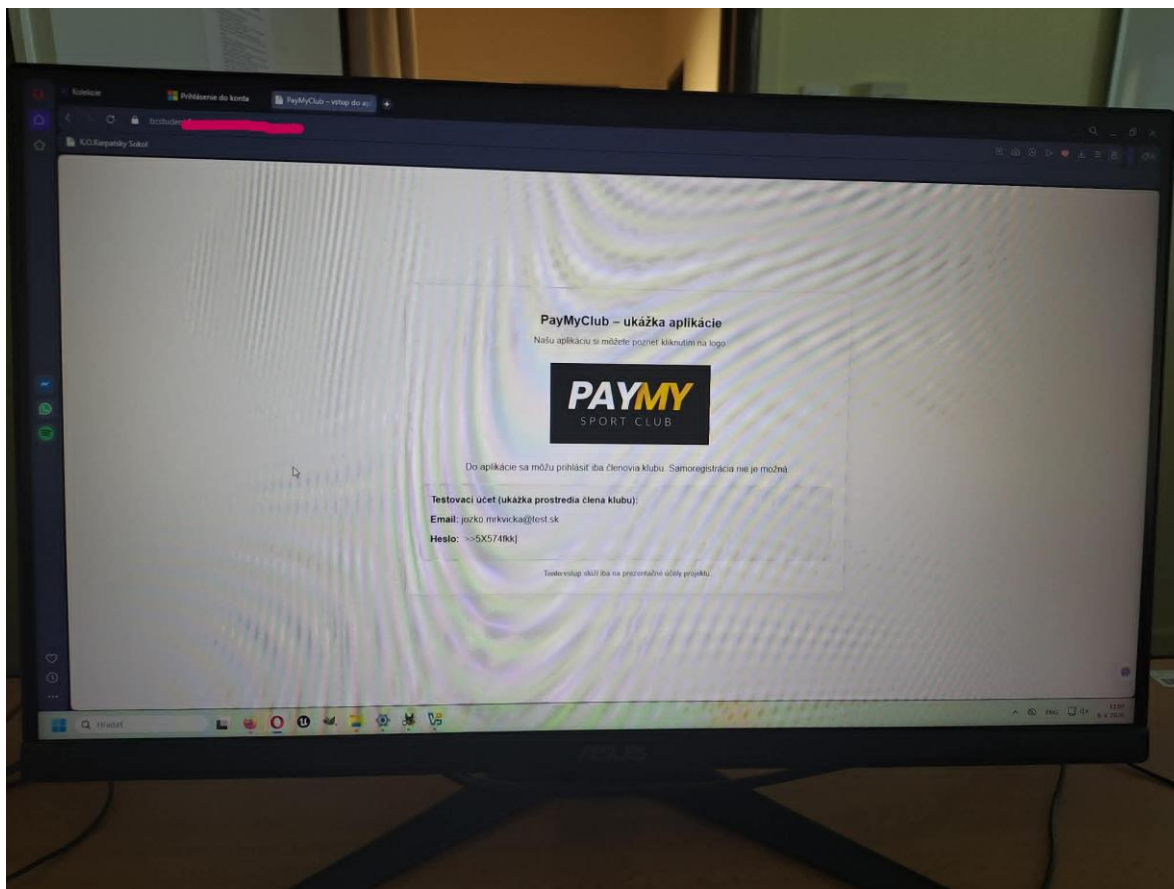
**Prihlasovacie údaje** sa dajú zneužiť na vzdialený SSH prístup na PC používateľa **cez SSH** alebo priamo.

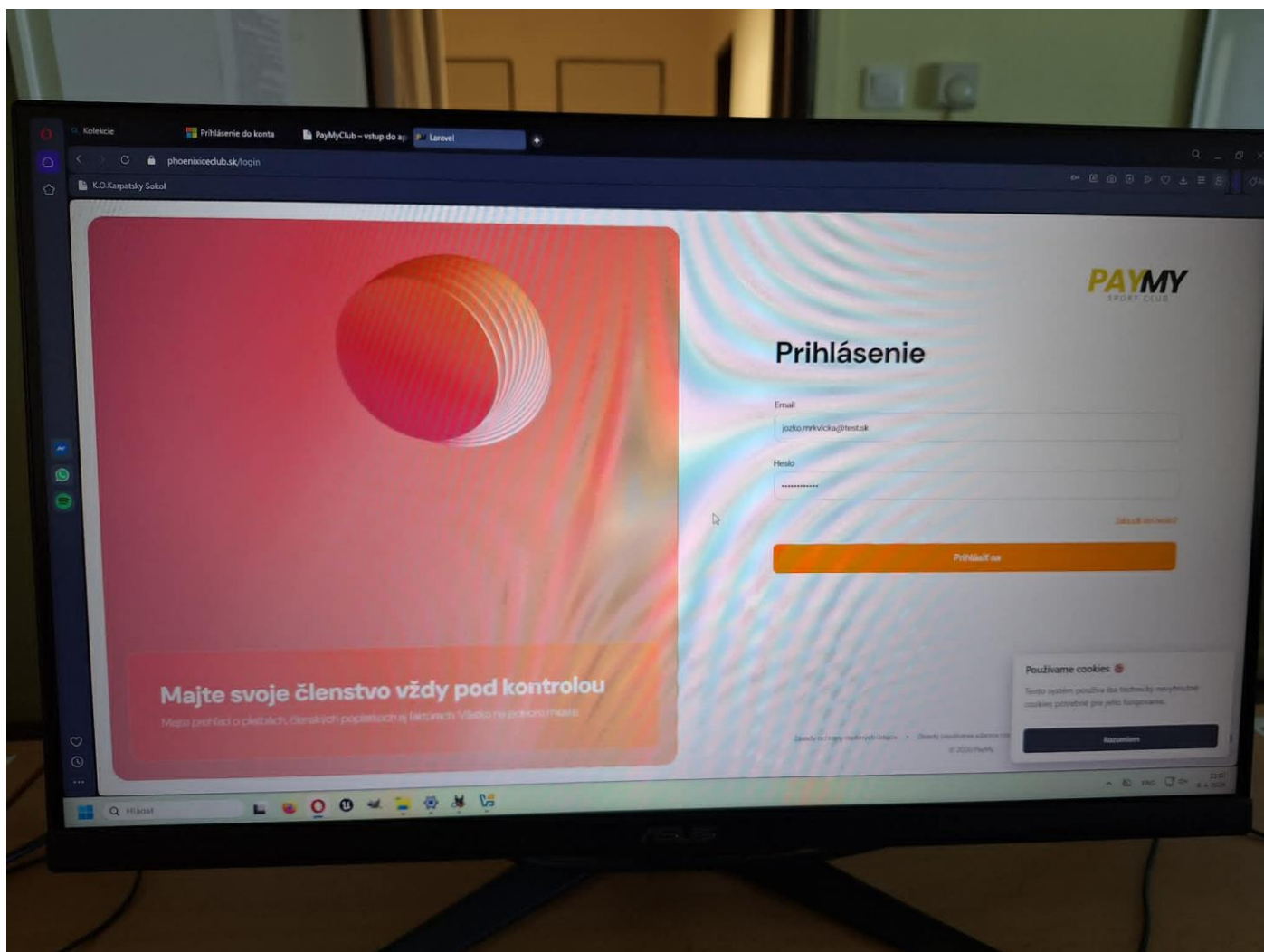






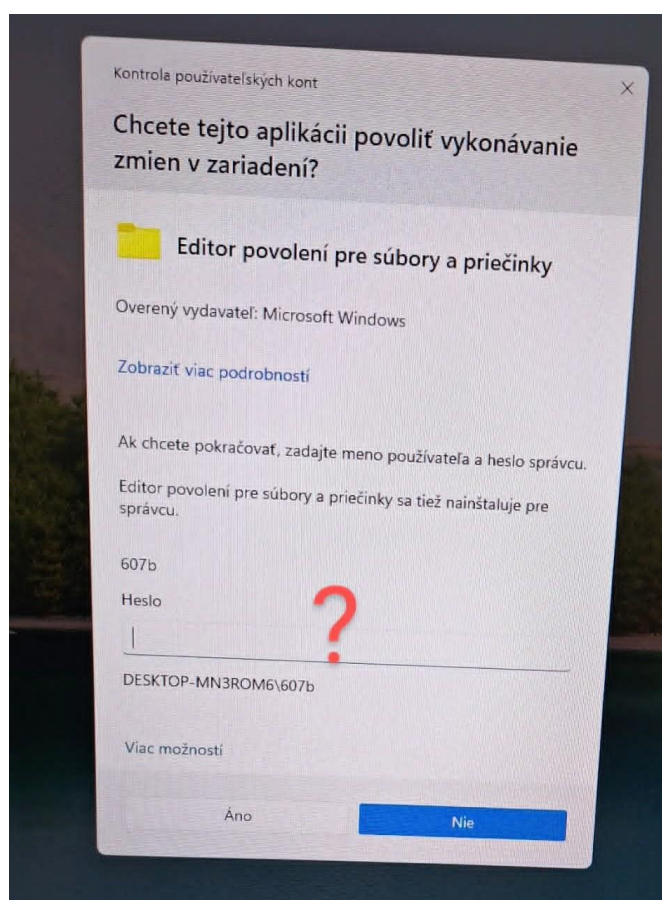
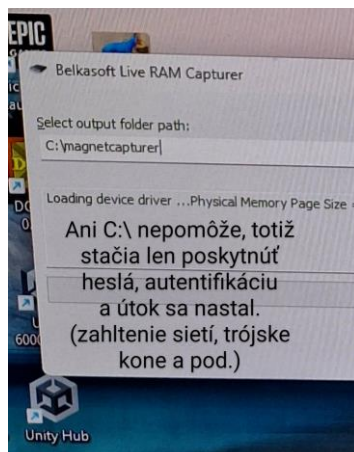
Pomocou *emailovej adresy*, prístup k *emailovej adresy a hesla* vieme *zaregistrovať* používateľov do rôznych *kompromitovaných aplikácií* ako *PAYMYClub*. Ide o identifikáciu typického *phishingového útoku*.

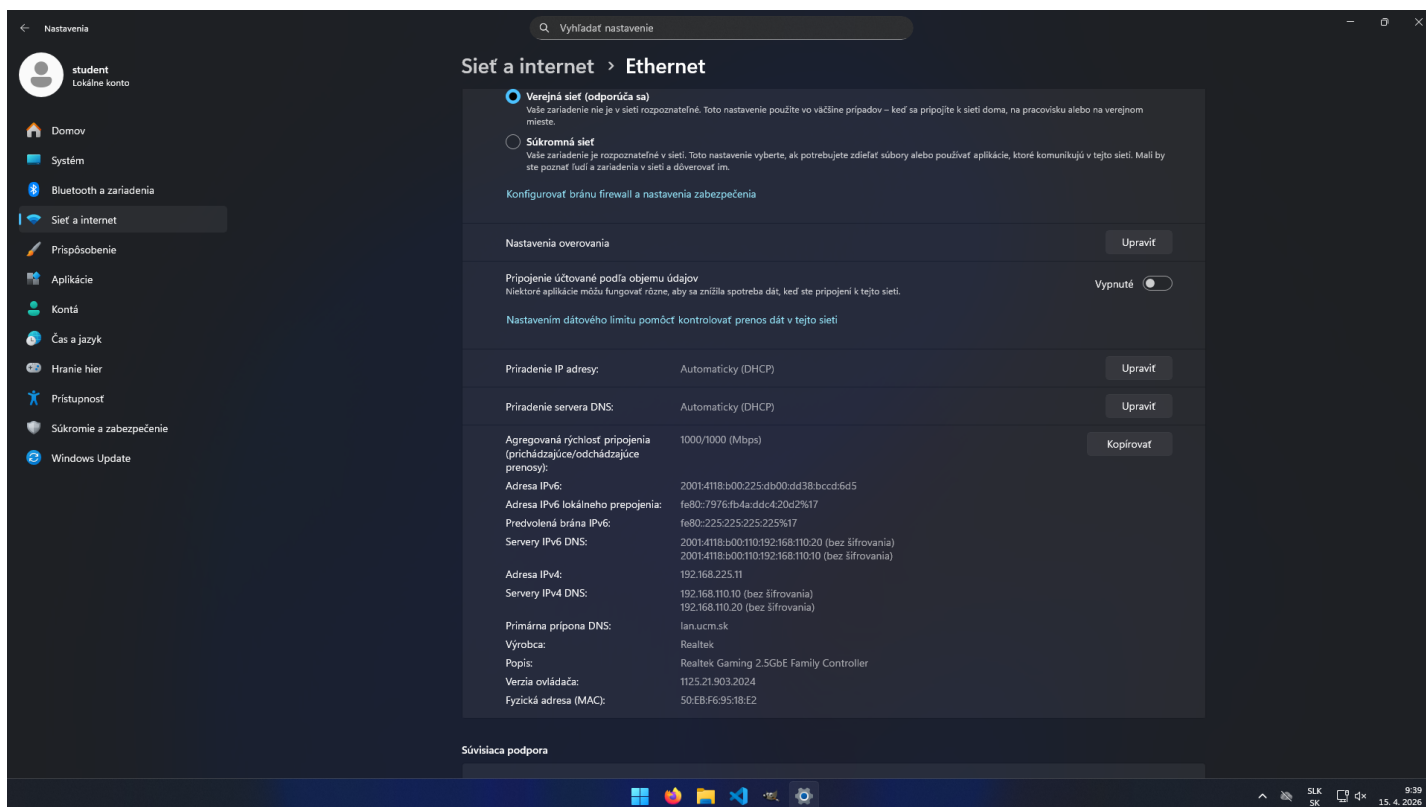


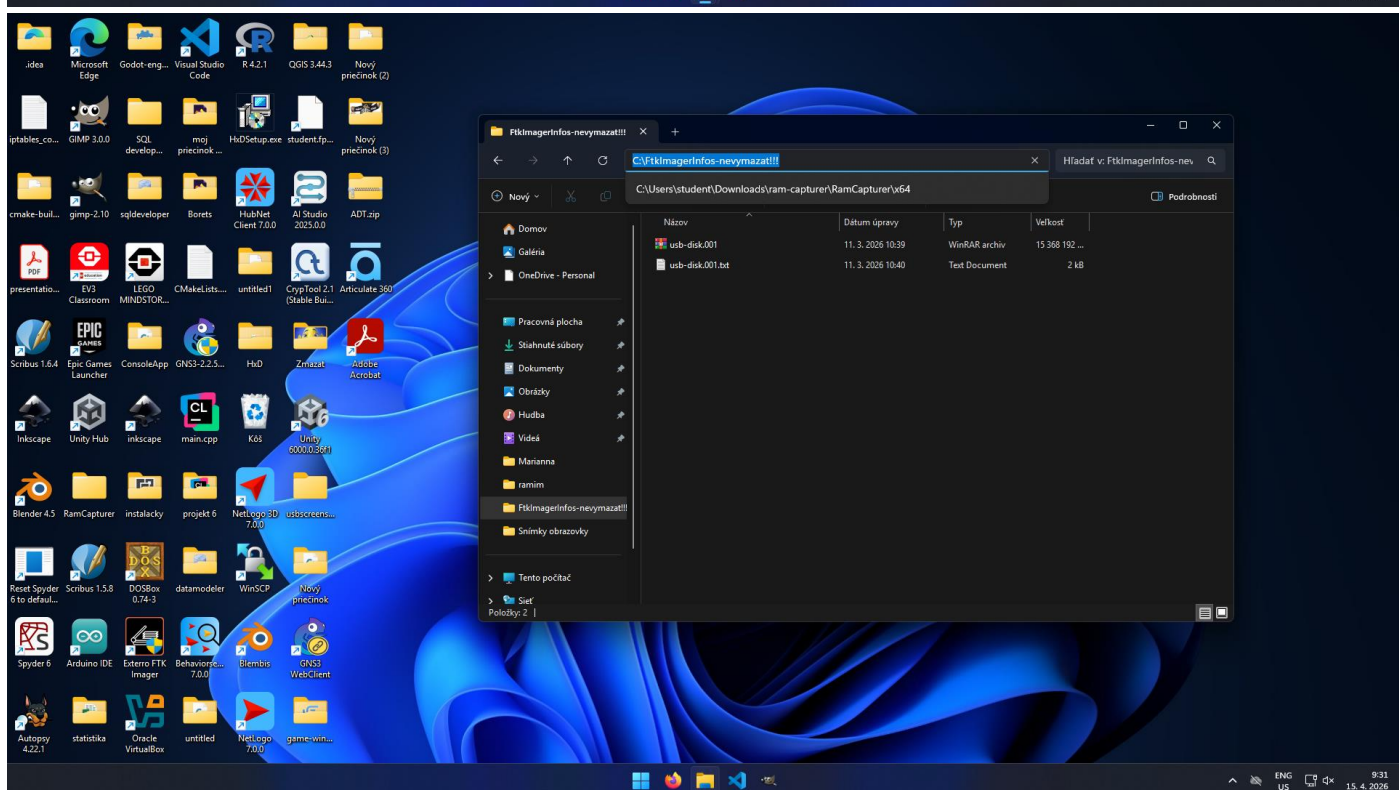
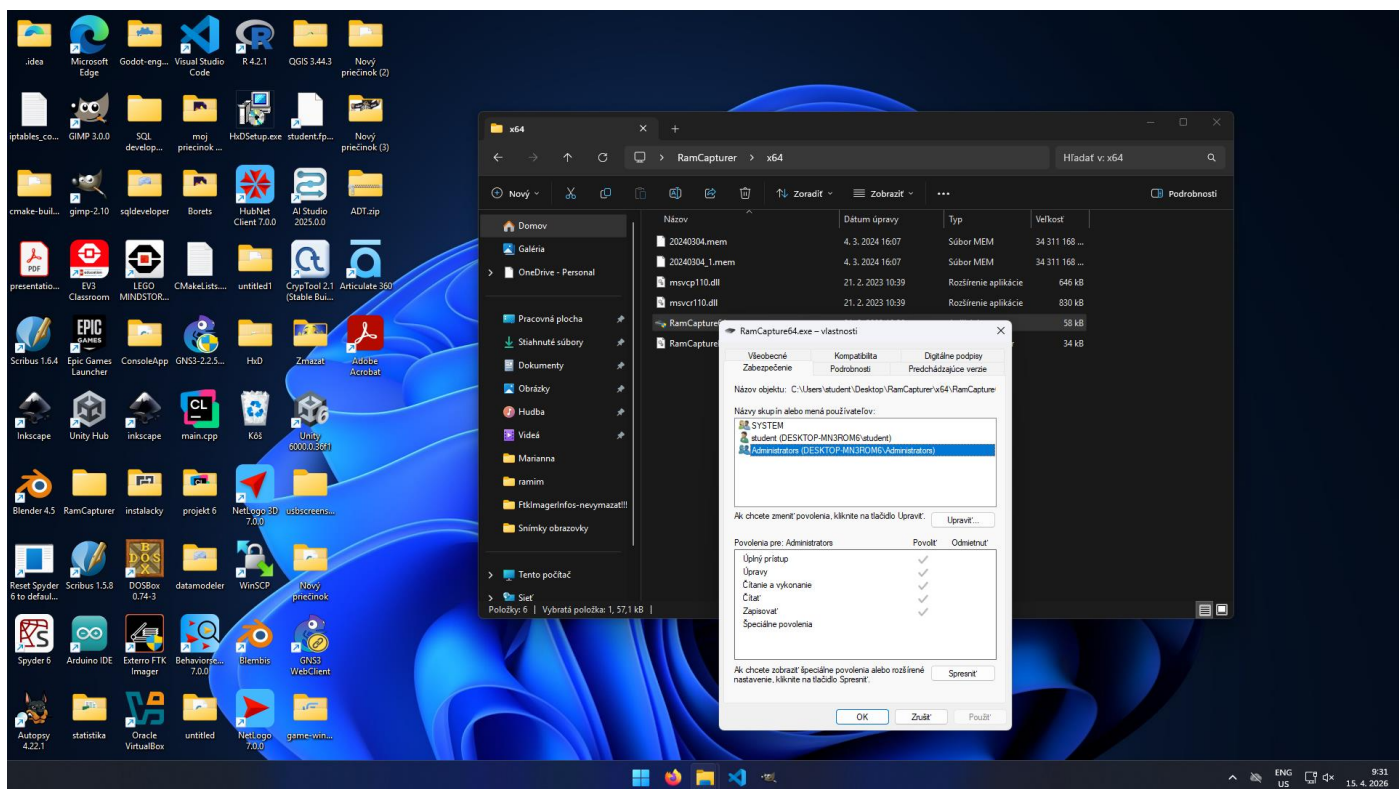


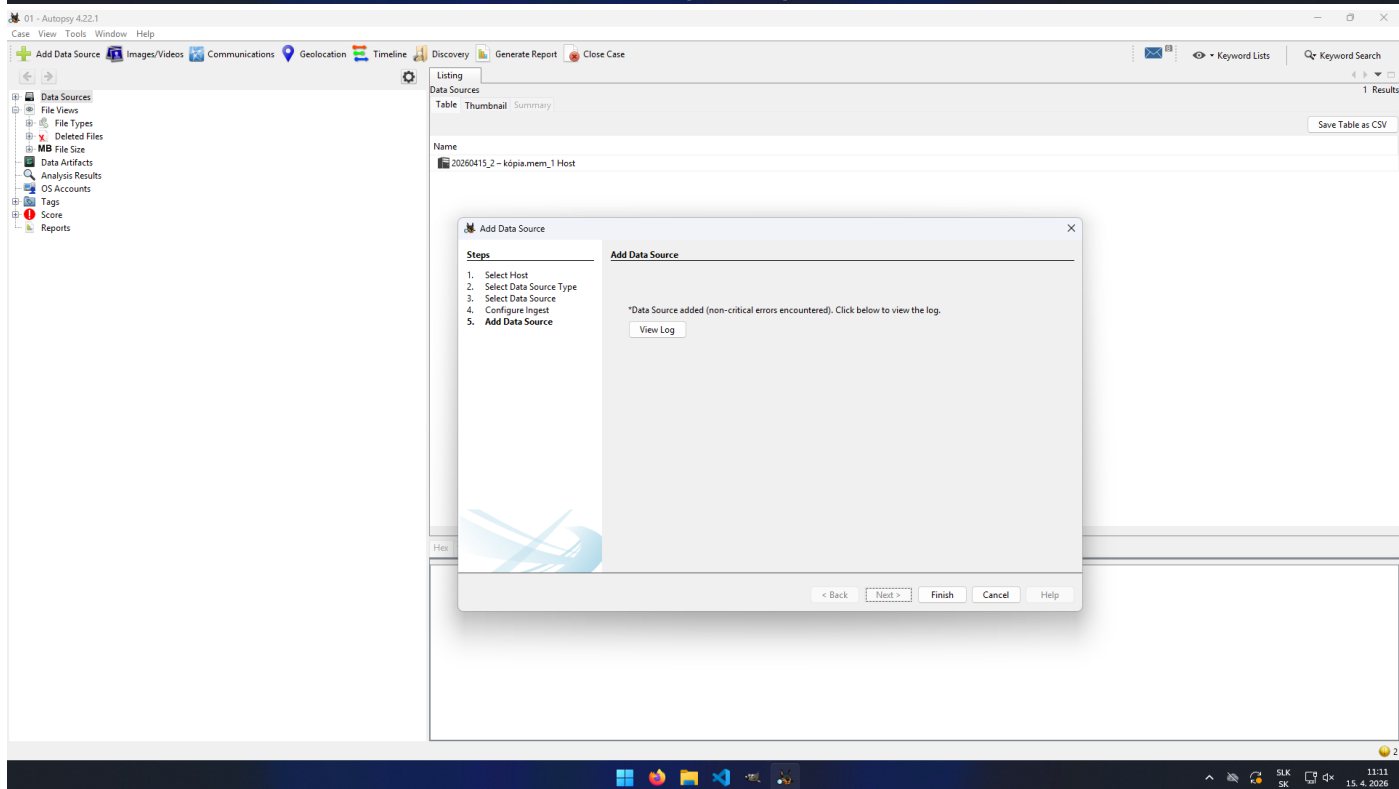
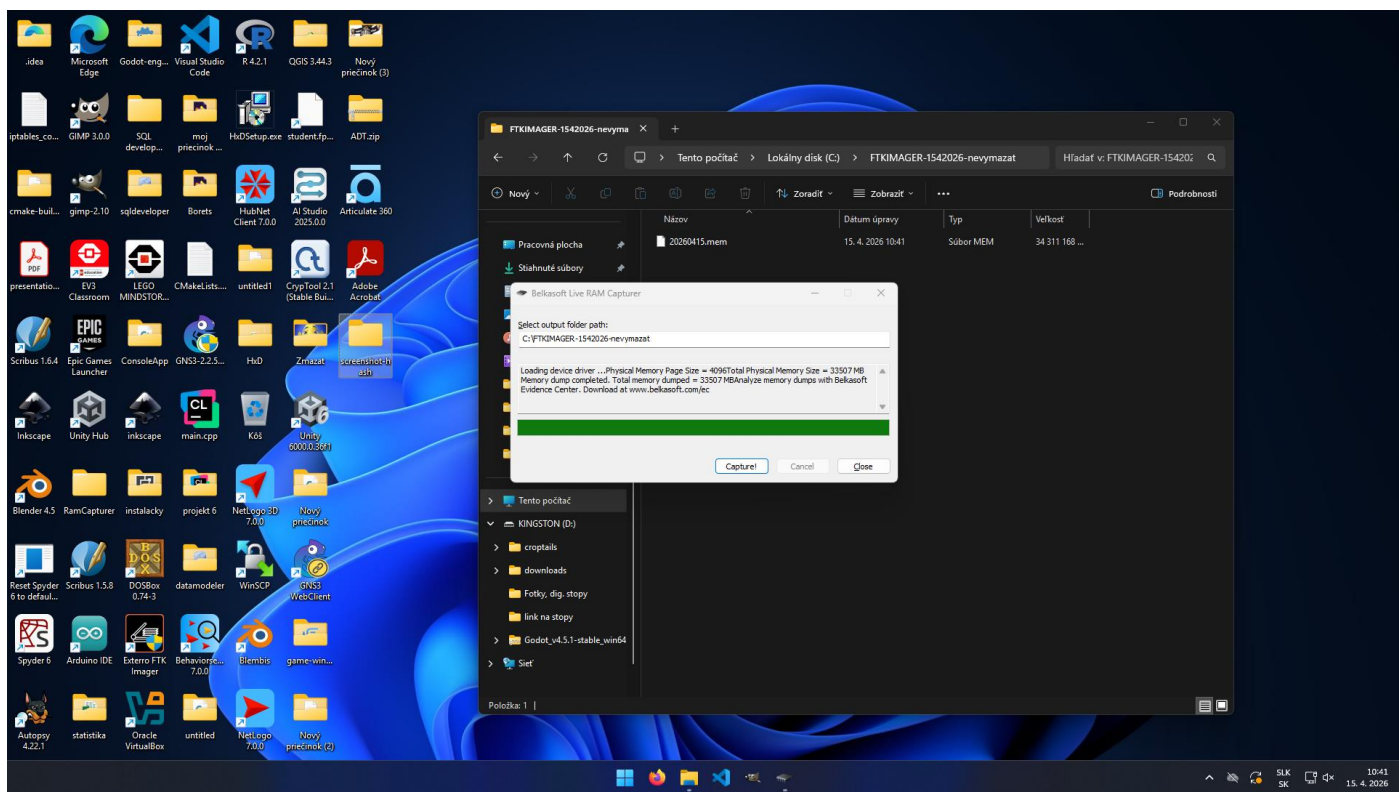
Samotný PC, čo útočník použil mal zrejme *administratívne prihlasovacie údaje* bud *cez VirtualBox*, alebo cez *phishingové kompromitované .pdf converter súbory* ako napr. <https://smallpdf.com/word-to-pdf> (čo je vlastne *malvér* tak ako je) , vlastne podobný prípad ako napr. náš príbeh YouTube videa [https://www.youtube.com/watch?v=x\\_LVxSkHMTl](https://www.youtube.com/watch?v=x_LVxSkHMTl) čo sme už uviedli vyššie.

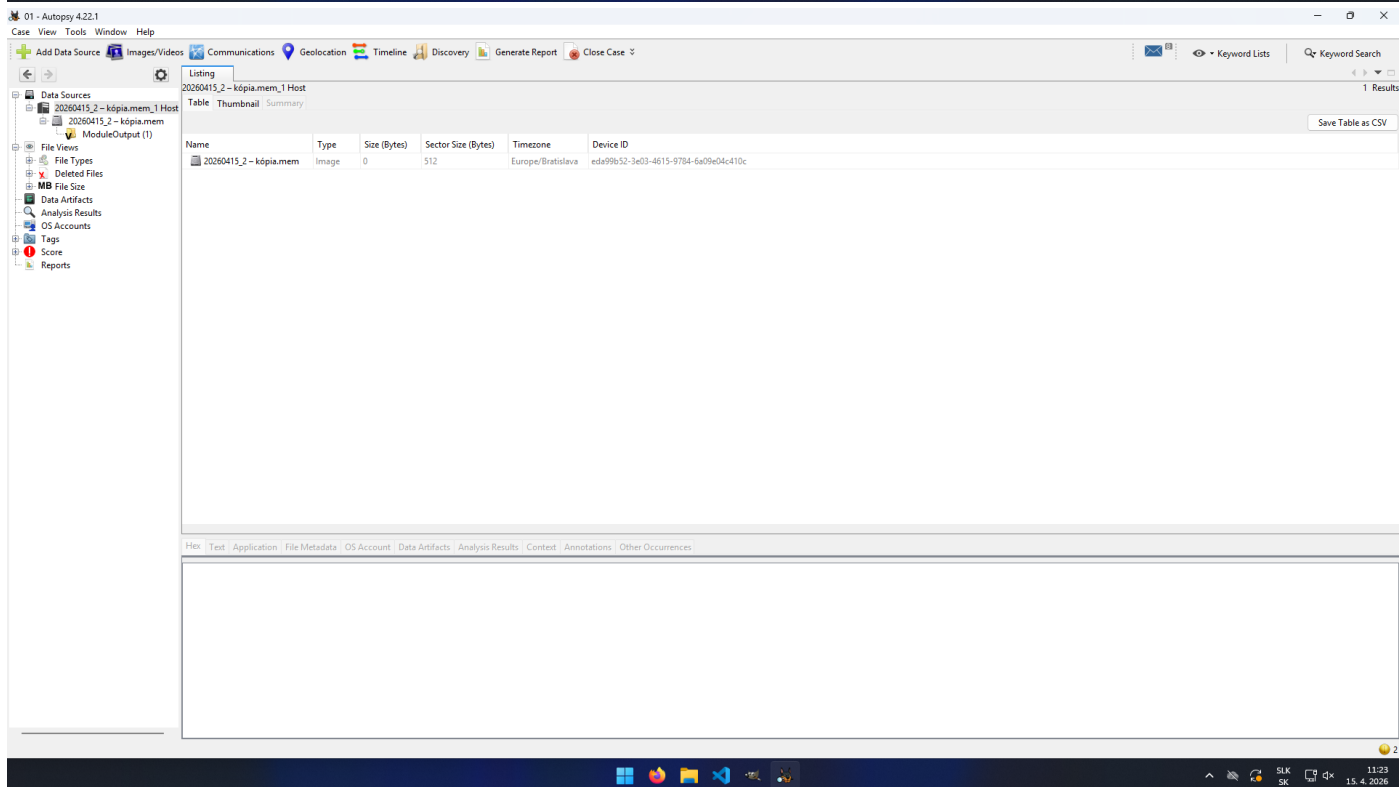
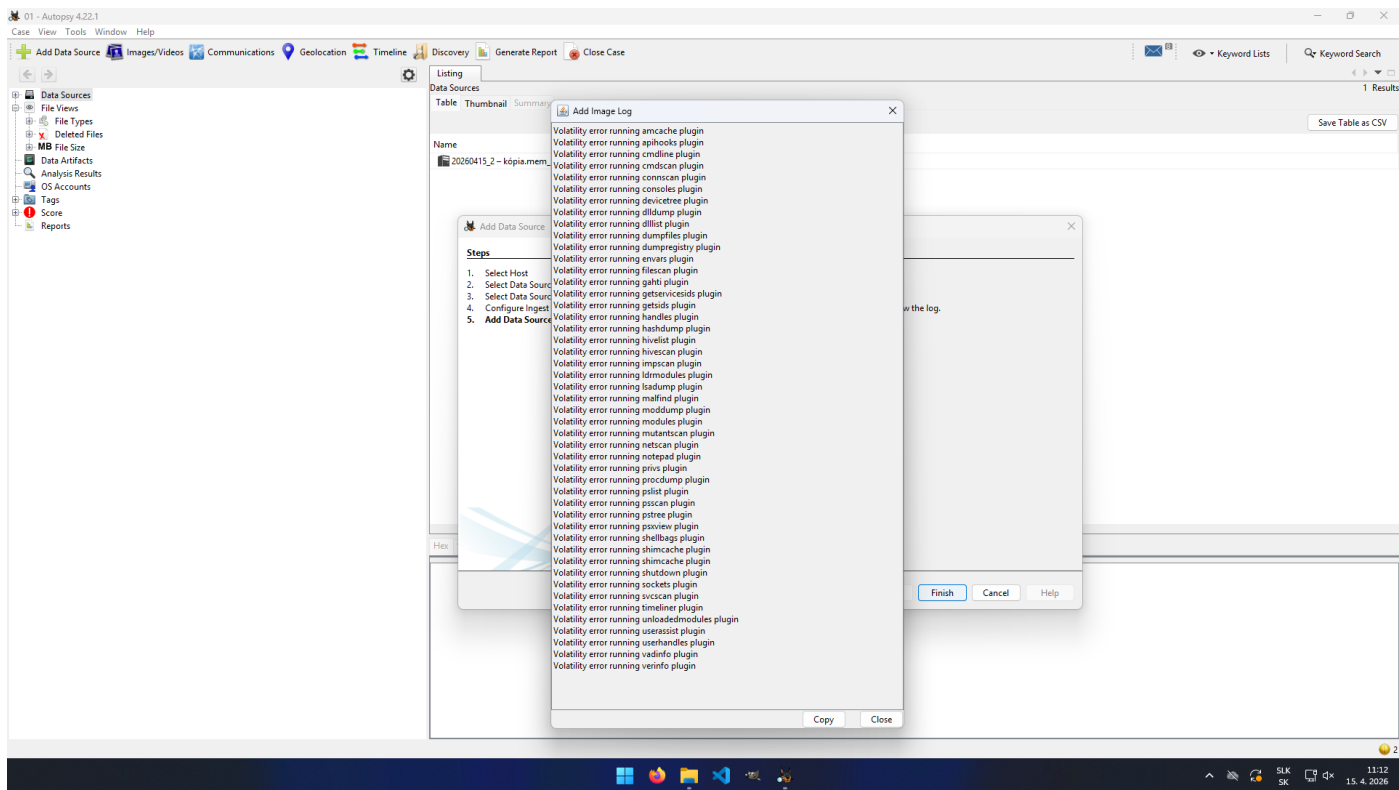
# Bezpečnostné opatrenia

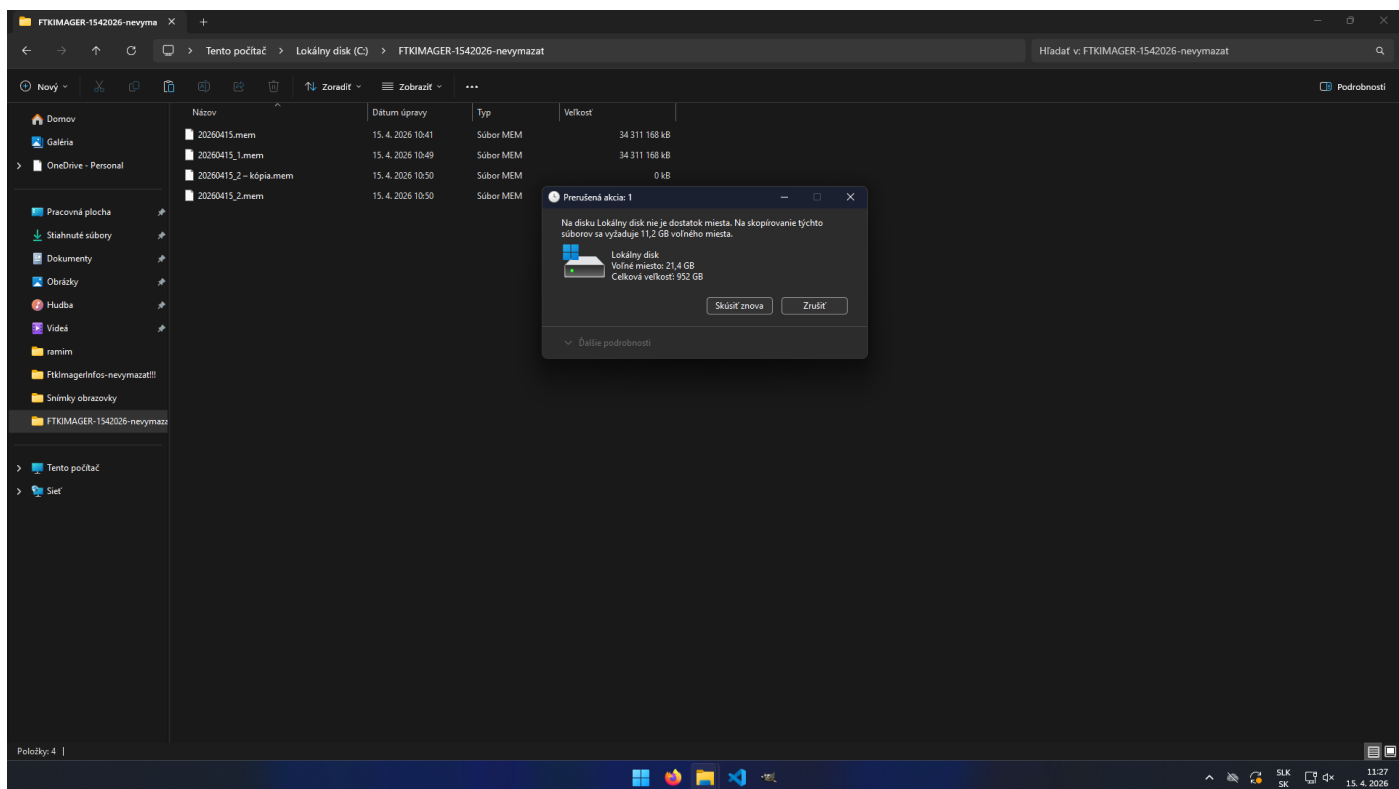












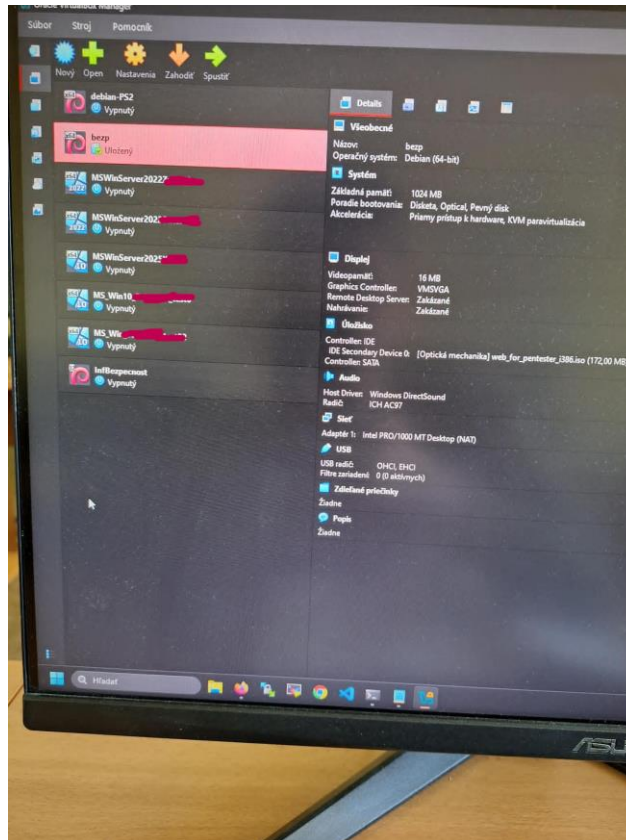
Plugins v autopsy a *nedostatok miesta na PC zneumožnili zobrazovať hash .mem* , resp. údaje boli poškodené (*non-critical plugin error check* ) . *Fyzické zariadenie bol poškodený páchatel'om.*



*Cez administratívne práva je možnosť zadefinovať na USB kľúč pripojený k Host PC cez sieťovú infraštruktúru sieťové rozhrania, čo je vlastne využitý na sieťovú komunikáciu cez RedHat virtuálnych strojov (a samozrejme monitorovaním jeho log dát a komunikácii cez PCI)*



Pomocou *virtuálneho stroja* s názvom *bezp* s operačným systémom *Debian(64-bit)* bol zrealizovaný *únik* a prenos *údajov* neoprávnene tak, že to obíde *hostiteľský operačný systém Windows*. Virtuálny stroj ani *nebol vypnutý* a *bežal v pozadí*. (stav *Uložený, nie Vypnutý*) Túto skutočnosť *únik dát* cez *L2 Cache* sme si overili aj z hľadiska *sieťovej infraštruktúry* pomocou *tracert*.



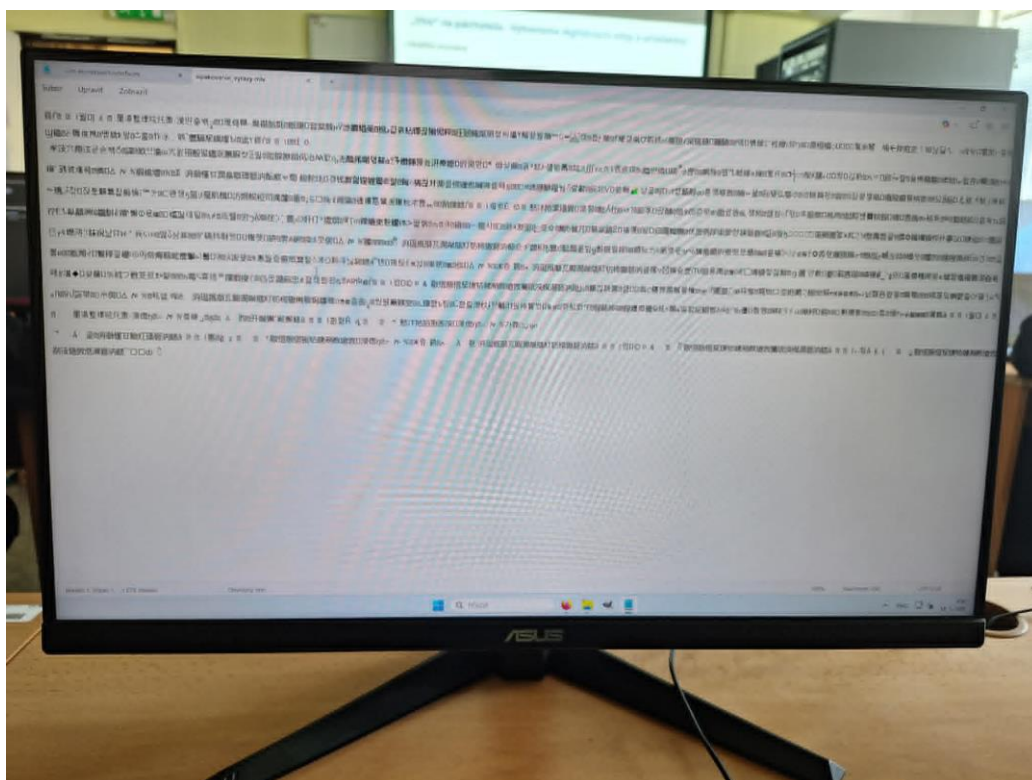
Príkazom *tracert 185.125.190.26* sme si zaznamenali **10minútové meškanie duplicitných odpovedí**. V procese **3-way handshake** proces **SYN-ACK** trval vyše **10 minút 11.22pm**. Z toho vieme, že ide o **synchronizovaný proces pripájania sa na iný server cez HOP3 10.69.253.127** (mal by byť koherentne **ako L1, L3 Cache** s next hopom bez COST špecifikácií, teda **HOP3 10.69.253.125**).

```
C:\Windows\System32>tracert 185.125.190.26

Tracing route to snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]
over a maximum of 30 hops:

 1  2 ms  1 ms  1 ms  192.168.1.1
```

Na počítači sme taktiež našli **šifru** na **verejný kľúč** na **zašifrovanie komunikácií cez sieťových rozhraní**.



**Pripájanie USB kľúču** do kompromitovaného počítača spôsobí **prístup externého zdroja** na samotný USB kľúč, ale tým pádom, že počítače by mali byť **chránené heslom administrátora**, by tieto zadefinovania nemohli nastať. V prednej časti .....**€?.....** je **zašifrovanie sieťových rozhraní**, čo sa konkrétne týka **thumbcache interface. (L2 cache)**

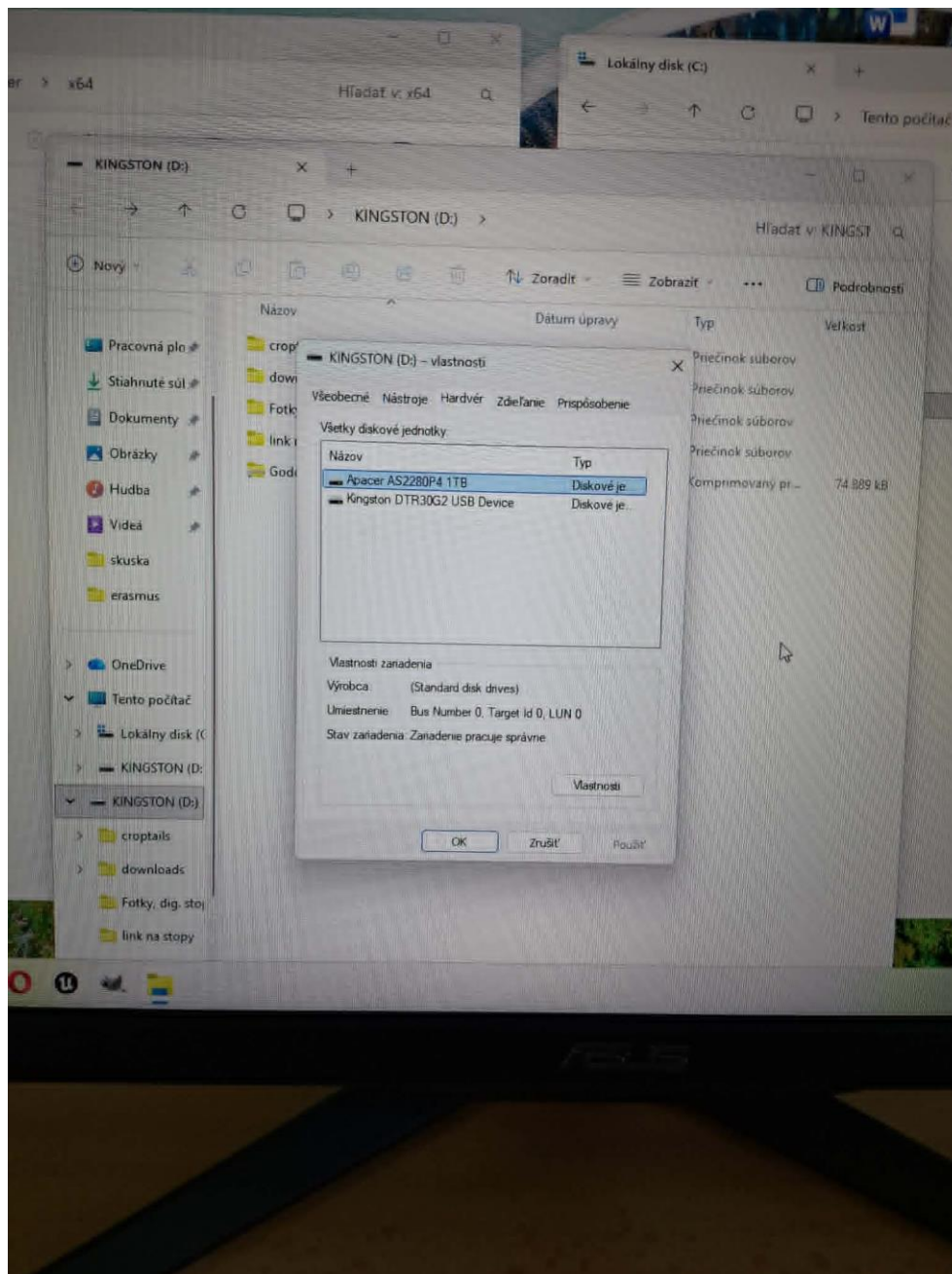
```

F Decoded text
O .....€?.....
F ..€?.....€?..€?
O ..€?..€?.....
O .....€?....
F .....€?
O .....
O ..€?.....
O í...ObNmã".ć....
O \.B.a.s.e.N.a.m.
O e.d.O.b.j.e.c.t.
O s.\.C.:.:.U.s.e.
O r.s.:.s.t.u.d.e.
O n.t.:.A.p.p.D.a.
O t.a.:.L.o.c.a.l.
O :.M.i.c.r.o.s.o.
O f.t.:.W.i.n.d.o.
O w.s.:.E.x.p.l.o.
O r.e.r.:.t.h.u.m.
O b.c.a.c.h.e._i.
O d.x...d.b!.r.w.

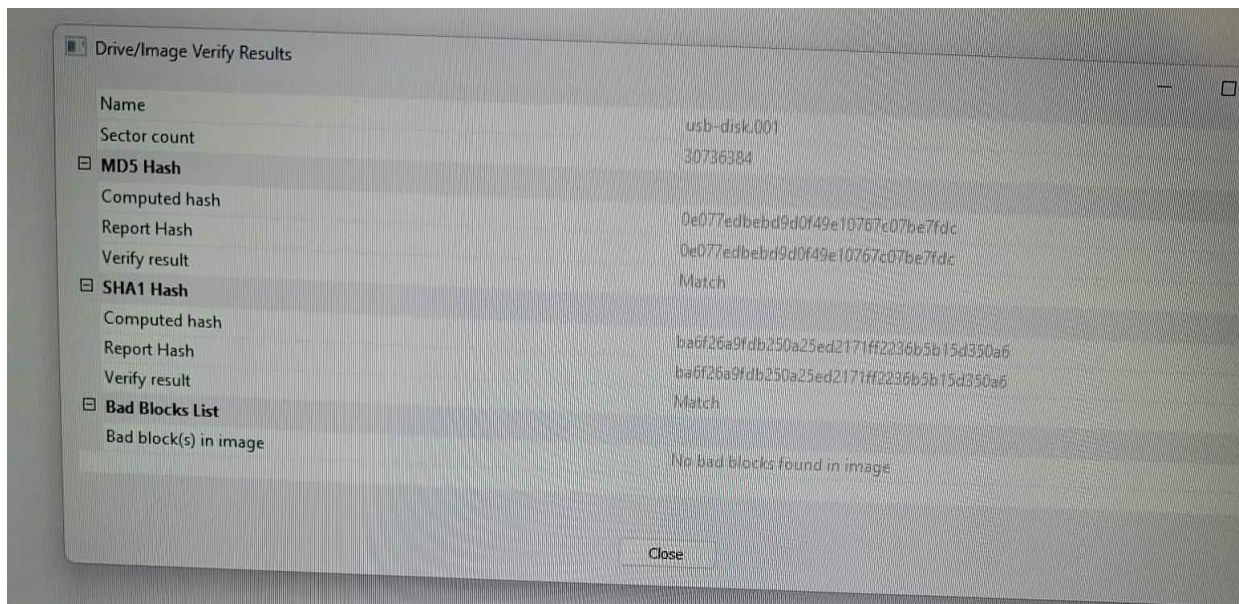
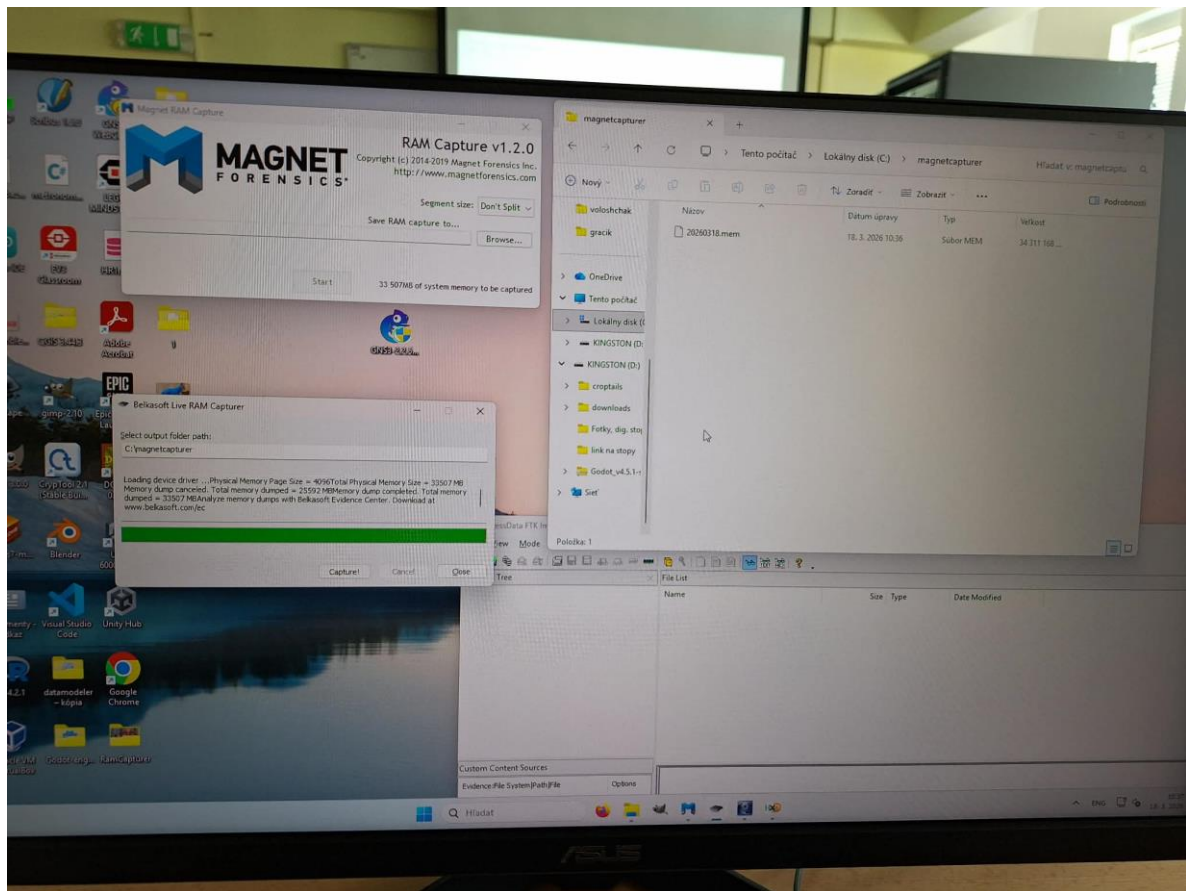
```

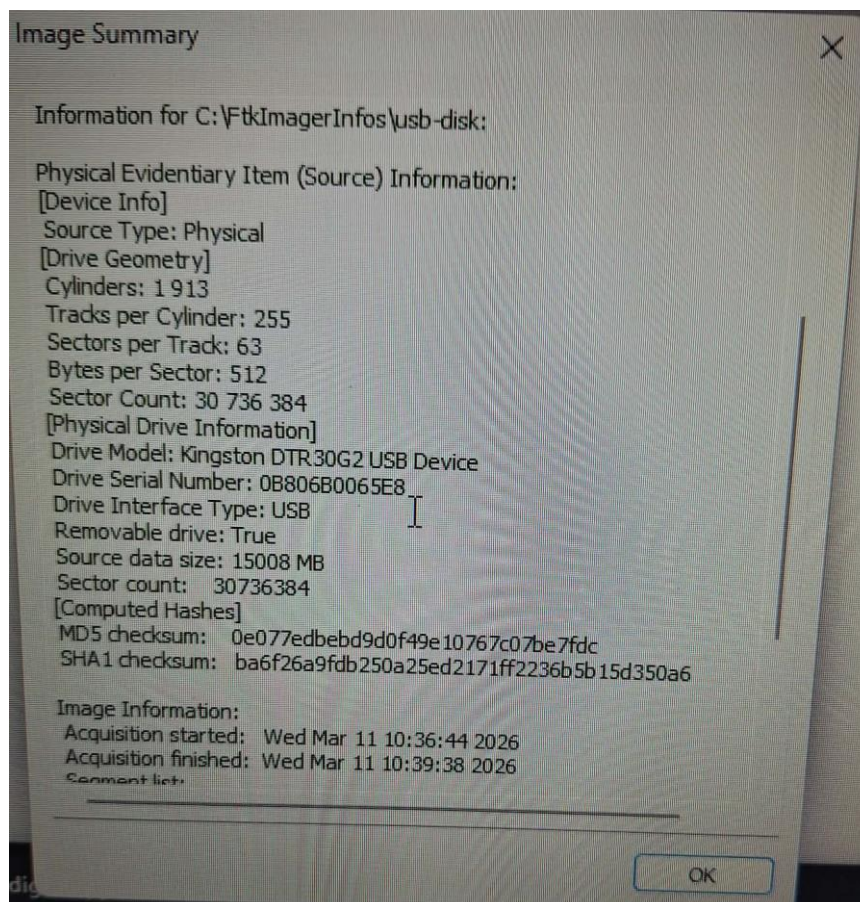
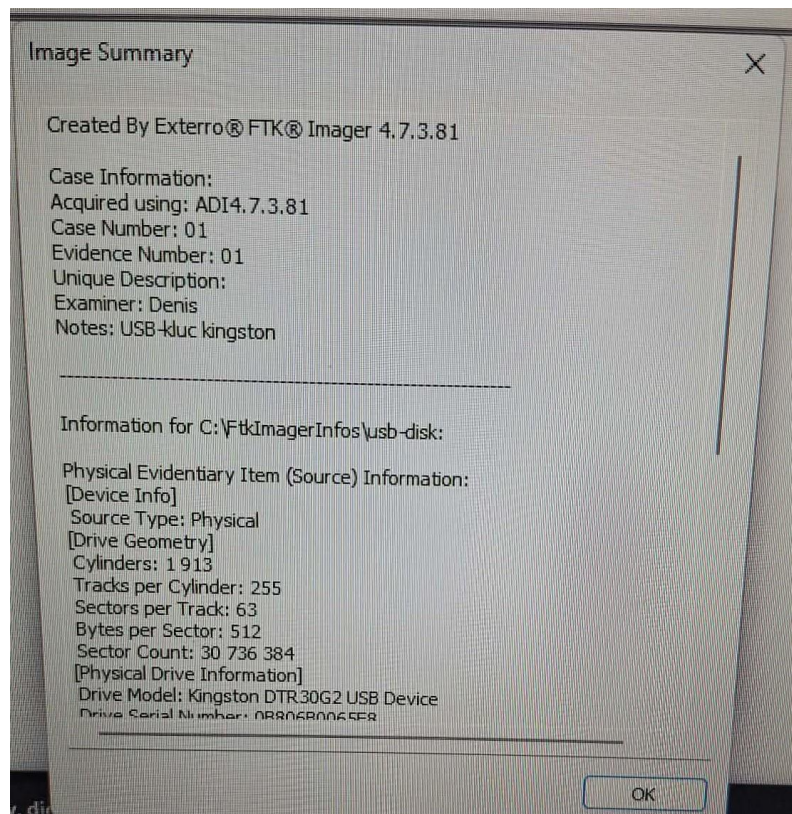
Externý zdroj **Apacer AS2280P4 1TB** disková jednotka neoprávnene sa pripájal k našej USB kľúč diskovej jednotke **Kingston DTR30G2 pri**

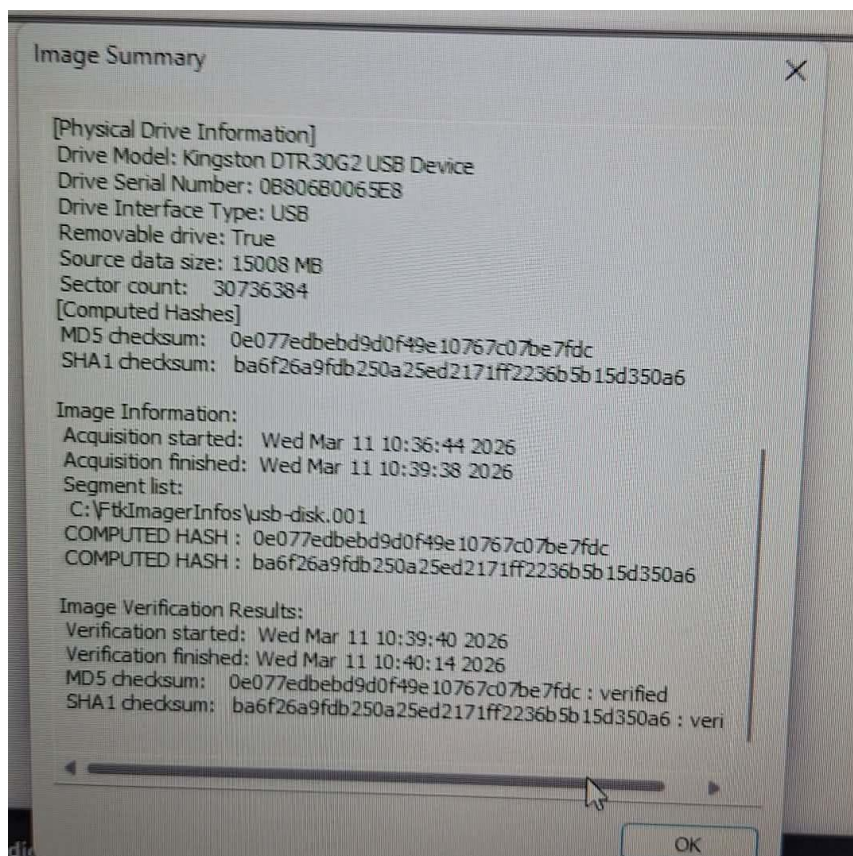
**zaist'ovani dôkazov**, to znamená, že **pomocou administrátorských oprávnení prepísal sieťové rozhrania** na našom USB zariadení (už ukázané vyššie)



## Zaistenie dôkazov z USB zariadení Kingston DTR30G2







## Chain of custody

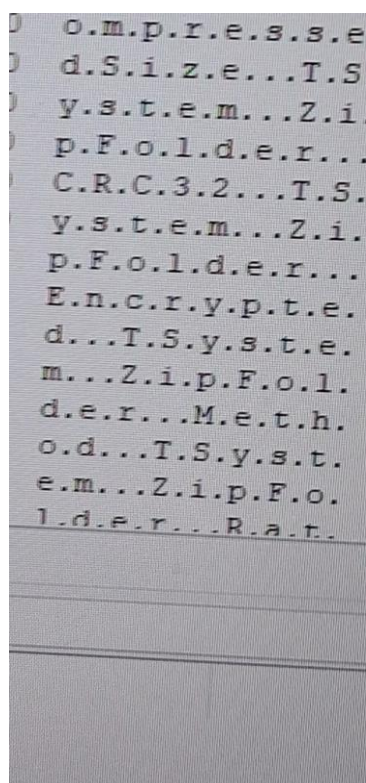
### ARNES 2017 – Identifikácia digitálnych stôp

|                |                                                                                                                                                                |                |  |                 |  |          |  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--|-----------------|--|----------|--|
| Číslo:         |                                                                                                                                                                | Typ súboru:    |  | Obnovený súbor: |  | Veľkosť: |  |
| 01             |                                                                                                                                                                | Ftk image file |  | Nie             |  | 15008 MB |  |
| Popis prípadu: | Dňa 11.3.2026 10:36:44 sme zaistili usb kľúč Kingston DTR30G2 obsahujúce dôkazy identifikovaných útokov a následne sme si vytvorili MD5 a SHA1 hash usb kľúču. |                |  |                 |  |          |  |
| Názov súboru:  | dig. Stopy; croptails; downloads; link na stopy; Godot (.zip file)                                                                                             |                |  |                 |  |          |  |

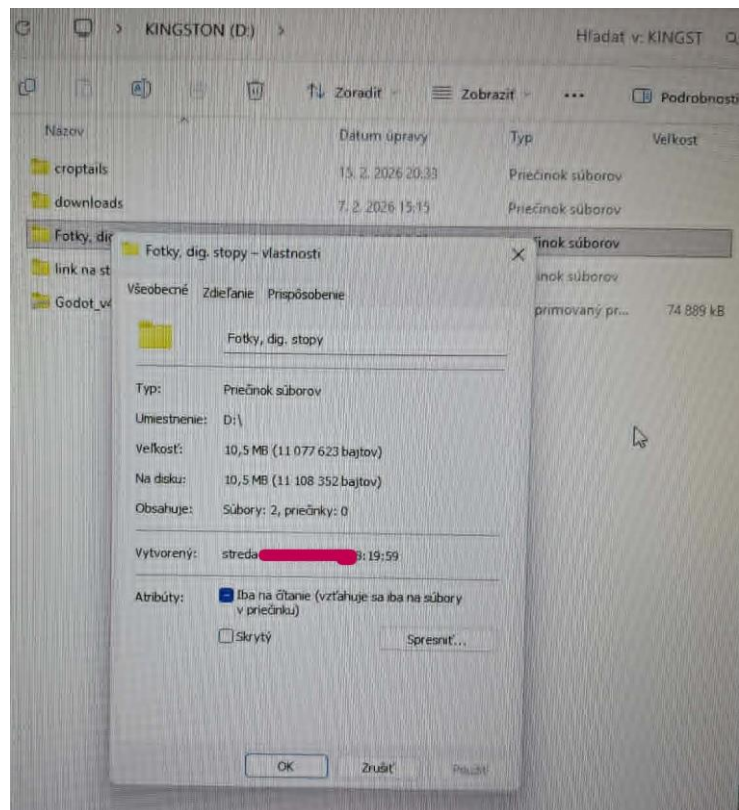
|                                   |      |                                                                                             |  |                |  |
|-----------------------------------|------|---------------------------------------------------------------------------------------------|--|----------------|--|
|                                   |      |                                                                                             |  |                |  |
| Miesto získania digitálnej stopy: |      | Počítač s MAC adresou 50:EB:F6:95:1B:E2 a priamo USB zariadenie Kingston DTR30G2 USB Device |  |                |  |
| Poznámky:                         |      | Počas zaistenia dôkazov sa nastal neoprávnený prístup na USB zariadenie.                    |  |                |  |
|                                   |      |                                                                                             |  |                |  |
| Časové pečiatky                   |      |                                                                                             |  |                |  |
| Access:<br>11.3.2026<br>10:36:44  |      | Modify:<br>Ano                                                                              |  | Change:<br>Ano |  |
|                                   |      |                                                                                             |  |                |  |
| Digitálny odtlačok (heš)          | MD5  | 0e077edbebd9d0f49e10767c07be7fdc                                                            |  |                |  |
|                                   | SHA1 | ba6f26a9fdb250a25ed2171ff2236b5b15d350a6                                                    |  |                |  |
|                                   |      |                                                                                             |  |                |  |
| Časová pečiatka                   |      | Akcia vykonaná s digitálnou stopou                                                          |  |                |  |
| 24.2.2026                         |      | Dátum začiatku získavania informácií (acquisition started).                                 |  |                |  |
| 03.5.2026                         |      | Dátum ukončenia získavania informácií (acquisition finished).                               |  |                |  |

*Neoprávnený prístup na USB kľúč pôsobil poškodenie všetkých súborov nachádzané sa na flash pamäti, boli prepísané nielen sieťové rozhrania na únik Cache pamäti, ale boli poškodené aj uložené dôkazy na útoky "Fotky, dig. stopy" čo sme si aj zadefinovali tu, taktiež bol poškodený softvérový projekt a samotný zdroj softvéru Godot (.zip file, jediný komprimovaný priečinok).*

## Dáta



o.m.p.r.e.s.s.e  
d.S.i.z.e...T.S  
y.s.t.e.m...Z.i.  
p.F.o.l.d.e.r...  
C.R.C.3.2...T.S.  
y.s.t.e.m...Z.i.  
p.F.o.l.d.e.r...  
E.n.c.r.y.p.t.e.  
d...T.S.y.s.t.e.  
m...Z.i.p.F.o.l.  
d.e.r...M.e.t.h.  
o.d...T.S.y.s.t.  
e.m...Z.i.p.F.o.  
l.d.e.r...R.a.t.



```

0B 0C 0D 0E 0F Decoded text
74 00 00 00 00 \W.R....slnt....
00 00 00 0A 00 SX.R....).....
67 67 73 00 0A ..rtA_Prín.ggs..
00 09 73 6C 6F batchNumber..slo
74 73 41 76 61 tsUsed..slotsAva
68 65 73 74 56 ilable..highestV
69 6F 6E 57 69 isibleLocationWi
69 6E 67 00 09 thoutScrolling..
53 65 73 73 69 startInvokeSessi
64 65 72 43 61 onId..providerCa
98 0D 53 75 67 chedStatus...Sug
77 4D 6F 64 65 gestionsViewMode
74 69 6F 6E 50 lRecommendationP
6F 63 6B 52 65 rovider...MockRe
6E 50 72 6F 76 commendationProv
72 61 74 65 46 ider..SubstrateF
64 61 74 69 6F ileRecommendatio
53 61 6D 70 6C nProvider..Sampl
50 72 6F 76 69 eTypescriptProvi
65 73 52 65 63 der..TopSitesRec
50 72 6F 76 69 ommendationProvi
63 6F 6D 6D 65 der..IrisRecommen
69 64 65 72 00 ndationProvider.
65 72 00 16 4D .WiseProvider..M
50 72 6F 76 69 eetingGroupProvi
6C 79 41 64 64 der..RecentlyAdd
69 64 65 72 00 edGroupProvider.
76 69 64 65 72 .GroupedProvider.
63 6F 6D 6D 65 ..MeetingRecommen
69 64 65 72 00 ndationProvider.
76 69 64 65 72 .MFUAppsProvider
64 65 72 00 16 ..MsanProvider..
00 00 00 0E 00 lš.R....).....
D FE 7F 00 00 ..('t...BLU]t...
B 78 3C 91 00 w.P1.R...X&x<1.

```

| Offset (h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text     |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 44B61A3B0  | 20 | 3A | 6F | 2E | 74 | 61 | 62 | 6C | 65 | 5F | 6E | 61 | 6D | 65 | 3B | 0A | :o.table_name;.  |
| 44B61A3C0  | 45 | 4E | 44 | 3B | 2C | 00 | 17 | 04 | C3 | 08 | 25 | 22 | 02 | C1 | 05 | 02 | END;...Ã.%.Ã..   |
| 44B61A3D0  | C1 | 02 | 01 | 80 | 01 | 80 | 04 | C3 | 08 | 25 | 1D | 01 | 4F | 01 | 4E | 7C | Ã..€.Ã.%.O.N     |
| 44B61A3E0  | 73 | 64 | 6F | 5F | 6E | 65 | 74 | 77 | 6F | 72 | 6B | 5F | 74 | 69 | 6D | 65 | sdo_network_time |
| 44B61A3F0  | 5F | 75 | 70 | 64 | 5F | 74 | 72 | 69 | 67 | 0A | 49 | 4E | 53 | 54 | 45 | 41 | _upd_trig.INSTEA |
| 44B61A400  | 44 | 20 | 4F | 46 | 20 | 55 | 50 | 44 | 41 | 54 | 45 | 20 | 4F | 4E | 20 | 6D | D OF UPDATE ON m |
| 44B61A410  | 64 | 73 | 79 | 73 | 2E | 75 | 73 | 65 | 72 | 5F | 73 | 64 | 6F | 5F | 6E | 65 | dsys.user_sdo ne |
| 44B61A420  | 74 | 77 | 6F | 72 | 6B | 5F | 74 | 69 | 6D | 65 | 73 | 74 | 61 | 6D | 70 | 73 | twork_timestamps |
| 44B61A430  | 0A | 52 | 45 | 46 | 45 | 52 | 45 | 4E | 43 | 49 | 4E | 47 | 20 | 4F | 4C | 44 | .REFERENCING OLD |
| 44B61A440  | 20 | 41 | 53 | 20 | 6F | 20 | 4E | 45 | 57 | 20 | 41 | 53 | 20 | 6E | 0A | 46 | AS o NEW AS n.F  |
| 44B61A450  | 4F | 52 | 20 | 45 | 41 | 43 | 48 | 20 | 52 | 4F | 57 | 0A | FF | 01 | 80 | 03 | OR EACH ROW. €.  |
| 44B61A460  | C2 | 05 | 23 | 02 | C1 | 02 | 02 | C1 | 02 | 01 | 80 | 01 | 80 | 01 | 80 | FF | Ã.#.Ã.Ã..€.€.    |
| 44B61A470  | 02 | C1 | 06 | 02 | C1 | 02 | 02 | C1 | 0A | 01 | 80 | FE | B2 | 01 | 44 | 45 | .Ã..Ã.Ã..€t..DE  |
| 44B61A480  | 43 | 4C | 41 | 52 | 45 | 0A | 20 | 20 | 75 | 73 | 65 | 72 | 5F | 6E | 61 | 6D | CLARE. user_nam  |
| 44B61A490  | 65 | 20 | 20 | 20 | 20 | 56 | 41 | 52 | 43 | 48 | 41 | 52 | 32 | 28 | 32 | 35 | e VARCHAR2(25    |
| 44B61A4A0  | 36 | 29 | 3B | 0A | 42 | 45 | 47 | 49 | 4E | 0A | 0A | 0A | 20 | 20 | 75 | 73 | 6);.BEGIN... us  |
| 44B61A4B0  | 65 | 72 | 5F | 6E | 61 | 6D | 65 | 20 | 3A | 3D | 20 | 73 | 79 | 73 | 5F | 63 | er_name := sys_c |
| 44B61A4C0  | 6F | 6E | 74 | 65 | 78 | 74 | 28 | 27 | 75 | 73 | 65 | 72 | 65 | 6E | 76 | 27 | ontext('userenv  |
| 44B61A4D0  | 2C | 20 | 27 | 73 | 65 | 73 | 69 | 6F | 6E | 5F | 75 | 73 | 65 | 72 | 27 |    | , 'session_user' |
| 44B61A4E0  | 29 | 3B | 0A | 20 | 20 | 55 | 50 | 44 | 41 | 54 | 45 | 20 | 73 | 64 | 6F | 5F | );. UPDATE sdo_  |
| 44B61A4F0  | 6E | 65 | 74 | 77 | 6F | 72 | 6B | 5F | 74 | 69 | 6D | 65 | 73 | 74 | 61 | 6D | network_timestam |
| 44B61A500  | 70 | 73 | 0A | 20 | 20 | 20 | 53 | 45 | 54 | 28 | 6E | 65 | 74 | 77 | 6F | 72 | ps. SET(network  |
| 44B61A510  | 6B | 2C | 74 | 61 | 62 | 6C | 65 | 5F | 6E | 61 | 6D | 65 | 2C | 6C | 61 | 73 | k,table_name,las |
| 44B61A520  | 74 | 5F | 64 | 6D | 6C | 5F | 74 | 69 | 6D | 65 | 29 | 0A | 20 | 20 | 20 | 20 | t_dml_time).     |
| 44B61A530  | 20 | 20 | 3D | 0A | 20 | 20 | 20 | 28 | 53 | 45 | 4C | 45 | 43 | 54 | 0A | 20 | =. (SELECT.      |
| 44B61A540  | 20 | 20 | 20 | 20 | 20 | 3A | 6E | 2E | 6E | 65 | 74 | 77 | 6F | 72 | 6B | 2C | :n.network,      |
| 44B61A550  | 3A | 6E | 2E | 74 | 61 | 62 | 6C | 65 | 5F | 6E | 61 | 6D | 65 | 2C | 3A | 6E | :n.table_name,:n |
| 44B61A560  | 2E | 6C | 61 | 73 | 74 | 5F | 64 | 6D | 6C | 5F | 74 | 69 | 6D | 65 | 0A | 20 | .last_dml_time.  |
| 44B61A570  | 20 | 20 | 20 | 46 | 52 | 4F | 4D | 20 | 53 | 59 | 53 | 2E | 44 | 55 | 41 | 4C | FROM SYS.DUAL    |
| 44B61A580  | 29 | 0A | 20 | 20 | 20 | 20 | 57 | 48 | 45 | 52 | 45 | 20 | 20 | 6F | 77 | 6E | ). WHERE own     |
| 44B61A590  | 65 | 72 | 20 | 3D | 20 | 73 | 64 | 6F | 5F | 75 | 74 | 69 | 6C | 2E | 67 | 65 | er = sdo_util.ge |
| 44B61A5A0  | 74 | 5F | 71 | 75 | 6F | 74 | 65 | 64 | 5F | 6E | 61 | 6D | 65 | 28 | 75 | 73 | t_quoted_name(us |
| 44B61A5B0  | 65 | 72 | 5F | 6E | 61 | 6D | 65 | 29 | 0A | 20 | 20 | 20 | 20 | 20 | 20 | 41 | er_name). A      |
| 44B61A5C0  | 4E | 44 | 20 | 20 | 4E | 4C | 53 | 5F | 55 | 50 | 50 | 45 | 52 | 28 | 6E | 65 | ND NLS_UPPER(ne  |
| 44B61A5D0  | 74 | 77 | 6F | 72 | 6B | 29 | 20 | 3D | 20 | 4E | 4C | 53 | 5F | 55 | 50 | 50 | twork) = NLS_UPP |
| 44B61A5E0  | 45 | 52 | 28 | 3A | 6F | 2E | 6E | 65 | 74 | 77 | 6F | 72 | 6B | 29 | 0A | 20 | ER(:o.network).  |
| 44B61A5F0  | 20 | 20 | 20 | 20 | 20 | 41 | 4E | 44 | 20 | 20 | 4E | 4C | 53 | 5F | 55 | 50 | AND NLS UP       |
| 44B61A600  | 50 | 45 | 52 | 28 | 74 | 61 | 62 | 6C | 65 | 5F | 6E | 61 | 6D | 65 | 29 | 20 | PER(table name)  |
| 44B61A610  | 3D | 20 | 4E | 4C | 53 | 5F | 55 | 50 | 50 | 45 | 52 | 28 | 3A | 6F | 2E | 74 | = NLS_UPPER(:o.t |
| 44B61A620  | 61 | 62 | 6C | 65 | 5F | 6E | 61 | 6D | 65 | 29 | 3B | 0A | 45 | 4E | 44 | 3B | able_name);.END; |
| 44B61A630  | 2C | 02 | 17 | 04 | C3 | 08 | 25 | 22 | 01 | 80 | 01 | 80 | 01 | 80 | 01 | 80 | ...Ã.%.Ã.€.€.    |
| 44B61A640  | 01 | 80 | FF | FF | FF | FF | 01 | 80 | 03 | C2 | 05 | 23 | FF | 02 | C1 | 02 | .€'...€.Ã.#.Ã.   |
| 44B61A650  | 01 | 80 | 01 | 80 | 01 | 80 | FF | 02 | C1 | 06 | 02 | C1 | 02 | 02 | C1 | 0A | .€.€..€.Ã.Ã.Ã.   |
| 44B61A660  | 01 | 80 | FE | B2 | 01 | 44 | 45 | 43 | 4C | 41 | 52 | 45 | 0A | 20 | 20 | 75 | .€t..DECLARE. u  |
| 44B61A670  | 73 | 65 | 72 | 5F | 6E | 61 | 6D | 65 | 20 | 20 | 20 | 20 | 20 | 56 | 41 | 52 | ser_name VARC    |
| 44B61A680  | 48 | 41 | 52 | 32 | 28 | 32 | 35 | 36 | 29 | 3B | 0A | 42 | 45 | 47 | 49 | 4E | HAR2(256);.BEGIN |
| 44B61A690  | 0A | 0A | 0A | 20 | 20 | 75 | 73 | 65 | 72 | 5F | 6E | 61 | 6D | 65 | 20 | 3A | ... user_name :  |
| 44B61A6A0  | 3D | 20 | 73 | 79 | 73 | 5F | 63 | 6F | 6E | 74 | 65 | 78 | 74 | 28 | 27 | 75 | = sys_context('u |
| 44B61A6B0  | 73 | 65 | 72 | 65 | 6E | 76 | 27 | 2C | 20 | 27 | 73 | 65 | 73 | 73 | 69 | 6F | serenv', 'sessio |
| 44B61A6C0  | 6E | 5F | 75 | 73 | 65 | 72 | 27 | 29 | 3B | 0A | 20 | 20 | 55 | 50 | 44 | 41 | n_user');. UPDA  |

Tu vidíme *zadefinovanie reportu do log tabuľky*, čo slúži ako *falšovaný report*.  
*(nie používateľ vykonal niečo, čo systém zaregistruje, ale je to autokonfigurované=útok, vlastne zamaskovali niečo čo tam vôbec nepatrí za legítimný jav)*

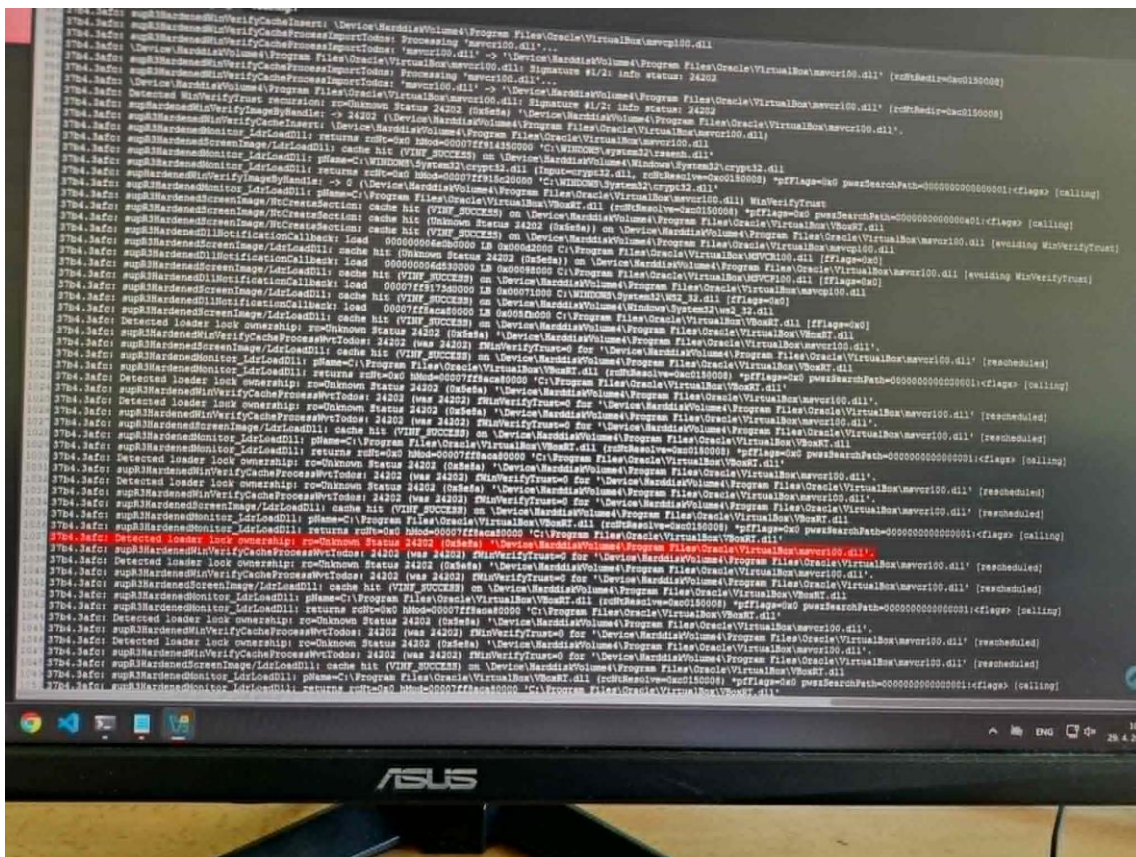
# Analýza log reportov, artefaktov z image RAM, VirtualBox

## Prečo

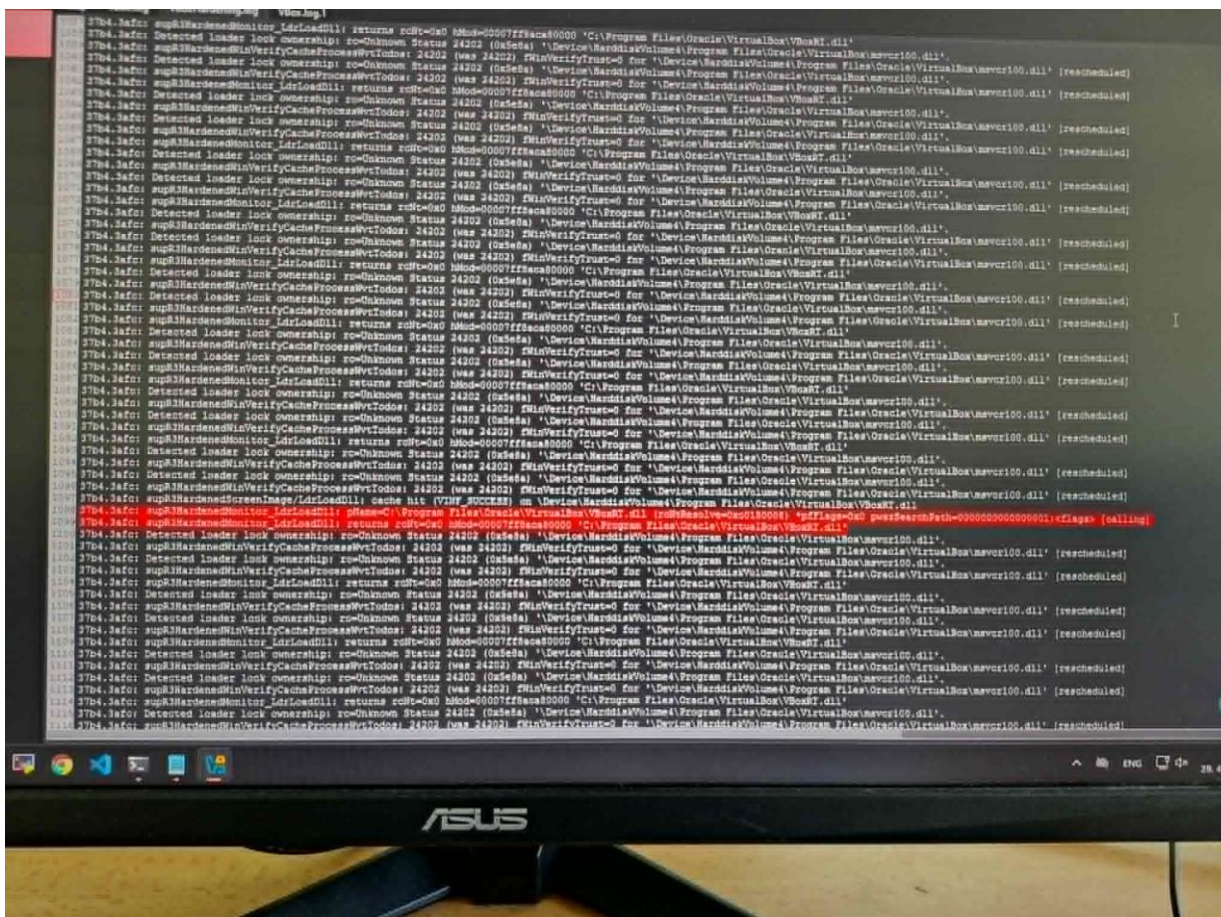
Lebo *WinVerifyCacheScheduleImports* overí reporty ale aj *vopred zamaskované falšované reporty L2 Cache cez SSH a virtuálneho stroja bezp s* operačným systémom *Debian(64-bit)*, to vidíme v log reportoch samotného virtuálneho stroja.







Vyhľadavanie súboru a sprístupnení súboru neoprávnene (obide Windows)





```

1211 00:00:04.012813 SSM: Saved state info:
1212 00:00:04.012818 SSM: Build Type: release
1213 00:00:04.012823 SSM: Host OS: win.amd64
1214 00:00:04.012960 PCI: PIIX3/0: register 60: 80 -> 8b
1215 00:00:04.012964 PCI: PIIX3/0: register 61: 00 -> 8a
1216 00:00:04.012966 PCI: PIIX3/0: register 62: 00 -> 89
1217 00:00:04.012969 PCI: PIIX3/0: register 63: 00 -> 8b
1218 00:00:04.012971 PCI: PIIX3/0: register 6d: 00 -> ef
1219 00:00:04.012973 PCI: PIIX3/0: register 6e: 00 -> be
1220 00:00:04.012977 PCI: piix3ide/0: 8-bit field LATENCY_TIMER: 0 -> 40
1221 00:00:04.012980 PCI: piix3ide/0: 32-bit field BASE_ADDRESS_4: 1 -> d001
1222 00:00:04.012984 PCI: piix3ide/0: register 41: 80 -> c0
1223 00:00:04.012986 PCI: piix3ide/0: register 42: 00 -> 03
1224 00:00:04.012988 PCI: piix3ide/0: register 43: 80 -> e3
1225 00:00:04.012991 PCI: piix3ide/0: register 48: 00 -> 04
1226 00:00:04.012993 PCI: piix3ide/0: register 4b: 00 -> 02

```

***LATENCY\_TIMER*** v prípade takéhoto princípu spôsobí *meškanie toku dát*, totiž *neide o legítimný prístup*, preto *SYN ACK* odpovede trvajú aj 10 minút s *duplicitnými outputmi*.

Zašifrovanie síťovej komunikácie ***BCryptOpenAlgorithmProvider, .dll***

```

678 37b4.3afc: supR3HardenedWinVerifyCacheInsert: \Device\HarddiskVolume4\Windows\System32\bcryptprimitives.dll
679 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: pName=C:\WINDOWS\system32\bcryptprimitives.dll (rcNtResolve=0xc0150008) *pfFlags=0x0 pwszSearchPath=C:\WINDOWS\system32\bcryptprimitives.dll
680 37b4.3afc: supR3HardenedDllNotificationCallback: load 00007ff915ba0000 LB 0x0007a000 C:\WINDOWS\system32\bcryptprimitives.dll [fFlags=0x0]
681 37b4.3afc: supR3HardenedScreenImage/LdrLoadDll: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\bcryptprimitives.dll [fFlags=0x0]
682 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: returns rcNt=0x0 hMod=00007ff915ba0000 'C:\WINDOWS\system32\bcryptprimitives.dll'
683 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('MD2',0,0) -> 0x0 (hAlgo=0000000001643230)
684 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('MD4',0,0) -> 0x0 (hAlgo=0000000001644000)
685 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('MD5',0,0) -> 0x0 (hAlgo=0000000001644350)
686 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('SHA1',0,0) -> 0x0 (hAlgo=00000000016446a0)
687 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('SHA256',0,0) -> 0x0 (hAlgo=00000000016449f0)
688 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('SHA512',0,0) -> 0x0 (hAlgo=0000000001644d40)
689 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('RSA',0,0) -> 0x0 (hAlgo=0000000001645100)
690 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('DSA',0,0) -> 0x0 (hAlgo=0000000001645450)
691 37b4.3afc: BCRYPT_OPEN_ALGORITHM_PROVIDER: ('ECDSA',0,0) -> 0x0 (hAlgo=0000000001645800)
692 37b4.3afc: supR3HardenedWinVerifyImageByHandle: -> 0 (\Device\HarddiskVolume4\Windows\System32\cryptsp.dll)
693 37b4.3afc: supR3HardenedWinVerifyCacheInsert: \Device\HarddiskVolume4\Windows\System32\cryptsp.dll
694 37b4.3afc: supR3HardenedDllNotificationCallback: load 00007ff914ac0000 LB 0x0001b000 C:\WINDOWS\system32\CRYPTSP.dll [fFlags=0x0]
695 37b4.3afc: supR3HardenedScreenImage/LdrLoadDll: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\cryptsp.dll [fFlags=0x0]
696 37b4.3afc: supR3HardenedWinVerifyImageByHandle: -> 0 (\Device\HarddiskVolume4\Windows\System32\rsaenh.dll)
697 37b4.3afc: supR3HardenedWinVerifyCacheInsert: \Device\HarddiskVolume4\Windows\System32\rsaenh.dll (rcNtResolve=0xc0150008) *pfFlags=0x0 pwszSearchPath=C:\WINDOWS\system32\rsaenh.dll
698 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: pName=C:\WINDOWS\system32\rsaenh.dll (rcNtResolve=0xc0150008) *pfFlags=0x0 pwszSearchPath=C:\WINDOWS\system32\rsaenh.dll

```

***Sfalšovaná autentifikácia***

```

821 37b4.3afc: supR3HardenedScreenImage/LdrLoadDll: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\rsaenh.dll
822 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: pName=C:\WINDOWS\system32\rsaenh.dll (rcNtResolve=0xc0150008) *pfFlags=0x0 pwszSearchPath=C:\WINDOWS\system32\rsaenh.dll
823 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: returns rcNt=0x0 hMod=00007ff914350000 'C:\WINDOWS\system32\rsaenh.dll'
824 37b4.3afc: supR3HardenedScreenImage/LdrLoadDll: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\crypt32.dll
825 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: pName=C:\WINDOWS\system32\crypt32.dll (In
826 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: returns rcNt=0x0 hMod=00007ff915c20000 'C:\WINDOWS\system32\crypt32.dll'
827 37b4.3afc: supR3HardNtViCallWinVerifyTrustCatFile: WinVerifyTrust => 0x0; cat='C:\WINDOWS\system32\crypt32.dll'
828 37b4.3afc: g_pfnWinVerifyTrust=00007ff915482480
829 37b4.3afc: supR3HardenedScreenImage/preload: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\crypt32.dll
830 37b4.3afc: supR3HardenedScreenImage/LdrLoadDll: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\crypt32.dll
831 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: pName=C:\WINDOWS\system32\rsaenh.dll (rcNtResolve=0xc0150008) *pfFlags=0x0 pwszSearchPath=C:\WINDOWS\system32\rsaenh.dll
832 37b4.3afc: supR3HardenedMonitor_LdrLoadDll: returns rcNt=0x0 hMod=00007ff914350000 'C:\WINDOWS\system32\rsaenh.dll'
833 37b4.3afc: supR3HardenedScreenImage/LdrLoadDll: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\crypt32.dll

```

***Únik cache dát + spustenie externých príkazov***

```

37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0x5c8b74b684ba00 C=US, O=Entrust, Inc., OU=www.digicert.com, CN=DigiCert Global
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xf5cd99e581e4ab00 C=US, O=SecureTrust Corporation, CN=SecureTrust CA
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xb2b0f0d2217f0bfb C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0x7c4fd32ec1bce000 C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xd4f2b673e5ccc600 C=PL, O=Unizeto Sp. z o.o., CN=Certum CA
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xb28612a94b4dad00 C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High As
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xe27add30c524b600 C=SE, O=GlobalSign nv-sa, CN=GlobalSign Code Signing Root R45
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0x357a29080824af00 C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0x59fa1086271bf000 C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., CN=Go Dadd
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0x3401b15e3761c700 C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xc30e361765128000 C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0x491857ead79dde00 C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certificate
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xb3ff821d139e9bf0 OU=GlobalSign ECC Root CA - R5, O=GlobalSign, CN=GlobalSign
37b4.3afc: supR3HardenedWinIsDesiredRootCA: Adding 0xc02ba72a37dfbe300 C=PL, O=Unizeto Technologies S.A., OU=Certum Certification Auth
37b4.3afc: supR3HardenedWinRetrieveTrustedRootCAs: Added=44
37b4.3afc: SUPR3HardenedMain: Load Runtime...
37b4.3afc: \Device\HarddiskVolume4\Program Files\Oracle\VirtualBox\VBBoxRT.dll: Signature #1/2: info status: 24202
37b4.3afc: supR3HardenedMonitor_LdrLoadDll: returns rcRt=0x0 hMod=00007ff914350000 'C:\WINDOWS\system32\rsaseh.dll'
37b4.3afc: supR3HardenedWinVerifyCacheScheduleImports: Import todo: #0 'msvcrt100.dll'
37b4.3afc: supR3HardenedWinVerifyCacheScheduleImports: Import todo: #1 'msvcpl100.dll'
37b4.3afc: supR3HardenedWinVerifyCacheScheduleImports: Import todo: #2 'rport4.dll'
37b4.3afc: supR3HardenedWinVerifyCacheScheduleImports: Import todo: #3 'ws2_32.dll'
37b4.3afc: supR3HardenedWinVerifyImageByHandle: -> 0 (\Device\HarddiskVolume4\Program Files\Oracle\VirtualBox\VBBoxRT.dll) WinVerifyTrust
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: Processing 'ws2_32.dll'...
37b4.3afc: supR3HardenedMonitor_LdrLoadDll: returns rcRt=0x0 hMod=00007ff914350000 'C:\WINDOWS\system32\rsaseh.dll'
37b4.3afc: supR3HardenedWinVerifyCacheScheduleImports: Import todo: #26 'rport4.dll'
37b4.3afc: supR3HardenedWinVerifyImageByHandle: -> 0 (\Device\HarddiskVolume4\Windows\System32\ws2_32.dll) WinVerifyTrust
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: Processing 'rport4.dll'...
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: Processing 'rport4.dll'...
37b4.3afc: supR3HardenedScreenImage/Imports: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\rport4.dll [rcRtRedir
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: Processing 'msvcpl100.dll'...
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: 'rport4.dll' -> '\Device\HarddiskVolume4\Program Files\Oracle\VirtualBox\msvcpl
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: Processing 'rport4.dll'...
37b4.3afc: supR3HardenedScreenImage/Imports: cache hit (VINF_SUCCESS) on \Device\HarddiskVolume4\Windows\System32\rport4.dll [rcRtRedir
37b4.3afc: supR3HardenedMonitor_LdrLoadDll: returns rcRt=0x0 hMod=00007ff914350000 'C:\WINDOWS\system32\rsaseh.dll'
37b4.3afc: supR3HardenedWinVerifyCacheScheduleImports: Import todo: #0 'msvcrt100.dll'
37b4.3afc: supR3HardenedWinVerifyImageByHandle: -> 0 (\Device\HarddiskVolume4\Program Files\Oracle\VirtualBox\msvcpl100.dll) WinVerifyTrust
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: Processing 'msvcpl100.dll'...
37b4.3afc: supR3HardenedWinVerifyCacheProcessImportTodos: 'msvcrt100.dll' -> '\Device\HarddiskVolume4\Program Files\Oracle\VirtualBox\msvcrt

```

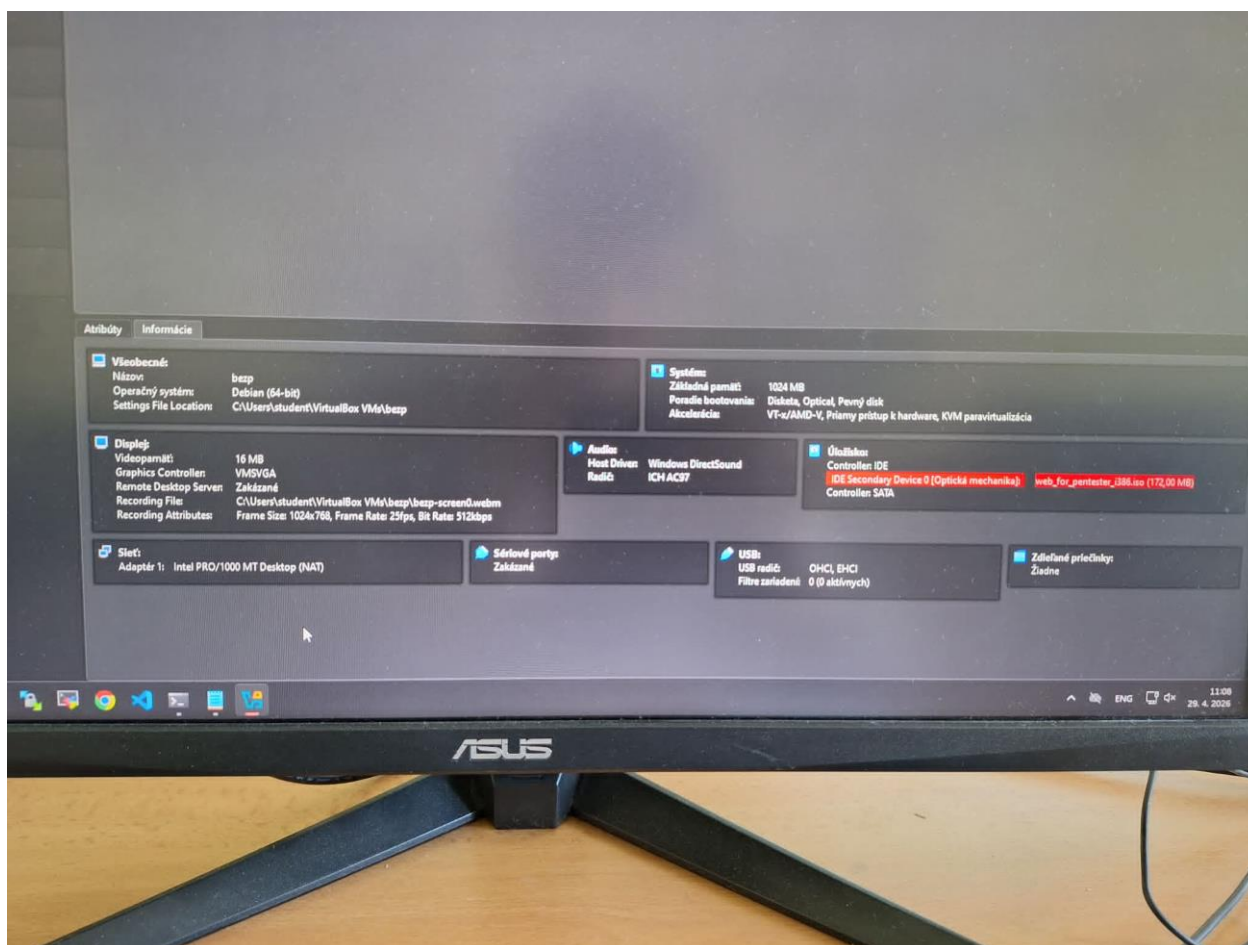
## Nepodarený prístup

```

37b4.3afc: Machine: VMBox.log.1
37b4.3afc: Timestamp: 0x8664 - amd64
37b4.3afc: Image Version: 0x2b0f54e7
37b4.3afc: SizeOfImage: 10.0
37b4.3afc: Resource Dir: 0x23000 (143340)
37b4.3afc: [Raw version resource found at 0x45! (ID/Name: 0x1; SubID/SubName: 0x409)]
37b4.3afc: ProductName: Microsoft Windows Operating System
37b4.3afc: ProductVersion: 10.0.22621.3085
37b4.3afc: FileVersion: 10.0.22621.3085 (WinBuild.160101.0800)
37b4.3afc: FileDescription: ApiSet Schema DLL
37b4.3afc: RtOpenDirectoryObject failed on \Driver: 0xc0000032
37b4.3afc: supR3HardenedWinFindAdversaries: 0x0
37b4.3afc: Calling main()
37b4.3afc: SUPR3HardenedMain: pszProgName=VirtualBoxVM fFlags=0x2
37b4.3afc: supR3HardenedWinInitAppBin(0x2): '\Device\HarddiskVolume4\Program Files\Oracle\VirtualBox\
37b4.3afc: \Device\HarddiskVolume4\Program Files\Oracle\VirtualBox\

```

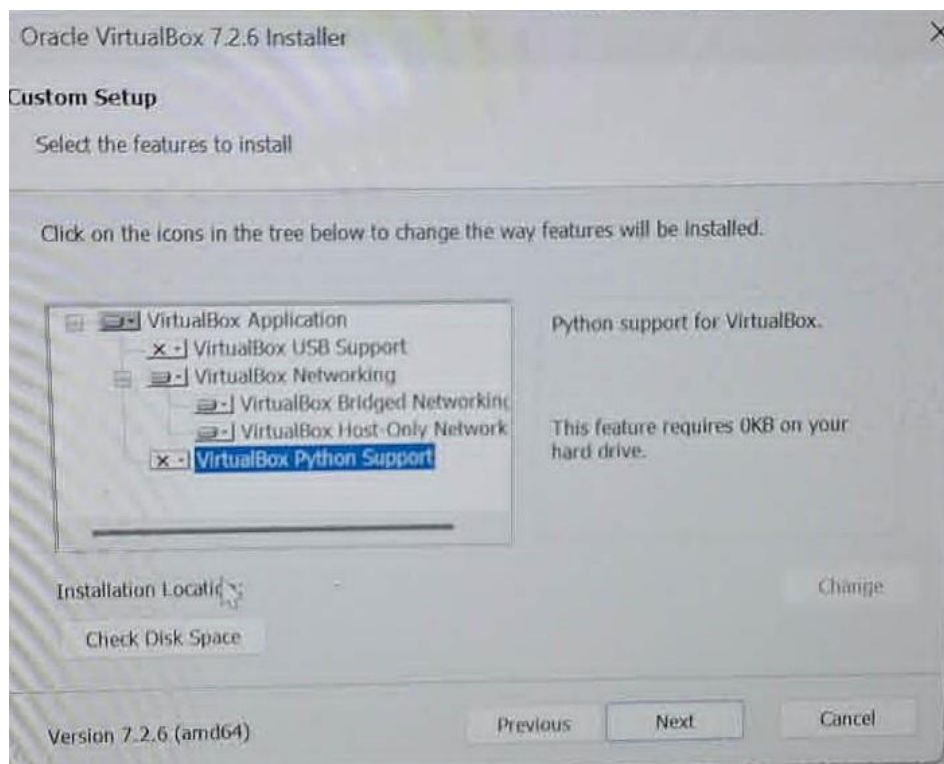
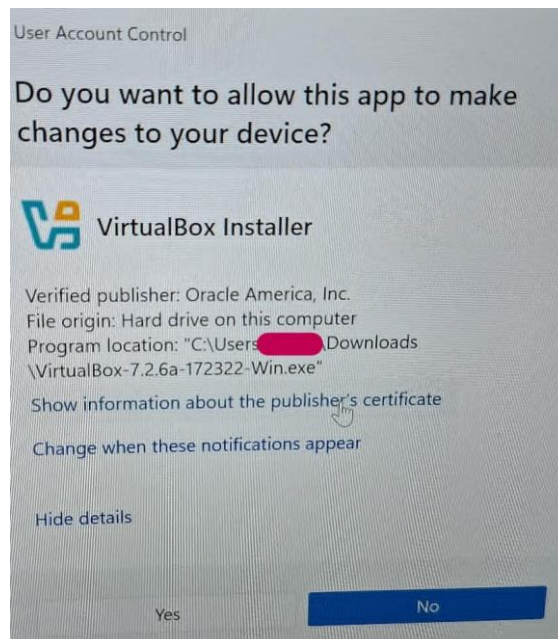
# Image VirtualBox zariadení



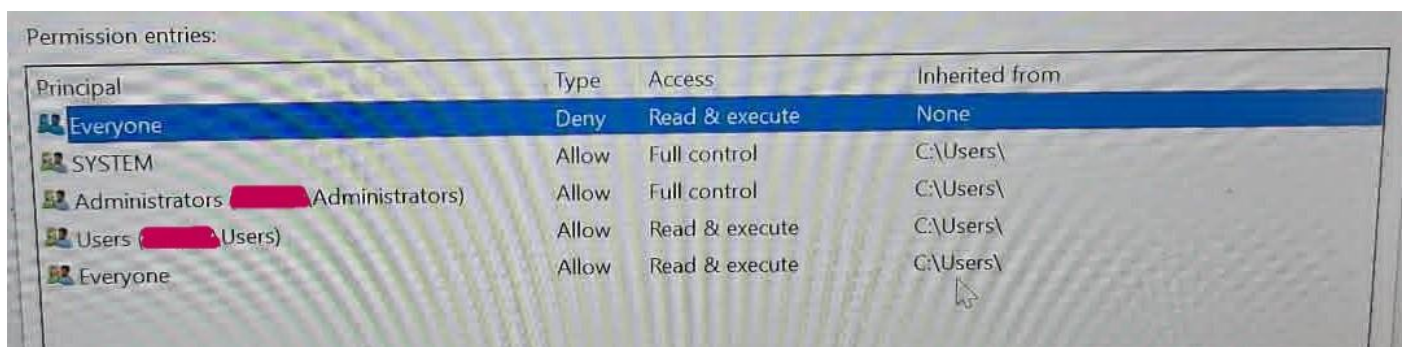
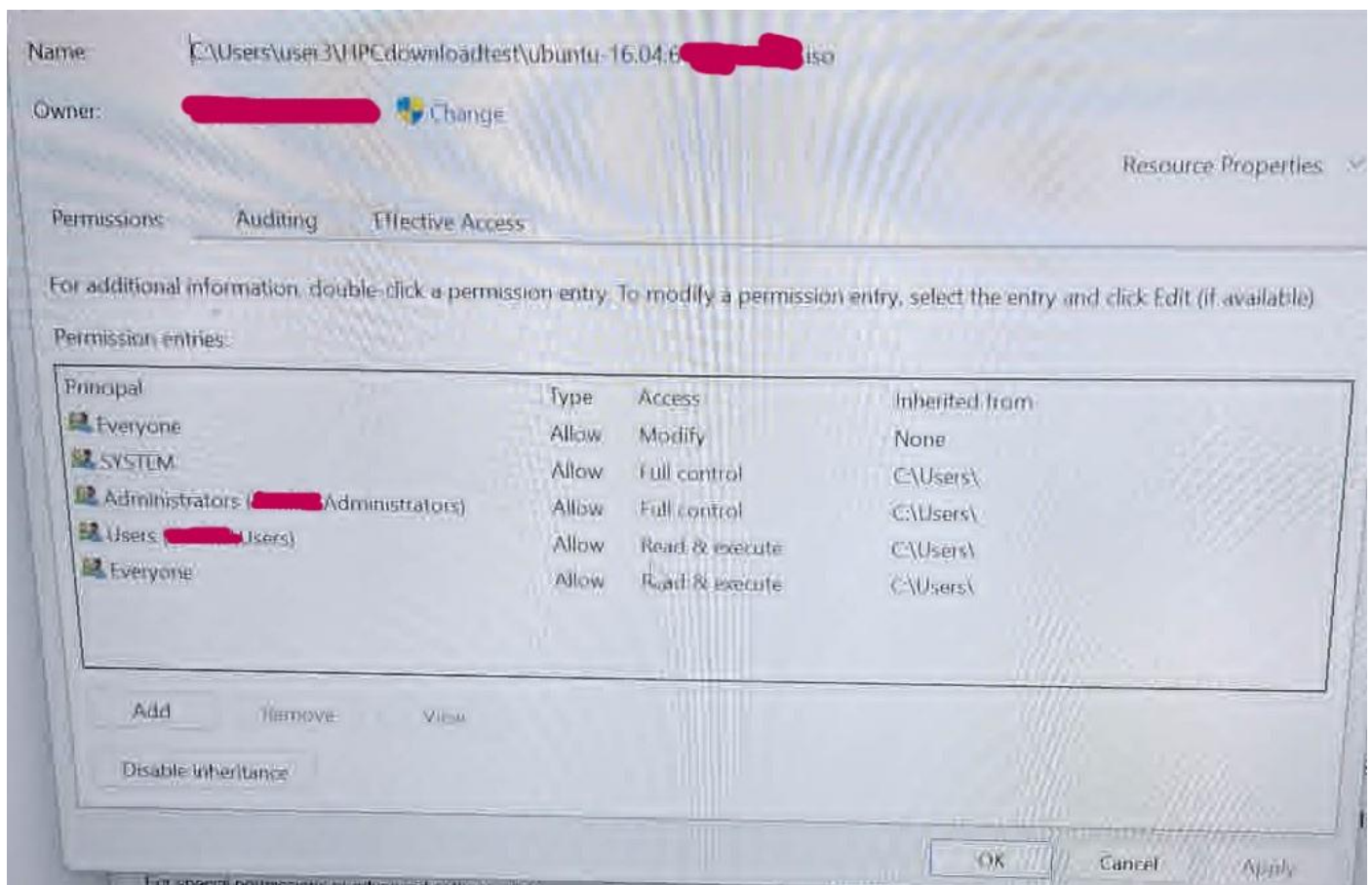
**Úložisko: IDE Secondary Device 0(Optická mechanika),  
web\_for\_pentester.\_i386.iso**

Nainštalovaný VirtualBox + **Operačné systémy (.iso image files)** a ich **problémy**:

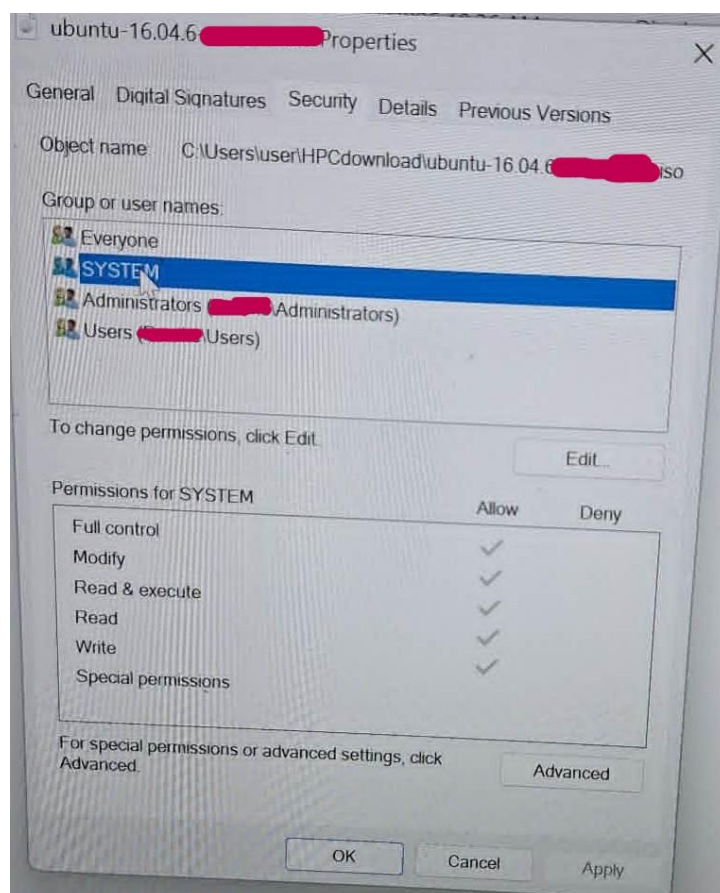
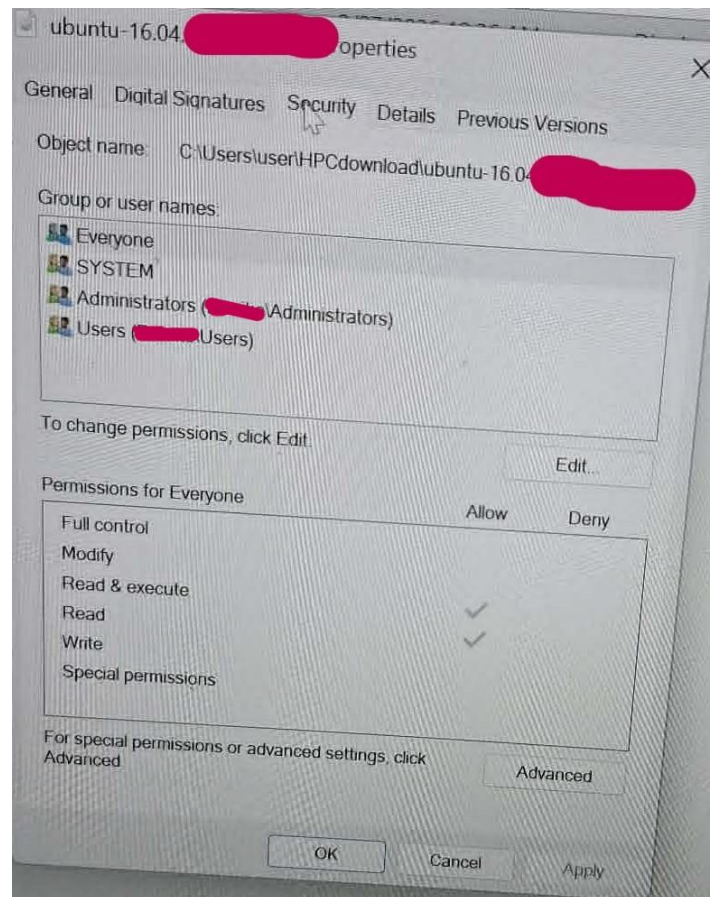
V prípade inštalácii VirtualBoxu je problém, že má **priamo prístup k pevnému disku** počítaču, preto každý VirtualBox by **nemal mať povolené rozšírenia python skript pluginov**, totiž pri **Open Source .iso** image-ov je to problém. (Voľne dostupné zdrojové kódy budú mať rozšírenia, čo práve pomocou takýchto skript pluginov kradnú údaje.)

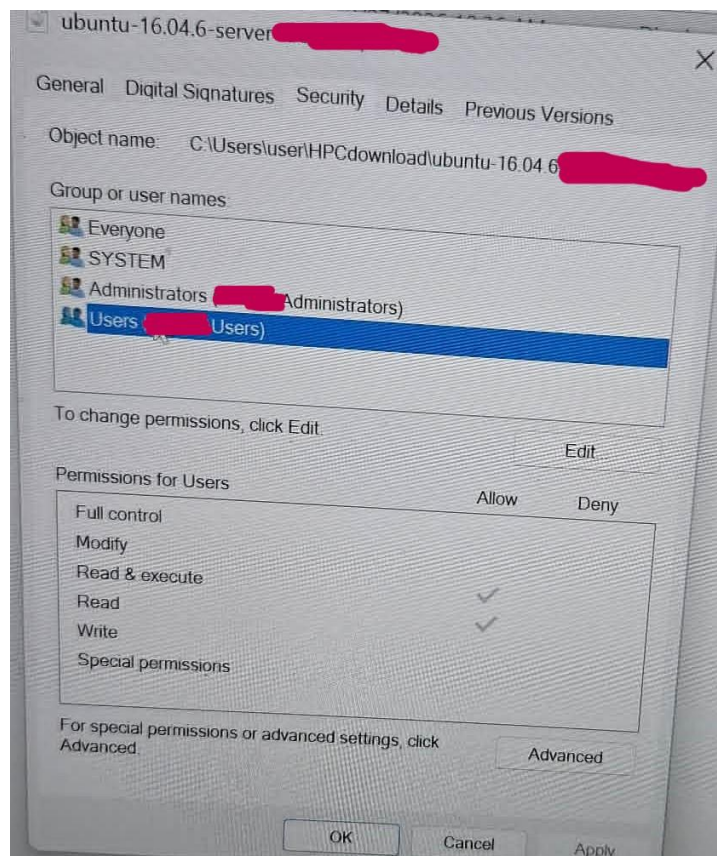
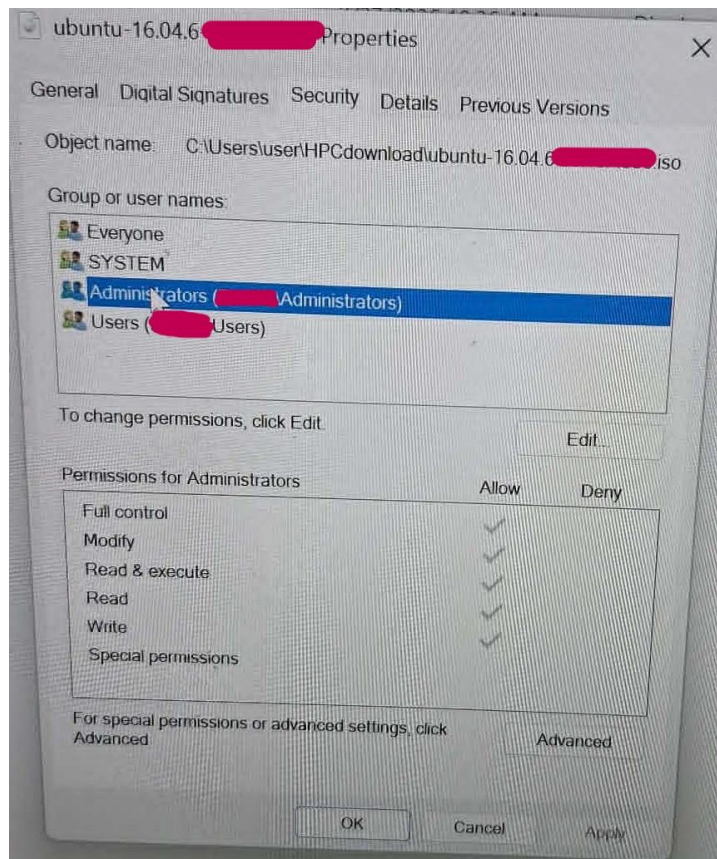


Žiadny iso image nesmie mať po stiahnutí v časti *Everyone mimo rámci C:\Users\* povolené **žiadne RWX** práva, totiž **bez zásahu používateľa** neporušený .iso image má RWX práva **len v rámci cesty C:\Users\** , teda **nesmie** tam byť **žiadna externá časť defaultne po stiahnutí nikdy**. V prípade výskytu externého RWX sekcii, treba dať “**deny**” **pre RWX**. Ale tieto sekcie už naznačia znaky útoku v rámci **servra**. (cez server, webovú stránku stiahneme ISO image)

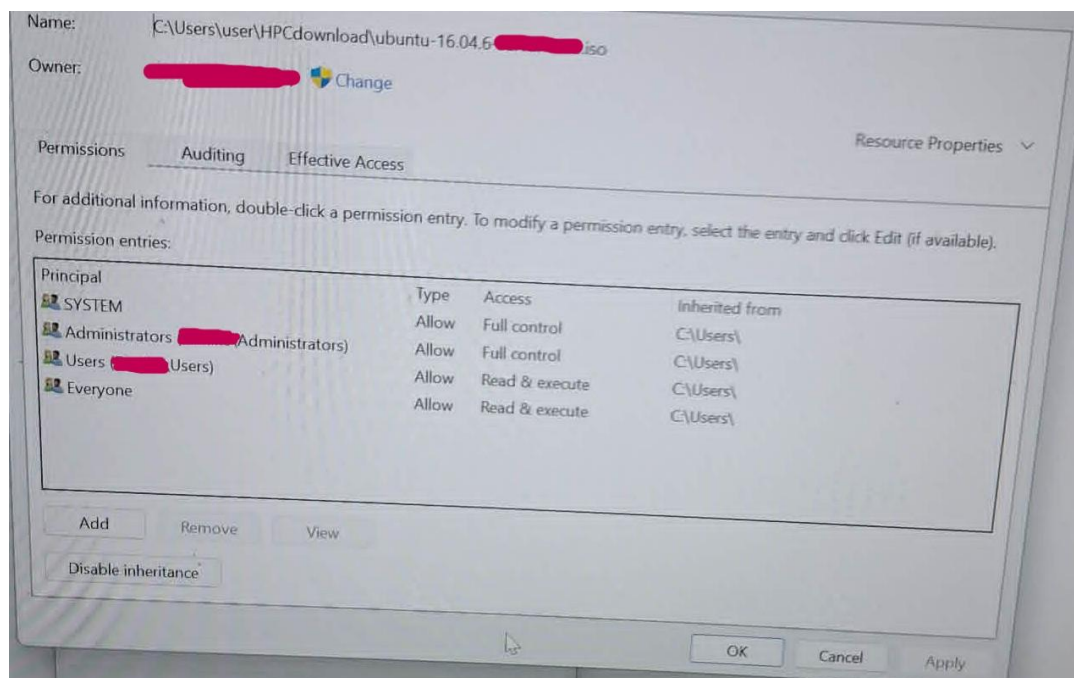


Pozrieme si jednotlivé **RWX**, **Modify**, **Full control** pravidlá (fotky):

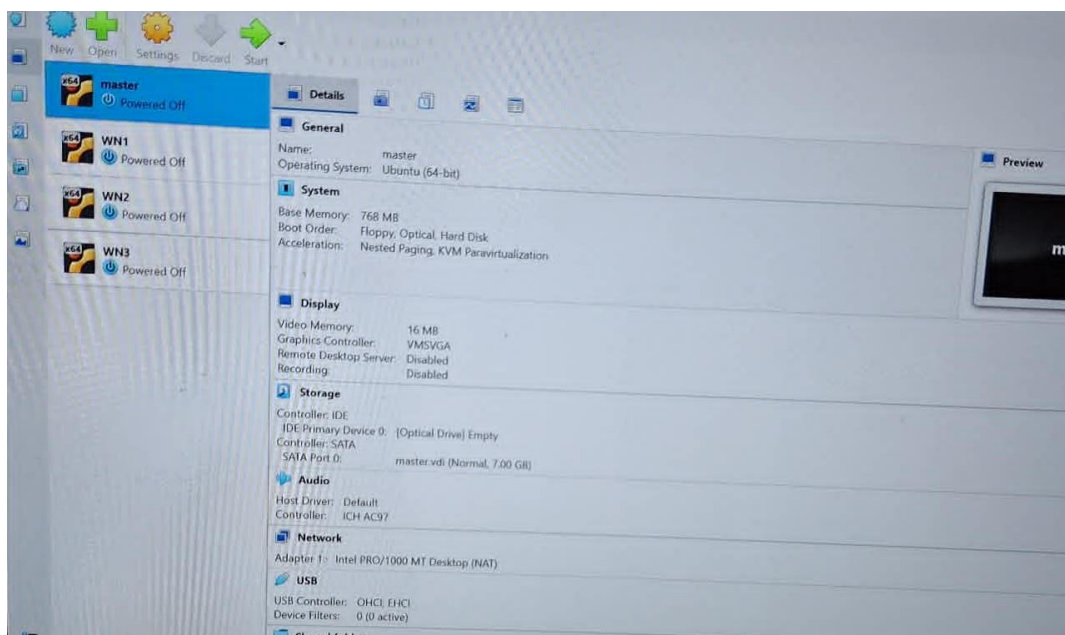




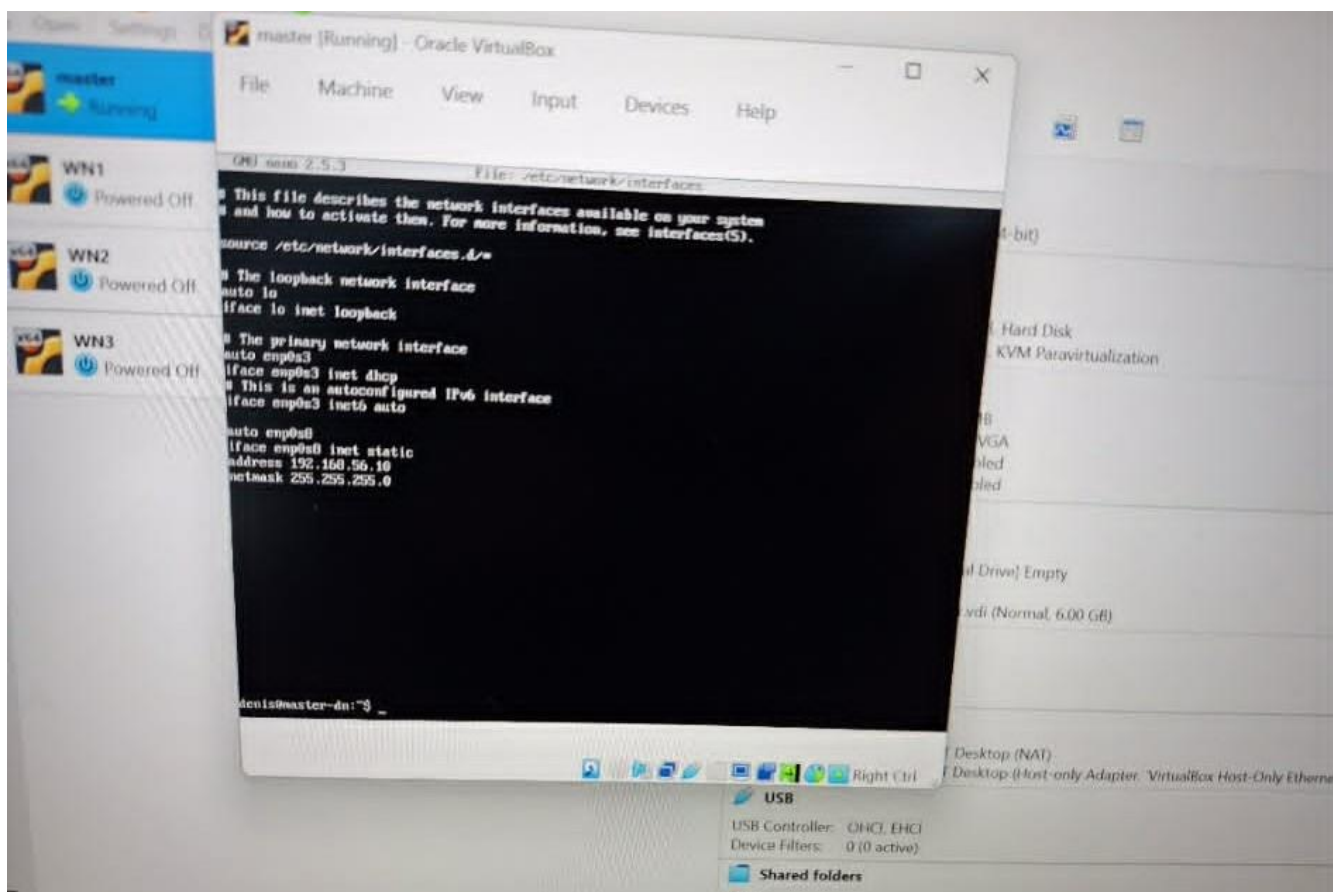
Správny **.iso image** bez zásahu používateľa, po stiahnutí zo servra by mal obsahovať **SYSTEM, Administrators, Users, Everyone** len v ceste **C:\Users\**



Po vyriešení a identifikácii problému s .ISO image spustíme 4 virtuálne stroje **Ubuntu Server 16.04.7 LTS**. Avšak musíme mať na vedomí, že tieto stroje ovplyvnia **fyzický disk , RAM , batériu** počítača, keď nie sú **perzistentné sieťové konfigurácie** nastavené správne. (Teda používateľ použije **verejnú IP adresu**, čo po **rebootovaní** následne **zmaže** a **prepíše** na **privátnu adresu**. Dôvodom je to, že **prvotná perzistentná konfigurácia pretrváva aj po zmenení adresy IP**. Verejná IP adresa slúži **ako server**, kde útočník **povolí vybraných host-ov**, zvyčajne **cez klávesové skratky jedného znaku ASCII** ako: ` . Server slúži na **optimalizáciu install apt** balíčkov a pomocou **sociálneho inžinierstva nefiltrované apt install** balíčky pomocou **zdrojových kódov (uvedené nižšie) presmeruje** súkromné údaje používateľa **cez sieť dial-up Set up a new router or access point via IPv6 autoconfiguration** or more.) Taktiež to slúži ako **keylogger** údajov, totiž **cez Control Panel – Hardware and Sound - .. - USB Input Device** útočník vie **nastaviť sieťové rozhrania počítača**. Taktiež je možnosť nastavenia **cez Control Panel** aj **sieťové adaptéry** ako **IPv6** (čo v našom prípade aj nastal, totiž IPv6 bola **autokonfigurovaná**, teda útočník sa už snažil prístupit k počítaču **ako k routeru na zahľtenie sietí používateľa**).



*Nesmie sa vyskytnúť žiadny **iface enp0s3 inet6 auto** , a jeho **zjavenie sa defaultne** naznačí o snahe manipulácie s použitím **rootovských práv** (napr. pomocou **softvérmí na kradnutie hesiel a SSH pripojení cez Control Panel Network adapters.** )*



Po vyšetrení **Ubuntu Server 16.04.7 LTS zdrojového kódu** a **GitHub** fór sme si dozvedeli, že open source softvér obsahuje Lamp stack na **odpočúvanie**, **presmerovanie údajov**, totiž **L1,L3 cache** sa nachádzajú **inde ako L2 cache**, čo sme v podstate aj overili pomocou príkazu **tracert**. Teda **zdrojový kód už ráta** s L2 a L1,L3 cache diferencií a **presmeruje (odpočúva) sieťový trafiku**, preto sa stane, že pri **IP** adrese **185.125.190.26** sa vyskytuje **duplicitný tok informácií**, resp. **latencia odpovedí aj v rádu minútach**, totiž **sieť sa nevie rozhodnúť kam poslať odpovede po presmerovaní, odpočúvaní údajov**. Nejednoznačnosť.

This repository was archived by the owner on Dec 20, 2025. It is now read-only.

Ubuntu 16.04: added ppa:ondrej/php and updated; apt is offering mysterious updates #1214

Closed



jrmmain opened on Aug 1, 2019 · edited by jrmmain

Edits · ...

I created a new VMWare VM just to test this. New Ubuntu 16.04 64-bit server install, with LAMP stack added. Updated and upgraded everything. Added ppa:ondrej/php and updated; apt immediately started showing a bunch of available updates that make no sense to me. Note that I haven't even installed anything from the ppa:ondrej/php source yet. Here are the updates it's telling me about:

```
libapache2-mod-php/xenial,xenial 2:7.3+69+ubuntu16.04.1+deb.sury.org+2+php7.3 all [upgradable from: 1:7.0+35ubuntu6.1]
libapache2-mod-php7.0/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
libjbig0/xenial 2.1-3.1+deb.sury.org~xenial+1 amd64 [upgradable from: 2.1-3.1]
libpcre3/xenial 2:8.43-1+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 2:8.38-3.1]
libxml2/xenial 2.9.4-1+deb.sury.org~xenial+2 amd64 [upgradable from: 2.9.3+dfsg1-1ubuntu0.6]
openssl/xenial 1.1.0h-2.0+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 1.0.2g-1ubuntu4.15]
php-common/xenial,xenial 2:69+ubuntu16.04.1+deb.sury.org+2+php7.3 all [upgradable from: 1:35ubuntu6.1]
php-mysql/xenial,xenial 2:7.3+69+ubuntu16.04.1+deb.sury.org+2+php7.3 all [upgradable from: 1:7.0+35ubuntu6.1]
php7.0-cli/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-common/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-json/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-mysql/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-opcache/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-readline/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
```

It's possible that these updates all make sense somehow, and are safe to install. Perhaps I'm being overly-cautious.



oerdnj on Aug 8, 2019

Owner · ...

I am not sure my goal here is to understand what makes and what doesn't make sense to you.

Could you please clearly describe the problem you are having? Yes, those are packages provided by the PPA, you either have trust or don't have trust in the PPA.

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants



```
libapache2-mod-php/xenial,xenial 2:7.3+69+ubuntu16.04.1+deb.sury.org+2+php7.3 all [upgradable from: 1:7.0+35ubuntu6.1]
libapache2-mod-php7.0/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
libjbig0/xenial 2.1-3.1+deb.sury.org~xenial+1 amd64 [upgradable from: 2.1-3.1]
libpcre3/xenial 2:8.43-1+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 2:8.38-3.1]
libxml2/xenial 2.9.4-1+deb.sury.org~xenial+2 amd64 [upgradable from: 2.9.3+dfsg1-1ubuntu0.6]
openssl/xenial 1.1.0h-2.0+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 1.0.2g-1ubuntu4.15]
php-common/xenial,xenial 2:69+ubuntu16.04.1+deb.sury.org+2+php7.3 all [upgradable from: 1:35ubuntu6.1]
php-mysql/xenial,xenial 2:7.3+69+ubuntu16.04.1+deb.sury.org+2+php7.3 all [upgradable from: 1:7.0+35ubuntu6.1]
php7.0-cli/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-common/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-json/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-mysql/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-opcache/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
php7.0-readline/xenial 7.0.33-8+ubuntu16.04.1+deb.sury.org+1 amd64 [upgradable from: 7.0.33-0ubuntu0.16.04.5]
```

*Ubuntu server*, odkiaľ bol stiahnutý *poškodený .ISO image* file a po inštalácii sme si všimli *pokus o sieťový útok* má nekonzistentné umiestnenie *L2 cache*, totiž L1, L3 cache sa smeruje cez trasu hop 3 = 10.69.253.125 ([www.ubuntu.com](http://www.ubuntu.com)), avšak L2 cache sa smeruje cez 10.69.253.127, čo ihneď už na začiatku sieťovej trasy bude znamenať *problém synchronizácii* v prípade odpočúvaní (bud'. Sa vyskytne *latencia* alebo *duplicita output správ*, alebo oba)

```
C:\Windows\System32>tracert www.ubuntu.com

Tracing route to www.ubuntu.com [185.125.190.20]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.1.1
  2    26 ms    23 ms    23 ms  st-static-bckb-153.213-81-233.telecom.sk [213.81.233.153]
  3    27 ms    24 ms    24 ms  10.69.253.125
  4    28 ms    26 ms    25 ms  80.156.161.128
  5    26 ms    25 ms    25 ms  62.159.61.127
  6    56 ms    63 ms    54 ms  ae2.3215.edge7.lon1.neo.colt.net [171.75.8.71]
  7     *       50 ms     *      swp10.il3-core2.canonical.com [194.88.86.2]
  8    48 ms    49 ms    49 ms  website-content-cache-1.ps5.canonical.com [185.125.190.20]

Trace complete.
```

```
C:\Windows\System32>tracert website-content-cache-1.ps5.canonical.com

Tracing route to website-content-cache-1.ps5.canonical.com [185.125.190.20]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    26 ms    24 ms    24 ms  st-static-bckb-153.213-81-233.telecom.sk [213.81.233.153]
  3    29 ms    24 ms    24 ms  10.69.253.125
  4    27 ms    26 ms    26 ms  80.156.161.128
  5    28 ms    26 ms    25 ms  62.159.61.127
  6    56 ms    62 ms     *      ae2.3215.edge7.lon1.neo.colt.net [171.75.8.71]
  7    50 ms    49 ms    49 ms  swp10.il3-core2.canonical.com [194.88.86.2]
  8    50 ms    48 ms    50 ms  website-content-cache-1.ps5.canonical.com [185.125.190.20]

Trace complete.
```

*L1 cache* cez Hop3 ide cez *IP* adresu *10.69.253.125*, je to oficiálna trasa [www.ubuntu.com](http://www.ubuntu.com). Akákoľvek iná *zmena sieťovej trasy* sa udeje pomocou *COST* trias, čo vyvoláva zmenu trias paketov v niektorých prípadoch. (napr. Pri situáciách, keď potrebujeme *inú trasu na server*, kde máme *únik dát*.)

```

C:\Windows\System32>tracert website-content-cache-2.ps5.canonical.com

Tracing route to website-content-cache-2.ps5.canonical.com [185.125.190.21]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  192.168.1.1
  2   26 ms   24 ms   24 ms  st-static-bckb-153.213-81-233.telecom.sk [213.81.233.153]
  3   25 ms   26 ms   28 ms  10.69.253.127
  4   27 ms   25 ms   26 ms  80.156.161.128
  5   37 ms   26 ms   33 ms  62.159.61.127
  6   56 ms    *      56 ms  ae2.3215.edge7.lon1.neo.colt.net [171.75.8.71]
  7   57 ms   54 ms   54 ms  swp10.il3-core2.canonical.com [194.88.86.2]
  8   51 ms   49 ms   49 ms  website-content-cache-2.ps5.canonical.com [185.125.190.21]

Trace complete.

```

**L2 cache** cez Hop3 ide cez **IP** adresu **10.69.253.127** , preto bude mať **problém so synchronizáciou** aj v **hodinách**, kde server **není vytážený**. (**11.22pm - 11.32pm** **latencia** a **duplicita output správ**)

```

C:\Windows\System32>tracert website-content-cache-3.ps5.canonical.com

Tracing route to website-content-cache-3.ps5.canonical.com [185.125.190.29]
over a maximum of 30 hops:

  1    3 ms    1 ms    1 ms  192.168.1.1
  2   24 ms   24 ms   23 ms  st-static-bckb-153.213-81-233.telecom.sk [213.81.233.153]
  3   25 ms   31 ms   30 ms  10.69.253.125
  4   48 ms   27 ms   25 ms  80.156.161.128
  5   27 ms   25 ms   26 ms  62.159.61.127
  6   56 ms   54 ms   55 ms  ae2.3215.edge7.lon1.neo.colt.net [171.75.8.71]
  7   56 ms   54 ms   54 ms  swp10.il3-core2.canonical.com [194.88.86.2]
  8   51 ms   49 ms   49 ms  website-content-cache-3.ps5.canonical.com [185.125.190.29]

Trace complete.

```

**L3 cache** cez Hop3 ide cez **IP** adresu **10.69.253.125**, čo je v poriadku.

**Latencia** v prípade smerovaní na cez **HOP3 10.69.253.127** v prípade sieťovej trasy IP adresy **tracert 185.125.190.26** mal **latenciu až 10 minút (port bonding)**

```

C:\Windows\System32>tracert 185.125.190.26

Tracing route to snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]
over a maximum of 30 hops:

```

```

  1    2 ms    1 ms    1 ms  192.168.1.1

```

```
C:\Windows\System32>tracert 185.125.190.26

Tracing route to snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  192.168.1.1
```

```
C:\Windows\System32>tracert 185.125.190.26

Tracing route to snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  192.168.1.1
```

```
C:\Windows\System32>tracert 185.125.190.26

Tracing route to snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]
over a maximum of 30 hops:

  1    3 ms    1 ms    1 ms  192.168.1.1
  2   27 ms   24 ms   24 ms  st-static-bckb-153.213-81-233.telecom.sk [213.81.233.153]
  3   26 ms   25 ms   24 ms  10.69.253.127
  4   28 ms   26 ms   26 ms  80.156.161.128
  5   27 ms   33 ms   26 ms  62.159.61.127
  6   59 ms    *    57 ms  ae2.3215.edge7.lon1.neo.colt.net [171.75.8.71]
  7   51 ms   48 ms   49 ms  swp10.il3-core2.canonical.com [194.88.86.2]
  8   55 ms   49 ms   52 ms  snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]

Trace complete.
```

```
C:\Windows\System32>tracert 185.125.190.26

Tracing route to snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]
over a maximum of 30 hops:

  1    3 ms    1 ms    1 ms  192.168.1.1
  2   27 ms   24 ms   24 ms  st-static-bckb-153.213-81-233.telecom.sk [213.81.233.153]
  3   26 ms   25 ms   24 ms  10.69.253.127
  4   28 ms   26 ms   26 ms  80.156.161.128
  5   27 ms   33 ms   26 ms  62.159.61.127
  6   59 ms    *    57 ms  ae2.3215.edge7.lon1.neo.colt.net [171.75.8.71]
  7   51 ms   48 ms   49 ms  swp10.il3-core2.canonical.com [194.88.86.2]
  8   55 ms   49 ms   52 ms  snapstore-content-cache-1.ps5.canonical.com [185.125.190.26]

Trace complete.

C:\Windows\System32>
```