7 - Fifty Shades of Grey Hat

Hungary

Details of Case

In early January 2021, Mr. CIC, a special agent in the FBI, learned that an individual only known as Mr. Evil Noodle is allegedly responsible for several of the most expensive computer intrusions of all time. Mr. Evil Noodle has a background in computer programming for the financial industry.

According to allegations, some of the various illegal activities and crimes, that Mr. Evil Noodle and the organization that he is a part of, may be involved in include:

- **Illegally accessing computer systems without authorization**
- **Phishing & ransomware attacks targeting financial institutions across the world that have collectively stolen over one billion dollars**
- **Illegal drug trafficking**
- **Illegal guns and weapons sales**

As illustrated by the information presented by Mr. CIC, a federal arrest warrant has been was issued for Mr. Evil Noodle within the United States with the following charges:

- **Suspicion of conspiracy to commit wire fraud**
- **Suspicion of conspiracy to commit computer-related fraud**
- **Suspicion of computer intrusion**

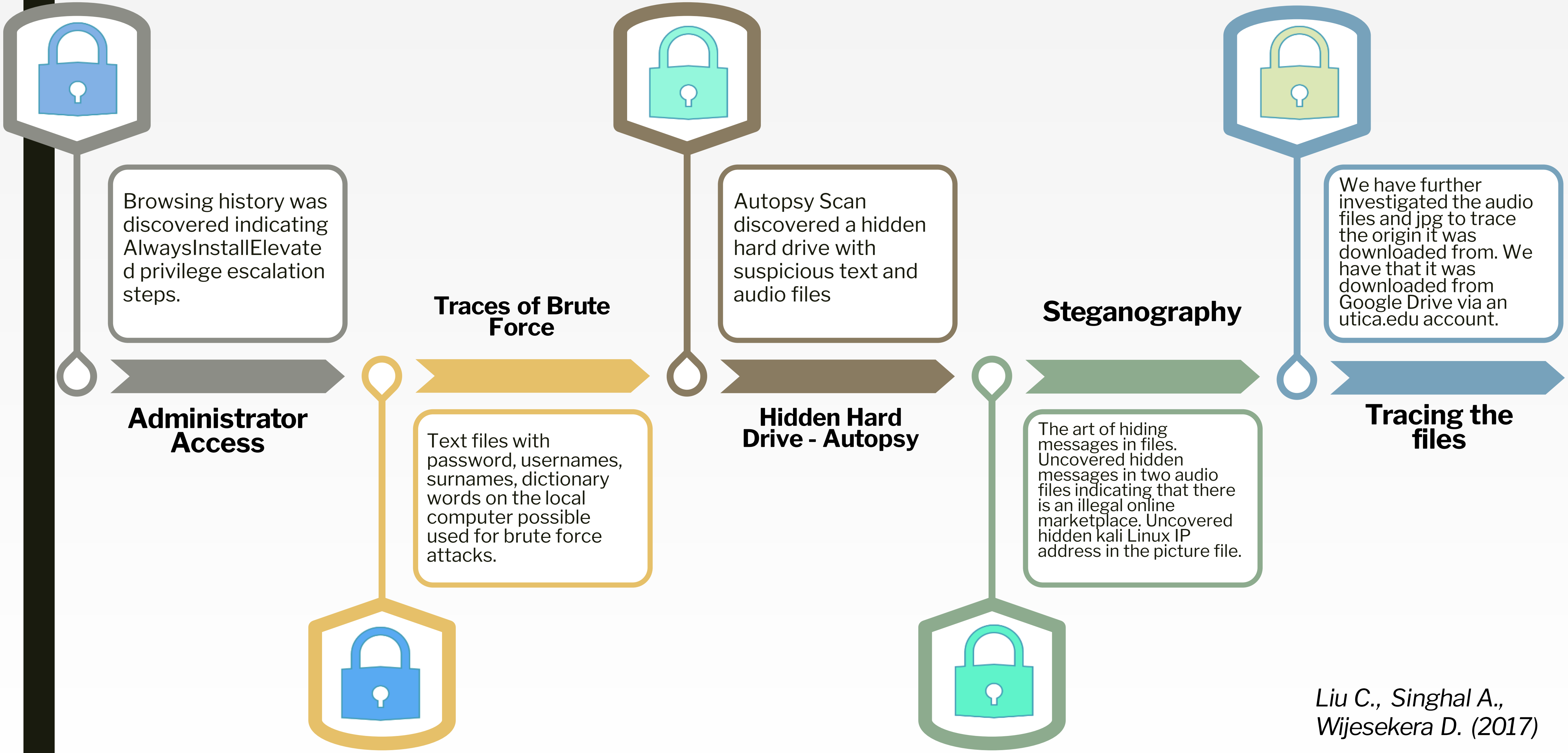
Investigation Scope

Initial Windows Machine

Discovered Kali Machine

Darknet Store

First Computer



Administrator Access

Browsing history was discovered indicating AlwaysInstallElevated privilege escalation steps.

Traces of Brute Force

Text files with password, usernames, surnames, dictionary words on the local computer possible used for brute force attacks.

Hidden Hard Drive - Autopsy

Autopsy Scan discovered a hidden hard drive with suspicious text and audio files

Steganography

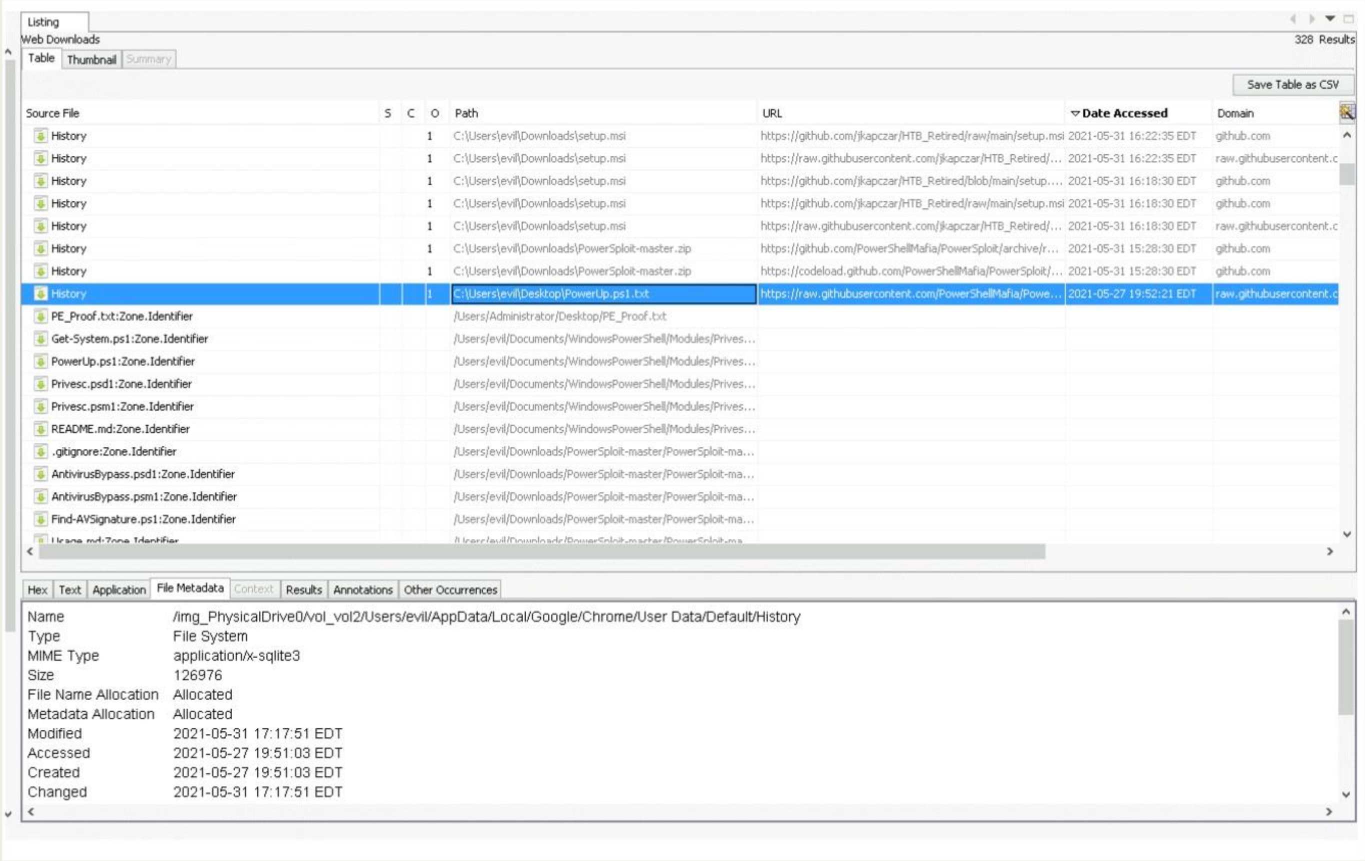
The art of hiding messages in files. Uncovered hidden messages in two audio files indicating that there is an illegal online marketplace. Uncovered hidden kali Linux IP address in the picture file.

Tracing the files

We have further investigated the audio files and jpg to trace the origin it was downloaded from. We have that it was downloaded from Google Drive via an utica.edu account.

Liu C., Singhal A., Wijesekera D. (2017)

Evidence #1 - Browser history

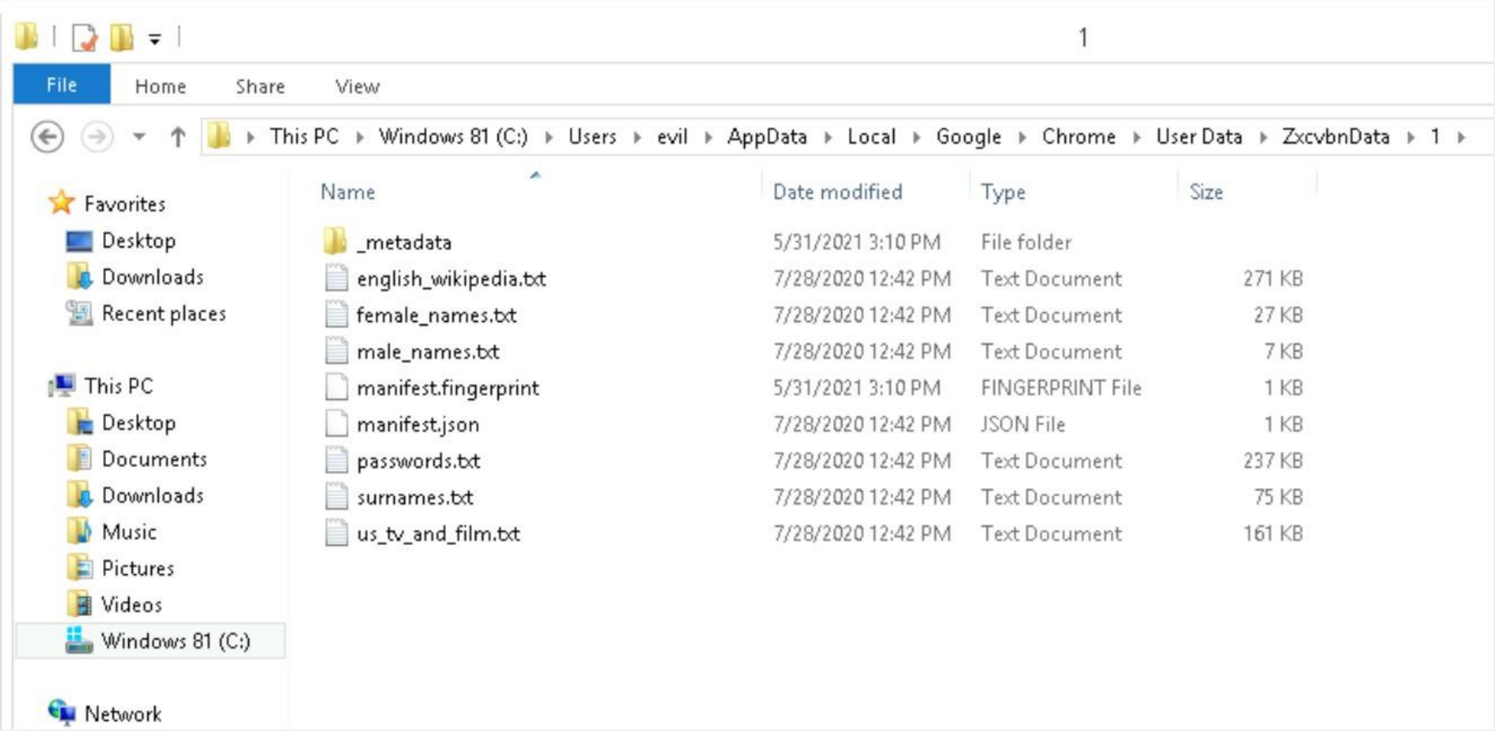


Source File	S	C	O	Path	URL	▽Date Accessed	Domain
History			1	C:\Users\evil\Downloads\setup.msi	https://github.com/jkapczar/HTB_Retired/raw/main/setup.msi	2021-05-31 16:22:35 EDT	github.com
History			1	C:\Users\evil\Downloads\setup.msi	https://raw.githubusercontent.com/jkapczar/HTB_Retired/...	2021-05-31 16:22:35 EDT	raw.githubusercontent.c
History			1	C:\Users\evil\Downloads\setup.msi	https://github.com/jkapczar/HTB_Retired/blob/main/setup....	2021-05-31 16:18:30 EDT	github.com
History			1	C:\Users\evil\Downloads\setup.msi	https://github.com/jkapczar/HTB_Retired/raw/main/setup.msi	2021-05-31 16:18:30 EDT	github.com
History			1	C:\Users\evil\Downloads\setup.msi	https://raw.githubusercontent.com/jkapczar/HTB_Retired/...	2021-05-31 16:18:30 EDT	raw.githubusercontent.c
History			1	C:\Users\evil\Downloads\PowerSploit-master.zip	https://github.com/PowerShellMafia/PowerSploit/archive/r...	2021-05-31 15:28:30 EDT	github.com
History			1	C:\Users\evil\Downloads\PowerSploit-master.zip	https://codeload.github.com/PowerShellMafia/PowerSploit/...	2021-05-31 15:28:30 EDT	github.com
History			1	C:\Users\evil\Desktop\PowerUp.ps1.txt	https://raw.githubusercontent.com/PowerShellMafia/Powe...	2021-05-27 19:52:21 EDT	raw.githubusercontent.c
PE_Proof.txt:Zone.Identifier				/Users/Administrator/Desktop/PE_Proof.txt			
Get-System.ps1:Zone.Identifier				/Users/evil/Documents/WindowsPowerShell/Modules/Prives...			
PowerUp.ps1:Zone.Identifier				/Users/evil/Documents/WindowsPowerShell/Modules/Prives...			
Privesc.psd1:Zone.Identifier				/Users/evil/Documents/WindowsPowerShell/Modules/Prives...			
Privesc.psm1:Zone.Identifier				/Users/evil/Documents/WindowsPowerShell/Modules/Prives...			
README.md:Zone.Identifier				/Users/evil/Documents/WindowsPowerShell/Modules/Prives...			
.gitignore:Zone.Identifier				/Users/evil/Downloads/PowerSploit-master/PowerSploit-ma...			
AntivirusBypass.psd1:Zone.Identifier				/Users/evil/Downloads/PowerSploit-master/PowerSploit-ma...			
AntivirusBypass.psm1:Zone.Identifier				/Users/evil/Downloads/PowerSploit-master/PowerSploit-ma...			
Find-AVSignature.ps1:Zone.Identifier				/Users/evil/Downloads/PowerSploit-master/PowerSploit-ma...			
Usage.md:Zone.Identifier				/Users/evil/Downloads/PowerSploit-master/PowerSploit-ma...			

Name	/img_PhysicalDrive0/vol_vol2/Users/evil/AppData/Local/Google/Chrome/User Data/Default/History
Type	File System
MIME Type	application/x-sqlite3
Size	126976
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2021-05-31 17:17:51 EDT
Accessed	2021-05-27 19:51:03 EDT
Created	2021-05-27 19:51:03 EDT
Changed	2021-05-31 17:17:51 EDT

The evidence shows the intention and the willingness of the perpetrator to gain unauthorized control over the compromised OS. - *U.S. Code § 2512 (1) (b)*

Evidence #2

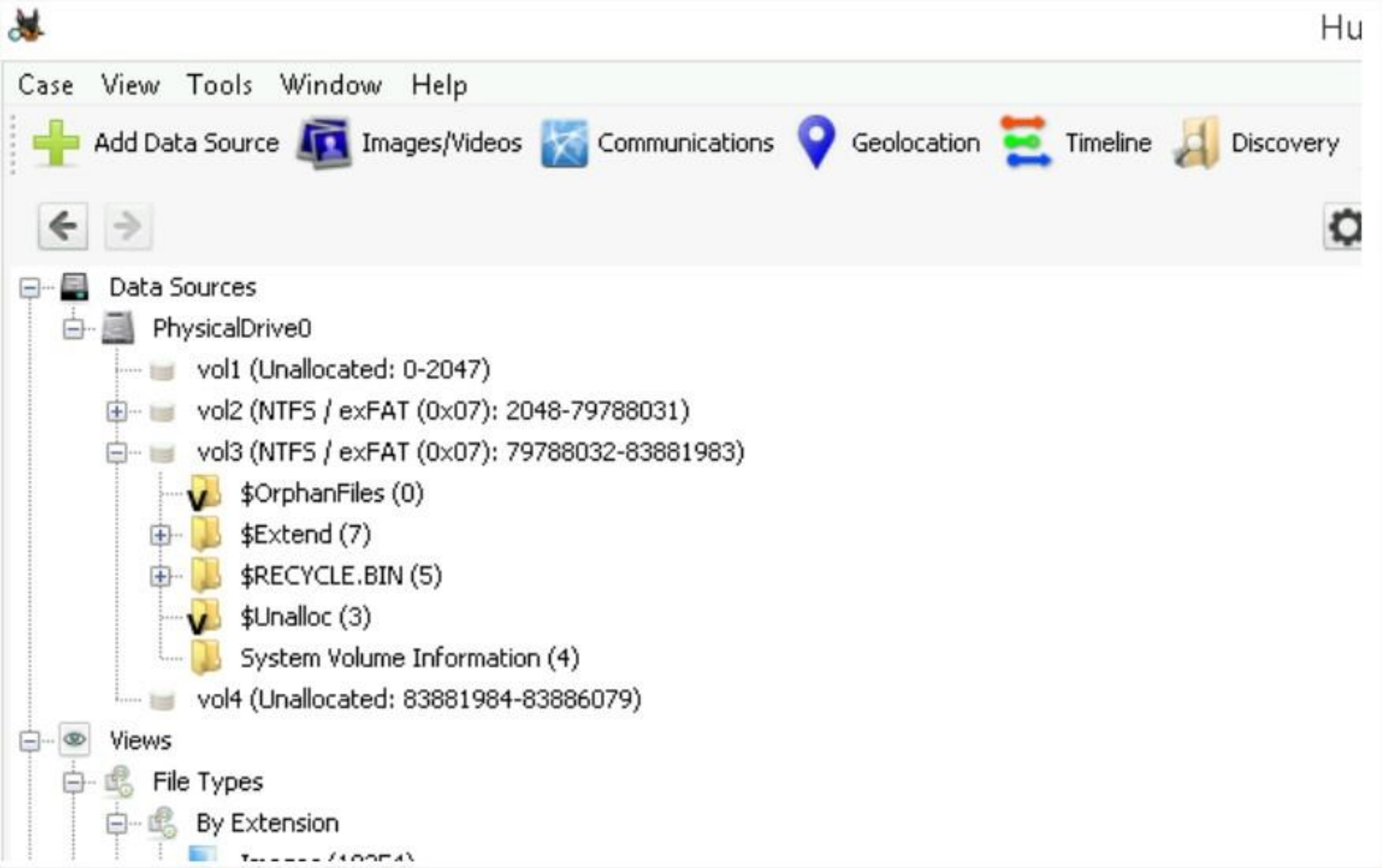


This PC ▸ Windows 81 (C:) ▸ Users ▸ evil ▸ AppData ▸ Local ▸ Google ▸ Chrome ▸ User Data ▸ ZxcvbnData ▸ 1 ▸

Name	Date modified	Type	Size
_metadata	5/31/2021 3:10 PM	File folder	
english_wikipedia.txt	7/28/2020 12:42 PM	Text Document	271 KB
female_names.txt	7/28/2020 12:42 PM	Text Document	27 KB
male_names.txt	7/28/2020 12:42 PM	Text Document	7 KB
manifest.fingerprint	5/31/2021 3:10 PM	FINGERPRINT File	1 KB
manifest.json	7/28/2020 12:42 PM	JSON File	1 KB
passwords.txt	7/28/2020 12:42 PM	Text Document	237 KB
surnames.txt	7/28/2020 12:42 PM	Text Document	75 KB
us_tv_and_film.txt	7/28/2020 12:42 PM	Text Document	161 KB

The evidence is a trace of illegal activities such as penetrating informational systems. - *U.S. Code § 2512 (1) (b)*

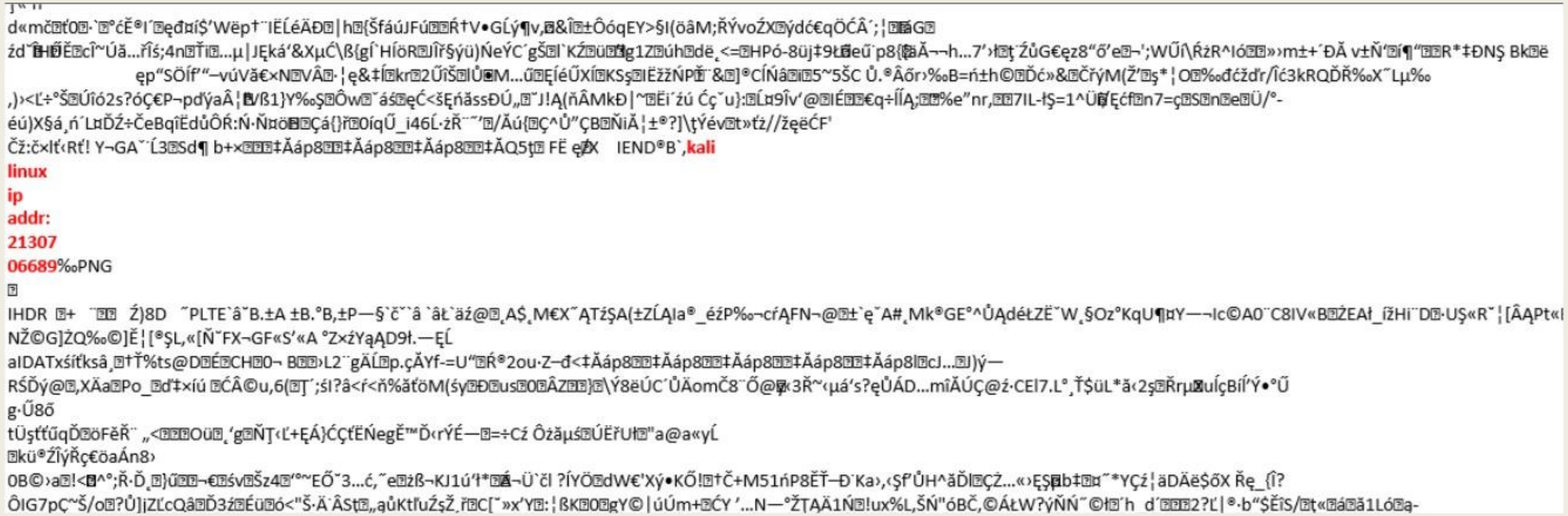
Evidence #3



```
Data Sources
    PhysicalDrive0
        vol1 (Unallocated: 0-2047)
        vol2 (NTFS / exFAT (0x07): 2048-79788031)
        vol3 (NTFS / exFAT (0x07): 79788032-83881983)
            $OrphanFiles (0)
            $Extend (7)
            $RECYCLE.BIN (5)
            $Unalloc (3)
            System Volume Information (4)
        vol4 (Unallocated: 83881984-83886079)
Views
    File Types
        By Extension
```

The evidence proves that the perpetrator tried to hide his illegal activities and whatever information he gained from them. - *18 U.S. Code § 371*

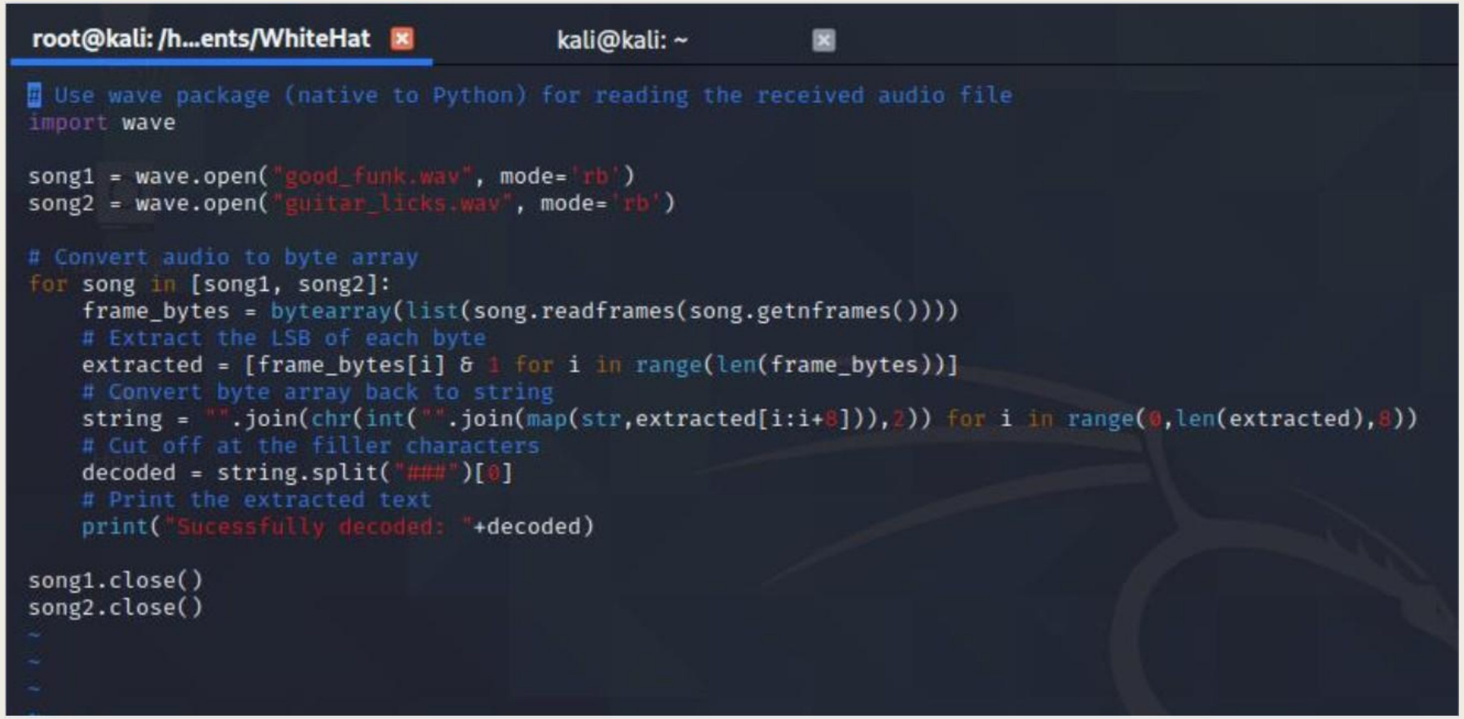
Evidence #4



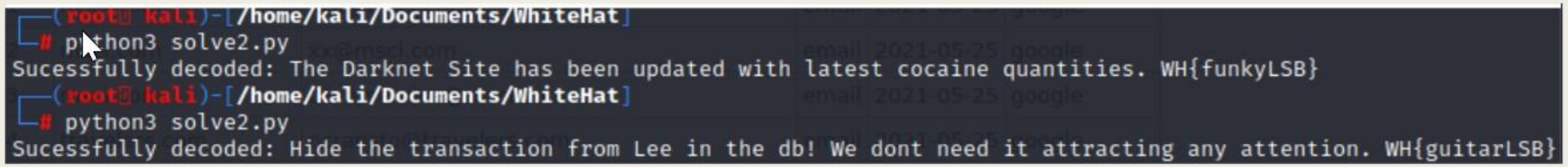
```
d«mč⍰ť0⍰·`⍰°ćĔ®I´⍰ęđ¤í$’Wëp†¨IĔĹéĂĐ⍰|h⍰{ŠfáúJFú⍰⍰Ŕ†V•GĹý¶v,⍰&Î⍰±ÔóqEY>§I(öâM;ŘÝvoŹX⍰ýdć€qÖĆÂ´;¦⍰⍰áG⍰
źd˘⍰H⍰ĔⓂcÎ~Úă…ř̂ś;4n⍰Ťi⍰…µ|JĘká‘&XµĆ\ß{gĺ`HíöR⍰Jîř§ýü)ŃeÝC´gŠ⍰l`KŹ⍰ü⍰⍰g1Z⍰úh⍰dë˛<=⍰HPó-8üj‡9Ł⍰eű¨p8{⍰ăĂ¬¬h…7’›ł⍰ţ˙ŹůG€ęz8“ő’e⍰¬';WŰí\ŔżR^Ió⍰⍰»›m±+´ĐĂ v±Ň‘⍰í¶“⍰⍰R*‡ĐNŞ Bk⍰ë
                         ęp“SÖÍf’“–vúVă€×N⍰VÂ⍰·¦ę&‡Í⍰kr⍰2ŰîŠ⍰IŮ⍰M…ű⍰ĘíéŰXÍ⍰KSş⍰IĔžžŃPŤ¨&⍰]®CĺŃâ⍰i⍰5~5ŠC Ů.®Âőr›%‰B=ń±h©⍰Ďć»&⍰ČřýM(Ž’⍰ş*¦O⍰%‰đćžďr/Îć3kRQĎŘ%‰X˝Lµ%‰
,)›<Ľ÷°Š⍰Úîó2s?óÇ€P¬pďýaÂ¦⍰/ß1}Y%‰Ş⍰Ôw⍰˘áś⍰ęĆ<šĘńăssĐÚ„⍰˘J!Ą(ňÂMkĐ|˜⍰Ëi´źú Ćç˘u}:⍰Ĺ¤9Îv‘@⍰IÉ⍰⍰€q÷ĺÍĄ;⍰⍰%e”nr,⍰⍰7IL-łŞ=1^Ü⍰/ĘćfⓂn7=ç⍰S⍰n⍰e⍰Ü/°-
éú)X§á¸ń´L¤ĎŹ÷ČeBqîËdůÔŔ:Ń·Ň¤ö⍰⍰Çá{}ř⍰0íqŰ_i46Ĺ·żŘ¨˝’⍰/Ăú{⍰Ç^Ů”ÇB⍰ŇiĂ¦±®?]\ţÝév⍰t»ťż//žęëĆF'
Čž:č×lť‹Rť! Y¬GA˘´Ĺ3⍰Sd¶ b+×⍰⍰⍰‡Ăáp8⍰⍰‡Ăáp8⍰⍰‡Ăáp8⍰⍰‡ĂQ5ţ⍰ FË ę⍰X    IEND®B`,kali
linux
ip
addr:
21307
06689%‰PNG
⍰
IHDR ⍰+  ¨⍰⍰  Ź)8D  ˝PLTE`â˘B.±A ±B.°B,±P—§`č˘`â `âŁ`äź@⍰˛A$˛M€X˝ĄTźŞA(±ZĹĄla®_éźP%‰¬cŕĄFN¬@⍰±`ę˘A#˛Mk®GE°^ŮĄdéŁZË˘W˛§Oz°KqU¶¤Y—¬Ic©A0¨C8IV«B⍰ŻEAł_ĺžHi¨D⍰·UŞ«R˘¦[ÂĄPt«
NŽ©G]ŽQ%‰©]Ĕ¦[®ŞL,«[Ň˘FX¬GF«S‘«A °Z×źYąĄD9ł.—ĘĹ
aIDATxśíťksâ¸⍰†Ť%ts@D⍰É⍰CH⍰0¬ B⍰⍰›L2¨gĂĹ⍰p.çĂYf-=U“⍰Ŕ®2ou·Z–đ<‡Ăáp8⍰⍰‡Ăáp8⍰⍰‡Ăáp8⍰⍰‡Ăáp8⍰⍰‡Ăáp8l⍰cJ…⍰J)ý—
RŚĎý@⍰,XĂa⍰Po_⍰ď‡×íú ⍰ĆÂ©u,6(⍰Ţ´;śI?â<ŕ<ň%ăťöM(śý⍰Đ⍰us⍰0⍰ÂZ⍰⍰}⍰\Ý8ëÚC´ŮĂomČ8¨Ő@⍰‹3Ř~‹µá‘s?ęŮÁD…mîĂÚÇ@ź·CEl7.L°¸Ť$üL*ă‹2ş⍰Řrµ⍰uĺçBíĺ’Ý•°Ű
g·Ű8ő
tÜşťűqĎ⍰öFěŘ¨ „<⍰⍰⍰Oü⍰˛‘g⍰ŇŢ‹Ľ+ĘÁ}ĆÇťËŃegĔ™Ď‹rÝÉ—⍰=÷Cź Ôžăµś⍰ÚËřUł⍰"a@a«yĹ
⍰kü®ŹÎýŘç€öaÁn8›
0B©›a⍰!<⍰^°;Ř·Ď¸⍰}ű⍰⍰¬€⍰śv⍰Šz4⍰‘°~EŐ˘3…ć,˝e⍰żß¬KJ1ú‘ł*⍰Á¬Ü`čl ?ÍÝÖ⍰dW€'Xý•KŐ!⍰†Č+M51ńP8ĔŤ–Đ`Ka›‹Şf’ŮH^ăĎl⍰ÇŻ…«›ĘŞ⍰b‡⍰¤˝*YÇź¦äDĂë$őX Řę_{Î?
ÔIG7pÇ˜Š/o⍰?Ů]¡ZĽcQâ⍰Ď3ź⍰Éü⍰ó<"Š·Ä`ÂSţ⍰„ąůKtľuŹşŽ¸ř⍰C[˘»x’Y⍰:¦ßK⍰0⍰gY©|úÚm+⍰ĆY ’…N—°ŽŢĄĂ1Ń⍰!ux%L,ŠŃ"óBČ,©ÁŁW?ýŇŃ˘©ł⍰´h  d´⍰⍰⍰2?Ľ|®·b“$ĔîS/⍰ţ«⍰á⍰ă1Ló⍰ą-
```

Kali Linux is used for penetration testing (legally) but can be used for hacking as well. Finding traces of the usage of this type of OS does not prove anything illegal on its own but with other evidence it is a sign of suspicious activity. - *8 U.S. Code § 371; U.S. Code § 2512 (1) (b)*

Evidence #5



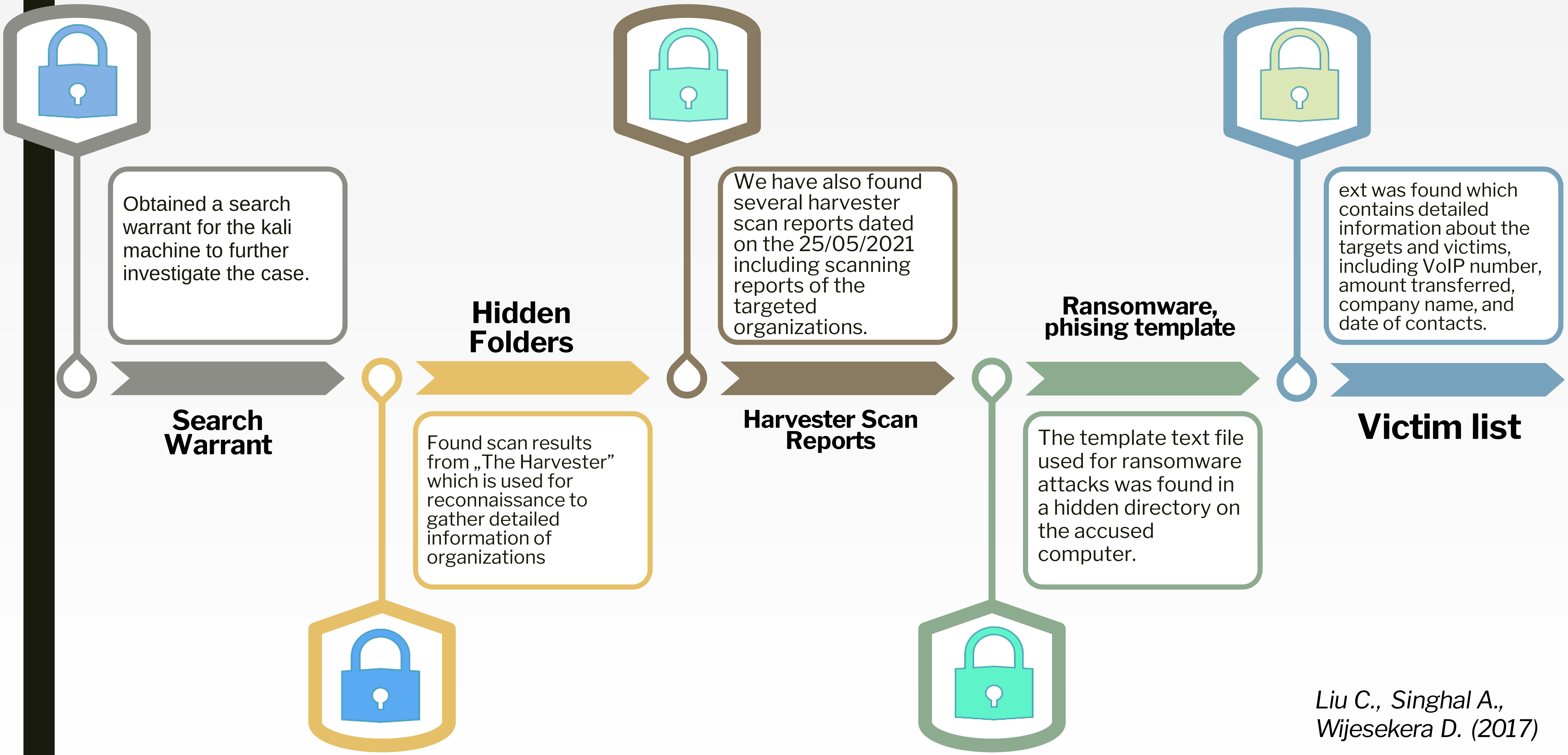
```
# Use wave package (native to Python) for reading the received audio file
import wave

song1 = wave.open("good_funk.wav", mode='rb')
song2 = wave.open("guitar_licks.wav", mode='rb')

# Convert audio to byte array
for song in [song1, song2]:
    frame_bytes = bytearray(list(song.readframes(song.getnframes())))
    # Extract the LSB of each byte
    extracted = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
    # Convert byte array back to string
    string = "".join(chr(int("".join(map(str,extracted[i:i+8])),2)) for i in range(0,len(extracted),8))
    # Cut off at the filler characters
    decoded = string.split("###")[0]
    # Print the extracted text
    print("Sucessfully decoded: "+decoded)

song1.close()
song2.close()
~
~
~
```



```
┌──(root㉿kali)-[/home/kali/Documents/WhiteHat]
└─# python3 solve2.py
Sucessfully decoded: The Darknet Site has been updated with latest cocaine quantities. WH{funkyLSB}
┌──(root㉿kali)-[/home/kali/Documents/WhiteHat]
└─# python3 solve2.py
Sucessfully decoded: Hide the transaction from Lee in the db! We dont need it attracting any attention. WH{guitarLSB}
```

Using encrypted messages is definitely evidence of conspiracy. - *8 U.S. Code § 371; 21 U.S. Code § 841 (a) (1) (2) (b) (A) (i) (ii) (II); U.S. Code § 922 (1) (A)*

Second Computer



Search Warrant

Obtained a search warrant for the kali machine to further investigate the case.

Hidden Folders

Found scan results from „The Harvester” which is used for reconnaissance to gather detailed information of organizations

Harvester Scan Reports

We have also found several harvester scan reports dated on the 25/05/2021 including scanning reports of the targeted organizations.

Ransomware, phising template

The template text file used for ransomware attacks was found in a hidden directory on the accused computer.

Victim list

ext was found which contains detailed information about the targets and victims, including VoIP number, amount transferred, company name, and date of contacts.

Liu C., Singhal A., Wijesekera D. (2017)

Evidence #6 and #7

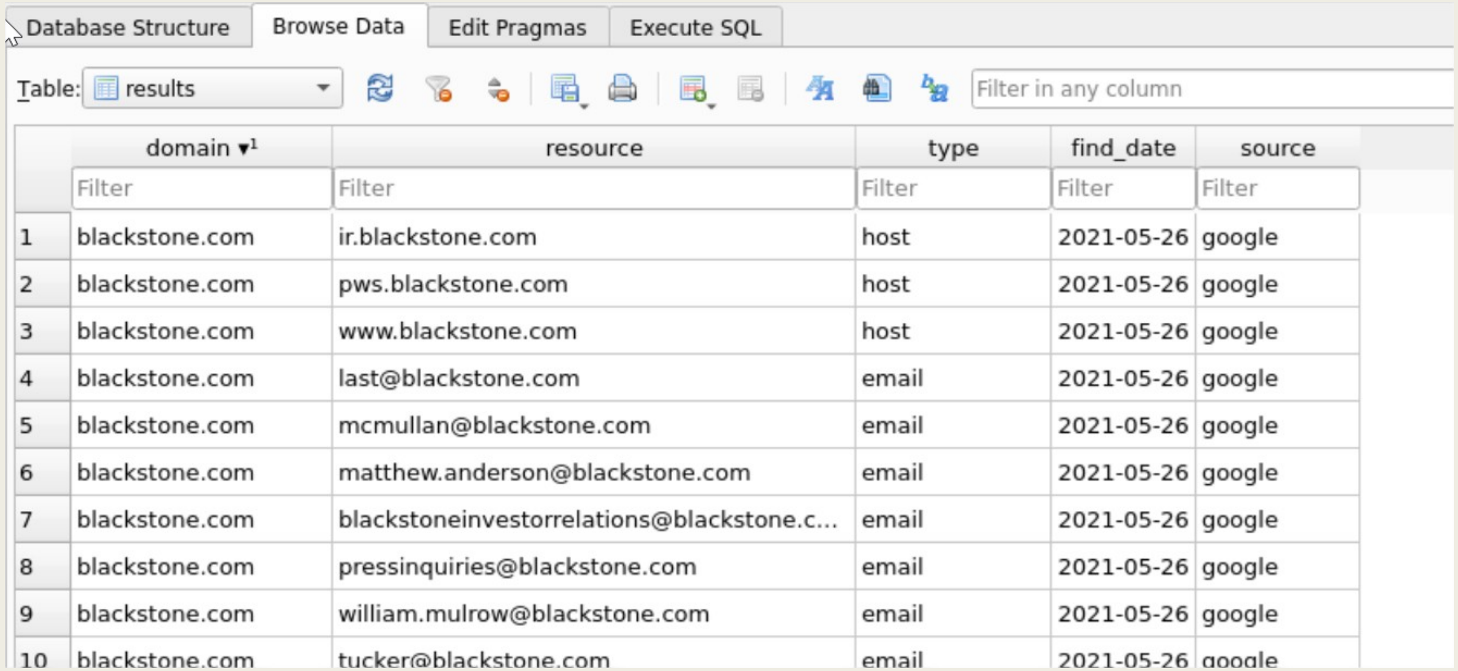
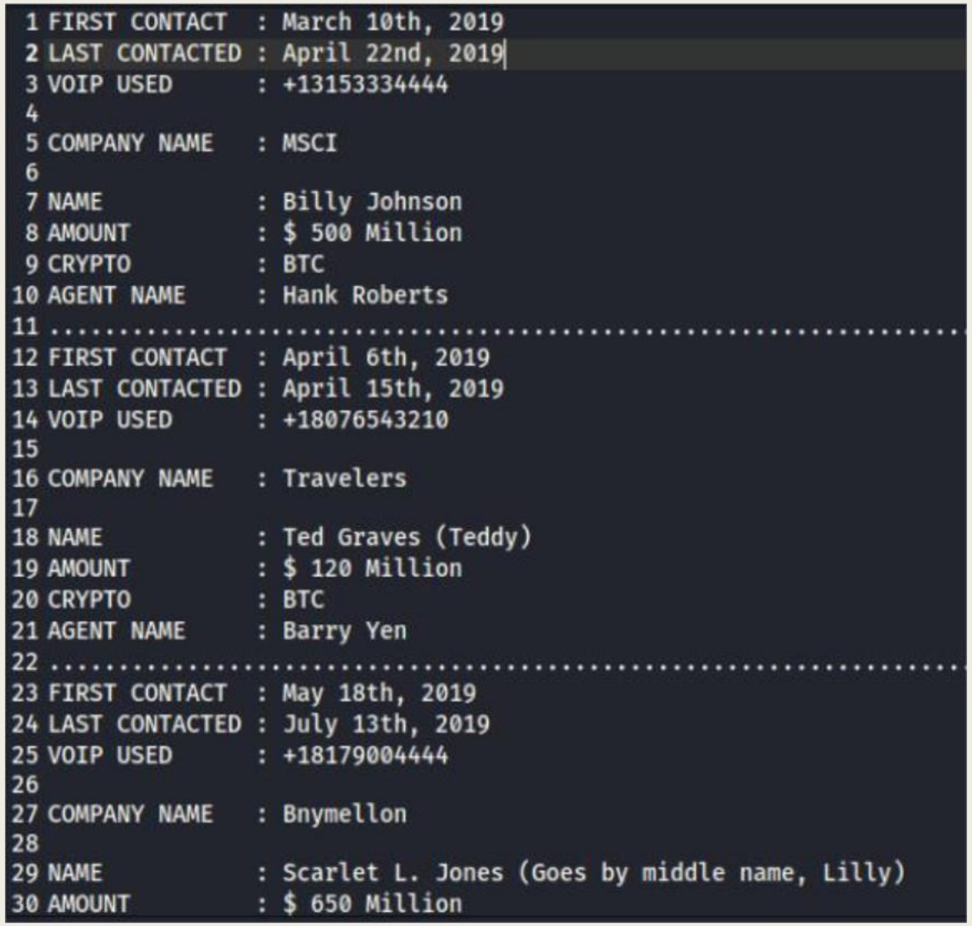


Table: results

	domain ▾1	resource	type	find_date	source
	Filter	Filter	Filter	Filter	Filter
1	blackstone.com	ir.blackstone.com	host	2021-05-26	google
2	blackstone.com	pws.blackstone.com	host	2021-05-26	google
3	blackstone.com	www.blackstone.com	host	2021-05-26	google
4	blackstone.com	last@blackstone.com	email	2021-05-26	google
5	blackstone.com	mcmullan@blackstone.com	email	2021-05-26	google
6	blackstone.com	matthew.anderson@blackstone.com	email	2021-05-26	google
7	blackstone.com	blackstoneinvestorrelations@blackstone.c...	email	2021-05-26	google
8	blackstone.com	pressinquiries@blackstone.com	email	2021-05-26	google
9	blackstone.com	william.mulrow@blackstone.com	email	2021-05-26	google
10	blackstone.com	tucker@blackstone.com	email	2021-05-26	google

The evidence shows that the perpetrator collected sensitive information about his targets including healthcare insurance companies and shows the intention of the perpetrator to explore his targets. - *18 U.S. Code § 669 (a); 18 U.S. Code § 1030 (a) (2) (A); U.S. Code § 2512 (1) (b) U.S. Code § 2512 (1) (b); U.S. Code § 1343*

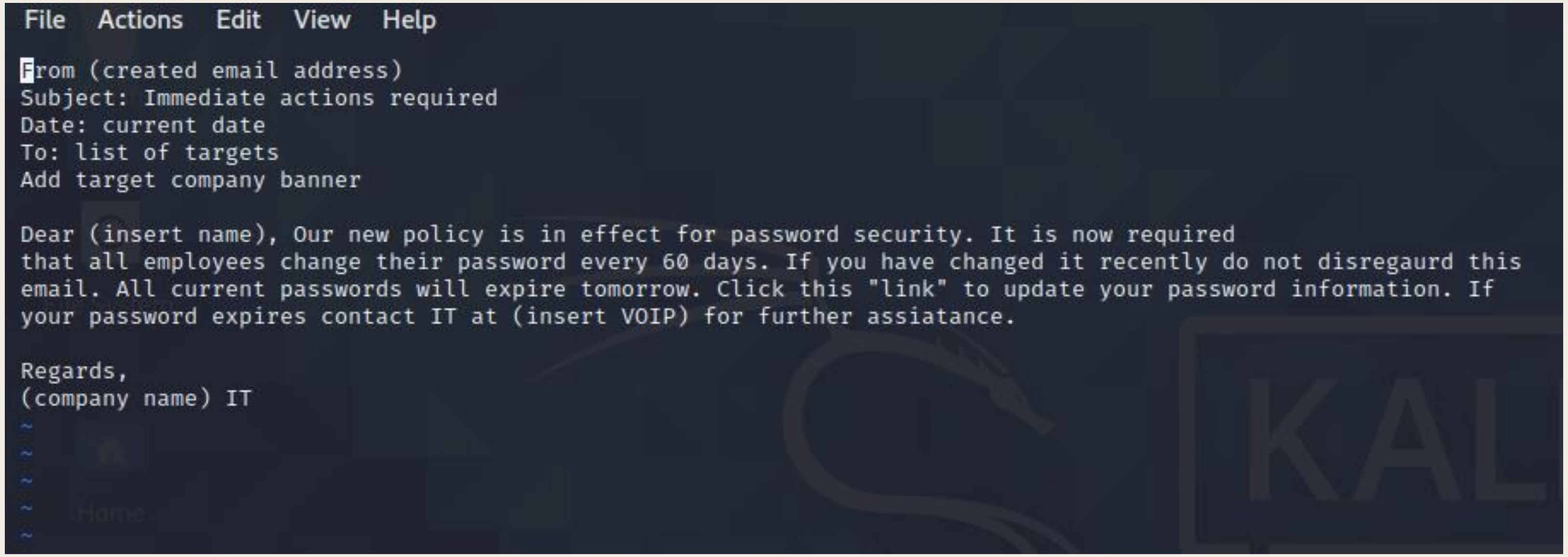
Evidence #8 and #9



```
FIRST CONTACT  : March 10th, 2019
LAST CONTACTED : April 22nd, 2019
VOIP USED      : +13153334444

COMPANY NAME   : MSCI

NAME           : Billy Johnson
AMOUNT         : $ 500 Million
CRYPTO         : BTC
AGENT NAME     : Hank Roberts
..................................................................
FIRST CONTACT  : April 6th, 2019
LAST CONTACTED : April 15th, 2019
VOIP USED      : +18076543210

COMPANY NAME   : Travelers

NAME           : Ted Graves (Teddy)
AMOUNT         : $ 120 Million
CRYPTO         : BTC
AGENT NAME     : Barry Yen
..................................................................
FIRST CONTACT  : May 18th, 2019
LAST CONTACTED : July 13th, 2019
VOIP USED      : +18179004444

COMPANY NAME   : Bnymellon

NAME           : Scarlet L. Jones (Goes by middle name, Lilly)
AMOUNT         : $ 650 Million
```

This is directly evidence of a committed crime. - *18 U.S. Code § 875 (d); 18 U.S. Code § 876 (d)*

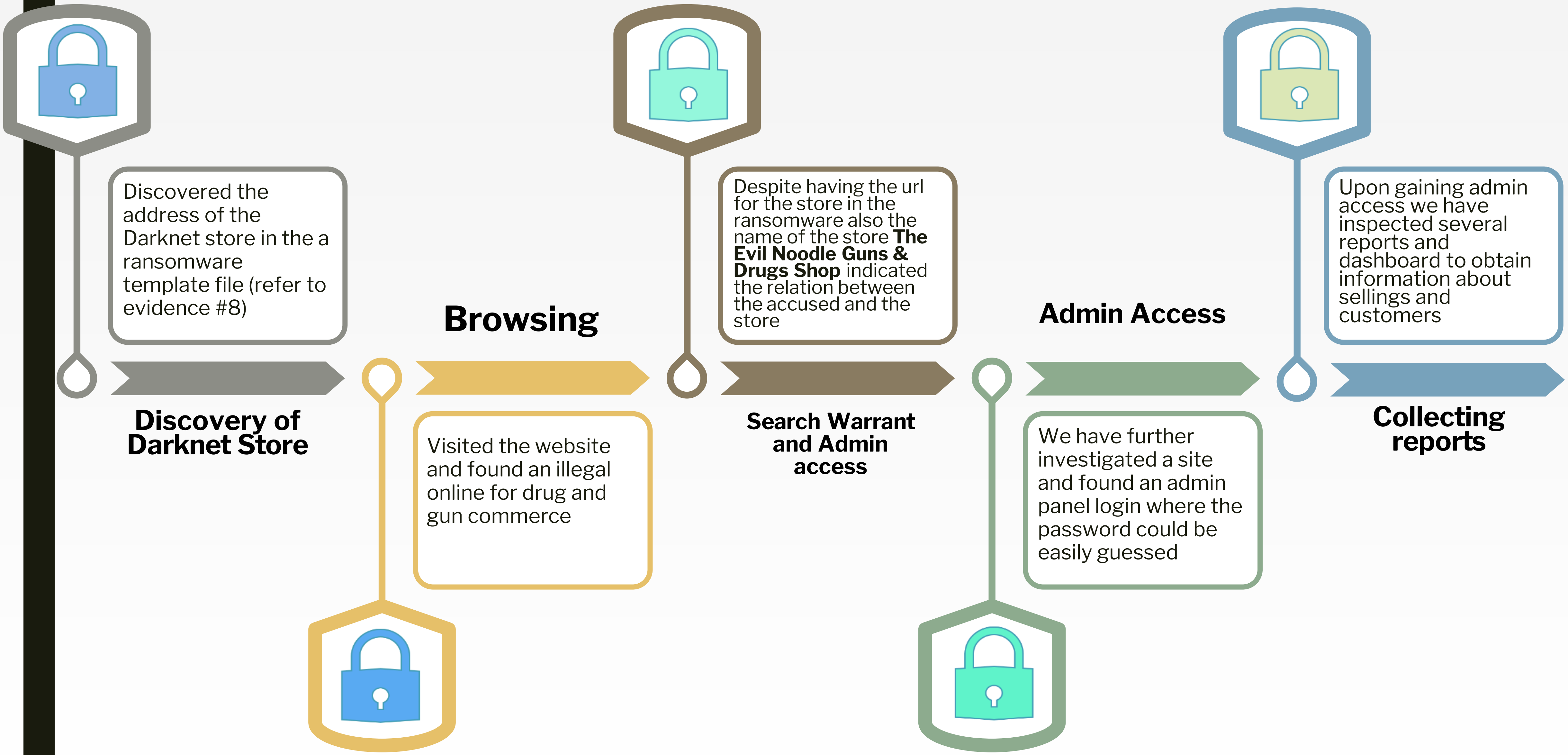
Evidence #10



```
From (created email address)
Subject: Immediate actions required
Date: current date
To: list of targets
Add target company banner

Dear (insert name), Our new policy is in effect for password security. It is now required
that all employees change their password every 60 days. If you have changed it recently do not disregaurd this
email. All current passwords will expire tomorrow. Click this "link" to update your password information. If
your password expires contact IT at (insert VOIP) for further assiatance.

Regards,
(company name) IT
~
~
~
~
~
```

Phishing is an activity of the perpetrator to gain more and more sensitive information about the future targets. The collected information is often used to commit cyber-attacks or are sold on certain DarkWeb marketplaces. - *U.S. Code § 1343; U.S. Code § 1344 (2)*

Darknet Store



Discovery of Darknet Store

Discovered the address of the Darknet store in the a ransomware template file (refer to evidence #8)

Browsing

Visited the website and found an illegal online for drug and gun commerce

Search Warrant and Admin access

Despite having the url for the store in the ransomware also the name of the store **The Evil Noodle Guns & Drugs Shop** indicated the relation between the accused and the store

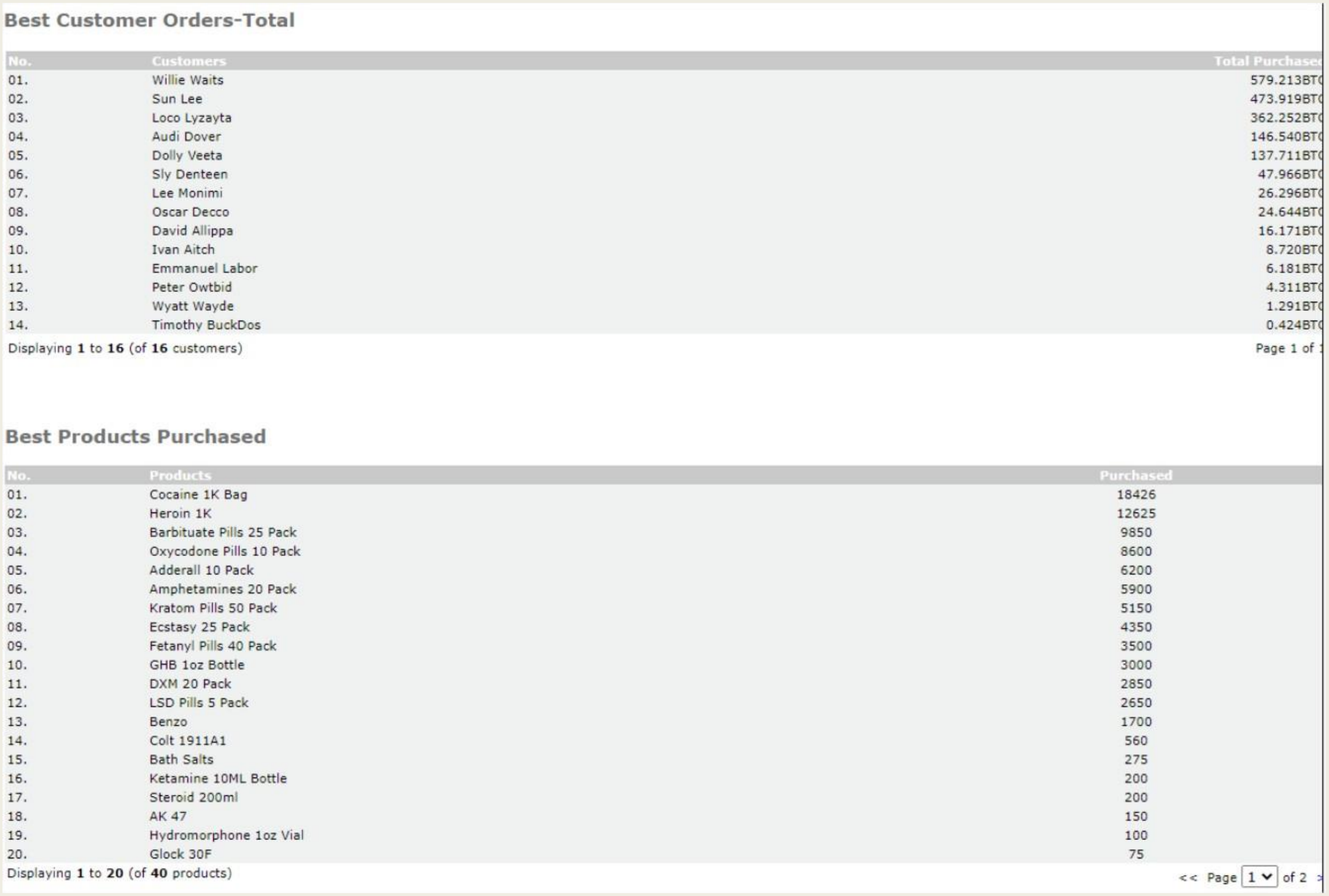
Admin Access

We have further investigated a site and found an admin panel login where the password could be easily guessed

Collecting reports

Upon gaining admin access we have inspected several reports and dashboard to obtain information about sellings and customers

Evidence #11



Best Customer Orders-Total

No.	Customers	Total Purchased
01.	Willie Waits	579.213BTC
02.	Sun Lee	473.919BTC
03.	Loco Lyzayta	362.252BTC
04.	Audi Dover	146.540BTC
05.	Dolly Veeta	137.711BTC
06.	Sly Denteen	47.966BTC
07.	Lee Monimi	26.296BTC
08.	Oscar Decco	24.644BTC
09.	David Allippa	16.171BTC
10.	Ivan Aitch	8.720BTC
11.	Emmanuel Labor	6.181BTC
12.	Peter Owtbid	4.311BTC
13.	Wyatt Wayde	1.291BTC
14.	Timothy BuckDos	0.424BTC

Displaying **1** to **16** (of **16** customers) Page 1 of 1

Best Products Purchased

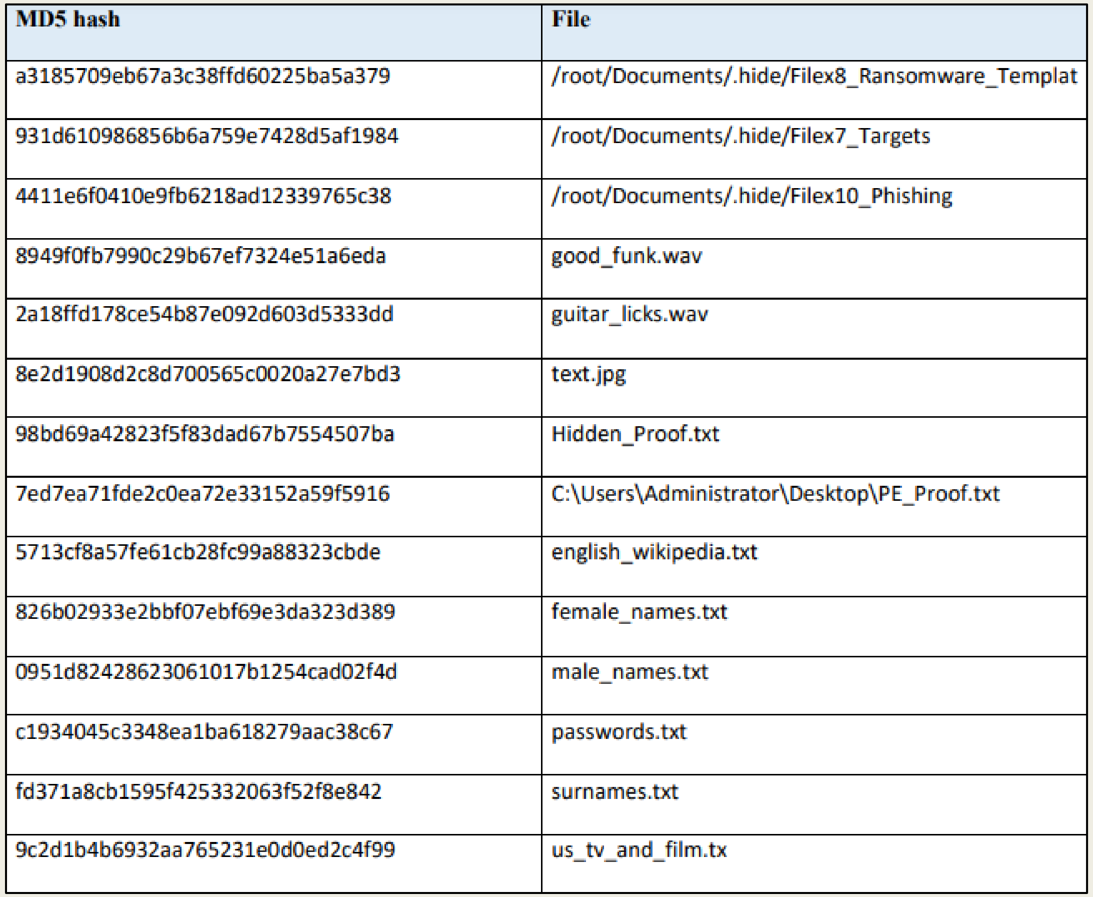
No.	Products	Purchased
01.	Cocaine 1K Bag	18426
02.	Heroin 1K	12625
03.	Barbituate Pills 25 Pack	9850
04.	Oxycodone Pills 10 Pack	8600
05.	Adderall 10 Pack	6200
06.	Amphetamines 20 Pack	5900
07.	Kratom Pills 50 Pack	5150
08.	Ecstasy 25 Pack	4350
09.	Fetanyl Pills 40 Pack	3500
10.	GHB 1oz Bottle	3000
11.	DXM 20 Pack	2850
12.	LSD Pills 5 Pack	2650
13.	Benzo	1700
14.	Colt 1911A1	560
15.	Bath Salts	275
16.	Ketamine 10ML Bottle	200
17.	Steroid 200ml	200
18.	AK 47	150
19.	Hydromorphone 1oz Vial	100
20.	Glock 30F	75

Displaying **1** to **20** (of **40** products)

The evidence directly proves two different illegal activities achieved by the perpetrator. - *21 U.S. Code § 841 (a) (1) (2) (b) (A) (i) (ii) (II); U.S. Code § 922 (1) (A*

Hashes

Since we have only worked with forensics copies of the files
we have provided the the hashes of the real files



MD5 hash	File
a3185709eb67a3c38ffd60225ba5a379	/root/Documents/.hide/Filex8_Ransomware_Templat
931d610986856b6a759e7428d5af1984	/root/Documents/.hide/Filex7_Targets
4411e6f0410e9fb6218ad12339765c38	/root/Documents/.hide/Filex10_Phishing
8949f0fb7990c29b67ef7324e51a6eda	good_funk.wav
2a18ffd178ce54b87e092d603d5333dd	guitar_licks.wav
8e2d1908d2c8d700565c0020a27e7bd3	text.jpg
98bd69a42823f5f83dad67b7554507ba	Hidden_Proof.txt
7ed7ea71fde2c0ea72e33152a59f5916	C:\Users\Administrator\Desktop\PE_Proof.txt
5713cf8a57fe61cb28fc99a88323cbde	english_wikipedia.txt
826b02933e2bbf07ebf69e3da323d389	female_names.txt
0951d82428623061017b1254cad02f4d	male_names.txt
c1934045c3348ea1ba618279aac38c67	passwords.txt
fd371a8cb1595f425332063f52f8e842	surnames.txt
9c2d1b4b6932aa765231e0d0ed2c4f99	us_tv_and_film.tx

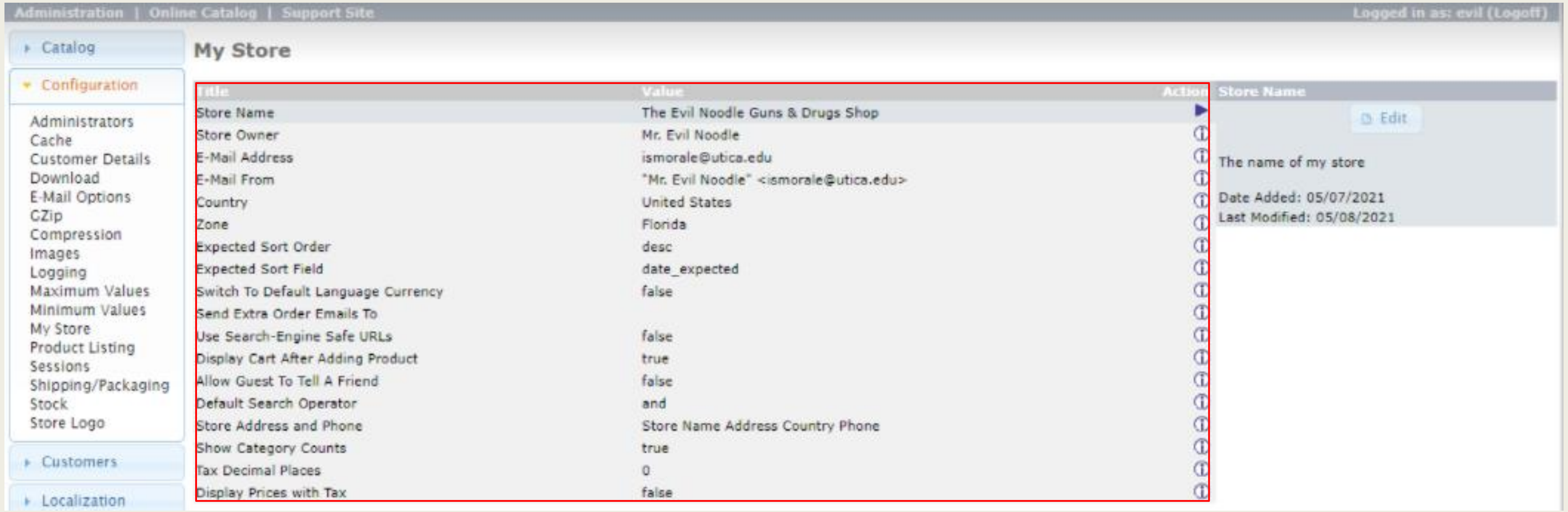
Nelson, B., Phillips, A., & Steuart, C. (2019)

Summary

We have found

- direct evidences of commited crimes
- indirect evidences that raise suspicion
- various type of signs that shows conspirative activity

According to our forensic review we determine that sufficient evidence exists to support the pursuit of charges against Mr. Evil Noodle for all of the above-mentioned crimes. And Mr. Ismail Morales will have some explaining to do :)



My Store

Title	Value	Action
Store Name	The Evil Noodle Guns & Drugs Shop	▶
Store Owner	Mr. Evil Noodle	ⓘ
E-Mail Address	ismorale@utica.edu	ⓘ
E-Mail From	"Mr. Evil Noodle" <ismorale@utica.edu>	ⓘ
Country	United States	ⓘ
Zone	Florida	ⓘ
Expected Sort Order	desc	ⓘ
Expected Sort Field	date_expected	ⓘ
Switch To Default Language Currency	false	ⓘ
Send Extra Order Emails To		ⓘ
Use Search-Engine Safe URLs	false	ⓘ
Display Cart After Adding Product	true	ⓘ
Allow Guest To Tell A Friend	false	ⓘ
Default Search Operator	and	ⓘ
Store Address and Phone	Store Name Address Country Phone	ⓘ
Show Category Counts	true	ⓘ
Tax Decimal Places	0	ⓘ
Display Prices with Tax	false	ⓘ

Store Name

The name of my store

Date Added: 05/07/2021
Last Modified: 05/08/2021

References

- **Liu C., Singhal A., Wijesekera D. (2017)** Identifying Evidence for Cloud Forensic Analysis. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, vol 511. Springer, Cham. https://doi.org/10.1007/978-3-319-67208-3_7
- **Nelson, B., Phillips, A., & Steuart, C. (2019)** Guide to Computer Forensics and Investigations, 6th Edition, Boston, MA: Cengage Learning Inc.
- **AlwaysInstallElevated Windows Priv Esc**: https://pentestlab.blog/2017/02/28/always-install-elevated/
- **LSB Audio manipulation:** Audio Steganography : The art of hiding secrets within earshot (part 2 of 2) | by Sumit Kumar Arora | Medium
- **CyberChef:** https://gchq.github.io/CyberChef/#recipe=Change_IP_format('Decimal','Dotted%20Decimal')&input =MjEzMD cwNjY4OQ Autopsy: https://www.autopsy.com/download/