



## Digital Forensics Report

Author	Number
João Cruz	90731
Rafael Figueiredo	90770
Ricardo Grade	90774

### 1 Can you suggest why the authorities have considered Rick to be a potential suspect of uploading the files to PharmaLeaks?

The Authorities could have considered Rick Chick as a Potential Suspect by analyzing the Annotated Email leaked and investigated its Comments and Highlights realizing that Rick Chick was its mentioned Author. [Figure: 1]

Another Path that the Authorities could have followed is checking if the Registered PharmaLeaks Account where the leaked files have been posted had any leads pointing to Rick Chick. The way that we found out that Rick Chick was Logged in will be explained later in this Report.

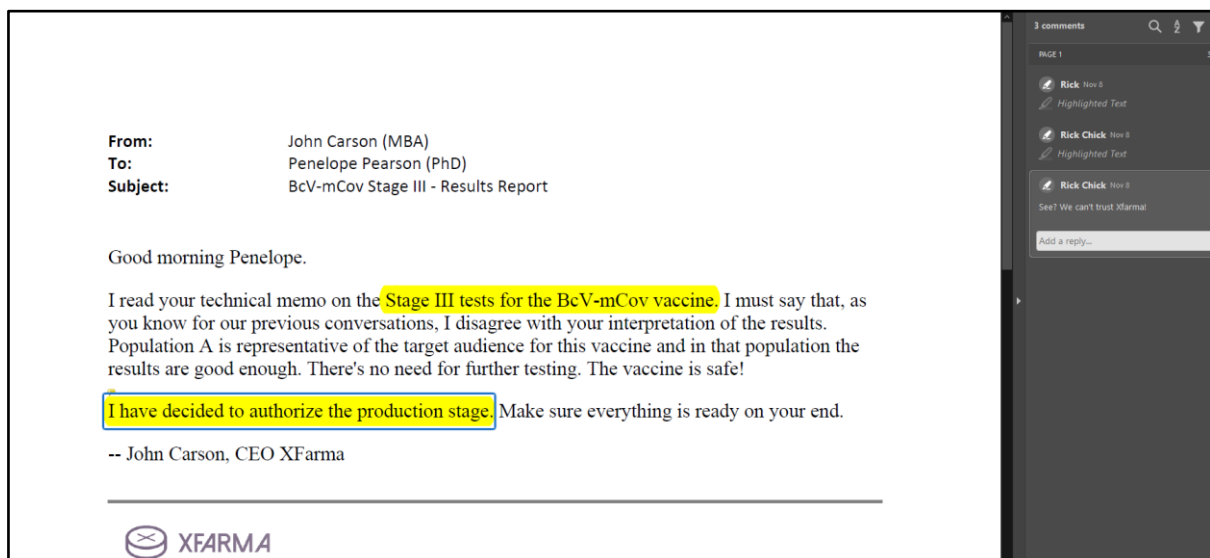


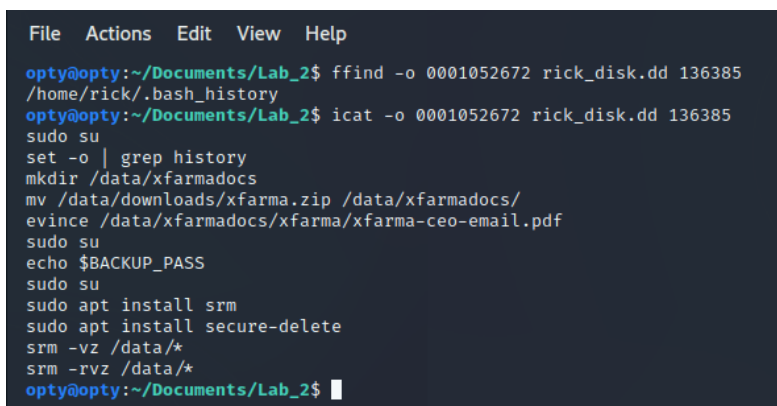
Figure 1: Annotated Email PDF

## 2 Do you find any traces of the PharmaLeaks files on Rick's computers?

Yes, we found the leaked files in the hard disk image of Rick's backup server.

The Steps we performed to find out the leaked files were:

1. We began by analyzing the `.bash_history` file in the `/home/rick` directory in the hard disk image of Rick's workstation. By analyzing it we were able to find out that the possible leaked files were downloaded as `xfarma.zip` and moved to the `/data/xfarmadocs` directory which was then securely deleted. Besides this we also find out that the `xfarma-ceo-email.pdf` was opened with evince (Document Viewer). We were also able to realize that an environment variable called `BACKUP_PASS` exists. [Figure: 2]
2. As we found out that the possible leaked files were deleted using the `srm` command, we went into the hard disk image of Rick's backup server and realized that on `/home/rick` there were a few backups. We extract those backups and find out that they were protected by a Password. We had a previously knowledge of the existence of a `BACKUP_PASS` in the hard disk image of Rick's workstation. [Figure: 3]
3. We began by checking all possible files where that environment variable could be. We found out that its definition was on `/etc/profile` and its value was the output of a python program obfuscator present on the `/home/rick/assets` directory. [Figure: 4]
4. We extracted obfuscator and executed it to find out the value of `BACKUP_PASS` which is `r1cK_7ru7h2020_CH1cK`. [Figure: 5]
5. Once we found out the value of `BACKUP_PASS`, we unzipped all the existing backups using that Password and found out that in the three most recent ones was the `xfarmadocs` directory with the leaked files, once that it hashes matches the ones leaked to PharmaLeaks. [Figure: 6]

A terminal window with a dark background and light blue text. The window title bar shows 'File Actions Edit View Help'. The terminal content shows a series of commands and their outputs. The user 'opty' is in the directory '~/Documents/Lab\_2'. They run 'ffind -o 0001052672 rick\_disk.dd 136385 /home/rick/.bash\_history'. Then they run 'icat -o 0001052672 rick\_disk.dd 136385' and press enter. They run 'sudo su' and press enter. They run 'set -o | grep history' and press enter. They run 'mkdir /data/xfarmadocs' and press enter. They run 'mv /data/downloads/xfarma.zip /data/xfarmadocs/' and press enter. They run 'evince /data/xfarmadocs/xfarma/xfarma-ceo-email.pdf' and press enter. They run 'sudo su' and press enter. They run 'echo \$BACKUP\_PASS' and press enter. They run 'sudo su' and press enter. They run 'sudo apt install srm' and press enter. They run 'sudo apt install secure-delete' and press enter. They run 'srm -vz /data/\*' and press enter. They run 'srm -rvz /data/\*' and press enter. The prompt returns to 'opty@opty:~/Documents/Lab\_2\$' with a cursor.

```
File Actions Edit View Help
opty@opty:~/Documents/Lab_2$ ffind -o 0001052672 rick_disk.dd 136385
/home/rick/.bash_history
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 136385
sudo su
set -o | grep history
mkdir /data/xfarmadocs
mv /data/downloads/xfarma.zip /data/xfarmadocs/
evince /data/xfarmadocs/xfarma/xfarma-ceo-email.pdf
sudo su
echo $BACKUP_PASS
sudo su
sudo apt install srm
sudo apt install secure-delete
srm -vz /data/*
srm -rvz /data/*
opty@opty:~/Documents/Lab_2$ █
```

Figure 2: Bash History

```

File  Actions  Edit  View  Help

root@root:~/Desktop/Proj_Lab2# find -o 0000002048 backup_disk.dd 606
/home/rick
root@root:~/Desktop/Proj_Lab2# find -o 0000002048 backup_disk.dd 606
r/r 34224:      .bash_logout
r/r 34400:      .bashrc
r/r 36017:      .profile
d/d 36031:      .cache
r/r 36034:      .sudo_as_admin_successful
d/d 9168:      .ssh
r/r 10533:      .bash_history
r/r * 36025(realloc): .backup_1604831402.zip.To7LJ3
r/r 27007:      backup_1604761201.zip
r/r 27008:      backup_1604763001.zip
r/r 11760:      backup_1604827801.zip
r/r 35731:      backup_1604829601.zip
r/r 36025:      backup_1604831402.zip
root@root:~/Desktop/Proj_Lab2# icat -o 0000002048 backup_disk.dd 36025 > backup_1604831402.zip
root@root:~/Desktop/Proj_Lab2# unzip -q backup_1604831402.zip
[backup_1604831402.zip] data/xfarmadocs/xfarma/xfarma-ceo-email.pdf password: █

```

Figure 3: Protected Backups

```

File  Actions  Edit  View  Help

opty@opty:~/Documents/Lab_2$ find -o 0001052672 rick_disk.dd 393442
/etc/profile
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 393442
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "${PS1}" ]; then
  if [ "${BASH}" ] && [ "$BASH" ≠ "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='h:w$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
    fi
  else
    if [ "`id -u`" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
    fi
  fi
fi

if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
unset i
fi

export BACKUP_PASS=$(python3 /home/rick/assets/obfuscator)

opty@opty:~/Documents/Lab_2$ █

```

Figure 4: BACKUP\_PASS Definition

```

File  Actions  Edit  View  Help

opty@opty:~/Documents/Lab_2$ find -o 0001052672 rick_disk.dd 136395
/home/rick/assets/obfuscator
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 136395 > obfuscator
opty@opty:~/Documents/Lab_2$ python3 obfuscator
rick_7ru7h2020_CH1cK
opty@opty:~/Documents/Lab_2$ █

```

Figure 5: BACKUP\_PASS Value

```

File Actions Edit View Help
opty@opty:~/Documents/Lab_2$ find -o 0000002048 backup_disk.dd 606
/home/rick
opty@opty:~/Documents/Lab_2$ fls -o 0000002048 backup_disk.dd 606
r/r 34224: .bash_logout
r/r 34400: .bashrc
r/r 36017: .profile
d/d 36031: .cache
r/r 36034: .sudo_as_admin_successful
d/d 9168: .ssh
r/r 10533: .bash_history
r/r * 36025(realloc): .backup_1604831402.zip.To7LJ3
r/r 27007: backup_1604761201.zip
r/r 27008: backup_1604763001.zip
r/r 11760: backup_1604827801.zip
r/r 35731: backup_1604829601.zip
r/r 36025: backup_1604831402.zip
opty@opty:~/Documents/Lab_2$ icat -o 0000002048 backup_disk.dd 36025 > backup_1604831402.zip
opty@opty:~/Documents/Lab_2$ unzip -q -P r1cK_7ru7h2020_CH1cK backup_1604831402.zip
opty@opty:~/Documents/Lab_2$ cd data/
opty@opty:~/Documents/Lab_2/data$ ls
downloads firefox_cache xfarmadocs
opty@opty:~/Documents/Lab_2/data$ cd xfarmadocs/
opty@opty:~/Documents/Lab_2/data/xfarmadocs$ ls
xfarma xfarma.zip
opty@opty:~/Documents/Lab_2/data/xfarmadocs$ cd xfarma/
opty@opty:~/Documents/Lab_2/data/xfarmadocs/xfarma$ ls
BcV-mCov_internal_report.pdf xfarma-ceo-email_annotated.pdf xfarma-ceo-email.pdf
opty@opty:~/Documents/Lab_2/data/xfarmadocs/xfarma$ md5sum BcV-mCov_internal_report.pdf
8e5a62390ef3e86a40f91be4a7eff550 BcV-mCov_internal_report.pdf
opty@opty:~/Documents/Lab_2/data/xfarmadocs/xfarma$ md5sum xfarma-ceo-email.pdf
87eca7a4b6ec8c47d2351172ab825a24 xfarma-ceo-email.pdf
opty@opty:~/Documents/Lab_2/data/xfarmadocs/xfarma$ md5sum xfarma-ceo-email_annotated.pdf
dc1abdb8679d3ca10a7f40b5b6436a35 xfarma-ceo-email_annotated.pdf
opty@opty:~/Documents/Lab_2/data/xfarmadocs/xfarma$

```

Figure 6: Leaked files

### 3 Can you find any evidence that PharmaLeaks file have indeed been uploaded from Rick’s computers, and what the source of these files may have been? Establish a timeline of relevant events.

We will present our hypothesis of how the events happened in the following timeline:

Timeline Events Hypothesis		
Event	Time	Description
1	Nov 7 14:32	Rick Logs into his PC [Figure: 7]
2	Nov 7 15:00	Creation of the Backup ZIP <i>backup_1604761201.zip</i> [Annex File: backup_1604761201.zip]
3	Nov 7 15:05	<p><b>From:</b> Rick Chick</p> <p><b>To:</b> N16H70WL</p> <p><b>Subject:</b> Job</p> <p><b>Message:</b></p> <p><i>We have a common friend. He told me you are the one I need for a job.</i></p> <p><i>Can we meet?</i></p> <p>-- R</p> <p>[Annex File: Sent]</p>

4	Nov 7 15:11	<b>From:</b> N16H70WL <b>To:</b> Rick Chick <b>Subject:</b> Re: Job <b>Message:</b> 38.737310, -9.130273 today 1715 [Annex File: Inbox]
		<b>Meeting Details:</b> <ul style="list-style-type: none"> <li>Coordinates: Fonte Luminosa in Alameda</li> <li>Time: Nov 7 17:15</li> </ul>
5	Nov 7 15:30	Creation of the Backup ZIP <i>backup_1604763001.zip</i> [Annex File: backup_1604763001.zip]
6	Nov 7 15:33	Rick Logs out of his PC [Figure: 7]
7	Nov 7 17:15	Supposedly Rick meets N16H70WL [According to Event: 4]
8	Nov 8 09:01	Rick Logs into his PC [Figure: 7]
9	Nov 8 09:15	<b>From:</b> N16H70WL <b>To:</b> Rick Chick <b>Subject:</b> Done <b>Message:</b> V2hhdCB5b3UgYXNrZWQgZm9yOiBodHRwczovL3d3dy5kcm9wYm94LmNvbS9zL25mN2M0azd1aWsxMW5iNC94ZmFybWEuemlwP2RsPTA= [Annex File: Inbox]
		<b>Message Decoded from Base64:</b> What you asked for: <a href="https://www.dropbox.com/s/nf7c4k7uik11nb4/xfarma.zip?dl=0">https://www.dropbox.com/s/nf7c4k7uik11nb4/xfarma.zip?dl=0</a>
10	Nov 8 09:20	Rick Visits the leaked files Dropbox [Figure: 11]
11	Nov 8 09:20	Rick Downloads the leaked files ZIP <i>xfarma.zip</i> [Figure: 10]
12	Nov 8 09:21	Rick Extracts the Email PDF <i>xfarma-ceo-email.pdf</i> [Annex: recently-used.xbel]
13	Nov 8 09:25	Rick Opens the Email PDF <i>xfarma-ceo-email.pdf</i> Using Document Viewer [Annex: recently-used.xbel]
14	Nov 8 09:26	Rick Creates an Annotated Email PDF <i>xfarma-ceo-email_annotated.pdf</i> [Annex: recently-used.xbel]
15	Nov 8 09:26	Rick Opens the Annotated Email PDF <i>xfarma-ceo-email_annotated.pdf</i> Using Document Viewer [Annex: recently-used.xbel]
16	Nov 8 09:30	Creation of the Backup ZIP <i>backup_1604827801.zip</i> [Annex File: backup_1604827801.zip]
17	Nov 8 09:40	Rick Registers himself on the PharmaLeaks Website [Figure: 11]

18	Nov 8 09:41	Rick Logins himself on the Pharma Leaks Website [Figure: 11]
19	Nov 8 09:42	Rick Gets in the Pharma Leaks Website [Figure: 11]
20	Nov 8 09:42	Rick Opens a New Page on the Pharma Leaks Website [Figure: 11]
21	Nov 8 09:43	The Report PDF <i>BcV-mCov_internal_report.pdf</i> and Annotated Email <i>xfarma-ceo-email_annotated.pdf</i> are Used by Firefox [Annex: recently-used.xbel]
22	Nov 8 09:44	Rick Does a Request on the Pharma Leaks Website with a Suspicious Description Suggesting that He is Leaking the Files [Figure: 11]  <b>Suspicious Description:</b> <i>What they don't wan't you to know!</i>
23	Nov 8 10:00	Creation of the Backup ZIP <i>backup_1604829601.zip</i> [Annex File: backup_1604829601.zip]
24	Nov 8 10:05	Rick Searches on Internet How to Permanently and Securely Delete Files [Figure: 11]
25	Nov 8 10:05	Rick Opens an Article that Explains How to Permanently and Securely Delete Files [Figure: 11]
		<b>Article Description:</b> <i>In this article, we will explain several command line tools for permanently and securely deleting files or memory in Linux.</i>
26	Nov 8 10:30	Creation of the Backup ZIP <i>backup_1604831402.zip</i> [Annex File: backup_1604831402.zip]
27	Nov 8 11:02	Rick Deletes the leaked files from his PC [Figure: 13]
28	Nov 8 11:02	Rick Logs out of his PC [Figure: 7]

#### Source of leaked files:

- The *BcV-mCov\_internal\_report.pdf* and *xfarma-ceo-email.pdf* has been downloaded from a Dropbox which Link was sent to Rick Chick from N16H70WL via Mail. [Events: 9, 10, 11]
- The *xfarma-ceo-email.pdf* was then highlighted and commented by Rick Chick in Document Viewer creating the *xfarma-ceo-email\_annotated.pdf*. [Events: 12, 13, 14, 15]

#### Evidence that Rick Chick has indeed uploaded the leaked files:

- Given that Rick Chick had in his possession the leaked files, and Rick's browser accesses it 1 minute before he does a Request to PharmaLeaks with a suspicious description suggesting that he is leaking the files, we strongly believe that Rick Chick has indeed Uploaded them to PharmaLeaks. [Events: 21, 22]

```

File Actions Edit View Help
opty@opty:~/Documents/Lab_2$ ffind -o 0001052672 rick_disk.dd 306149
/var/log/wtmp
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 306149 > wtmp 66 last -f wtmp
rick      :0      :0      Sun Nov  8 09:01 - down    (02:00)
reboot    system boot  5.4.0-52-generic Sun Nov  8 09:01 - 11:02 (02:01)
rick      :0      :0      Sat Nov  7 14:32 - down    (01:00)
reboot    system boot  5.4.0-52-generic Sat Nov  7 14:32 - 15:33 (01:00)
rick      :0      :0      Fri Nov  6 18:29 - down    (00:05)
reboot    system boot  5.4.0-52-generic Fri Nov  6 18:29 - 18:35 (00:06)
rick      :0      :0      Fri Nov  6 16:07 - crash   (02:21)
reboot    system boot  5.4.0-52-generic Fri Nov  6 16:06 - 18:35 (02:28)
rick      :0      :0      Fri Nov  6 15:57 - down    (00:09)
reboot    system boot  5.4.0-52-generic Fri Nov  6 15:56 - 16:06 (00:10)

wtmp begins Fri Nov  6 15:56:08 2020
opty@opty:~/Documents/Lab_2$ █

```

Figure 7: Login Logs

```

File Actions Edit View Help

opty@opty:~/Documents/Lab_2$ ffind -o 0001052672 rick_disk.dd 10698
/home/rick/.thunderbird/fskdv8po.default-release/Mail/outlook.office365.com
opty@opty:~/Documents/Lab_2$ fls -o 0001052672 rick_disk.dd 10698
r/r 10703:      Inbox
r/r 10707:      Inbox.msf
r/r 10709:      Trash
r/r 10710:      Trash.msf
r/r 10468:      popstate.dat
r/r 11149:      msgFilterRules.dat
r/r 11148:      filterlog.html
r/r 10635:      Drafts
r/r 10864:      Drafts.msf
r/r 10874:      Sent
r/r 10875:      Sent.msf
r/r * 10468(realloc):  popstate-1.dat
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 10874 > Sent
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 10703 > Inbox
opty@opty:~/Documents/Lab_2$ md5sum Sent
f734ddb6e63e1de47d4c072d00ec1793  Sent
opty@opty:~/Documents/Lab_2$ md5sum Inbox
ba4d14d3fd6e938e03adbaee1c224e18  Inbox
opty@opty:~/Documents/Lab_2$

```

Figure 8: Mail Logs

```

File Actions Edit View Help

opty@opty:~/Documents/Lab_2$ cd data/
opty@opty:~/Documents/Lab_2/data$ ls
downloads  firefox_cache  xfarmadocs
opty@opty:~/Documents/Lab_2/data$ cd firefox_cache/
opty@opty:~/Documents/Lab_2/data/firefox_cache$ ls
addons.json          content-prefs.sqlite      formhistory.sqlite      protections.sqlite      SiteSecurityServiceState.txt
addonStartup.json.lz4 cookies.sqlite            gmp-gmpopenh264        safebrowsing            startupCache
AlternateServices.txt cookies.sqlite-wal        handlers.json           saved-telemetry-pings   storage
bookmarkbackups      crashes                  key4.db                search.json.mozlz4      storage.sqlite
broadcast-listeners.json datareporting            minidumps              SecurityPreloadState.txt thumbnails
cache2               extension-preferences.json OfflineCache            sessionCheckpoints.json times.json
cert9.db             extensions.json          permissions.sqlite     sessionstore-backups    weave
ClientAuthRememberList.txt extensions.json          pkcs11.txt            settings                 webappsstore.sqlite
compatibility.ini     favicons.sqlite         places.sqlite          shield-preference-experiments.json webappsstore.sqlite-wal
containers.json       favicons.sqlite-wal     prefs.js               xulstore.json
opty@opty:~/Documents/Lab_2/data/firefox_cache$ md5sum places.sqlite
58690f087b47dcc17ff800d92177ce46  places.sqlite
opty@opty:~/Documents/Lab_2/data/firefox_cache$ sqlitebrowser places.sqlite

```

Figure 9: Places Table Found

DB Browser for SQLite - places.sqlite

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma's Execute SQL

Table: moz\_annos

	id	place_id	anno_attribute_	content	flags	expiration	type	dateAdded	lastModified
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	13	1	file:///data/downloads/xfarma.zip	0	4	3	1604827221887000	1604827221887000
2	2	13	2	{"state":1,"endTime":1604827221844,"fileSize":329389}	0	4	3	1604827221926000	1604827221926000

Figure 10: Downloads



DB Browser for SQLite - places.sqlite										
File Edit View Tools Help										
New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database										
Database Structure Browse Data Edit Pragma Execute SQL										
Table: moz_places										
	id	url	title	rev_host	last_visit_date	guid	url_hash	description	New Record~ Delete Record	
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
1	1	https://www.mozilla.org/privacy/firefox/	Firefox Privacy Notice — Mozilla	gro.allizom.www.	1604687655622714	C-6jxiACTQ2L	47356411089529	NULL	1	
2	2	https://www.mozilla.org/en-US/privacy/firefox/	Firefox Privacy Notice — Mozilla	gro.allizom.www.	1604687655789510	4kQOnsNAF3X	47358032558425	...	1	
3	3	https://support.mozilla.org/en-US/products/firefox	NULL	gro.allizom.troppus.	NULL	LmkwZyctwXVZ	47357795150914	NULL	2	
4	4	https://support.mozilla.org/en-US/kb/customize-firefox...	NULL	gro.allizom.troppus.	NULL	wpDoosaOTy4D	47359532431620	NULL	2	
5	5	https://www.mozilla.org/en-US/contribute/	NULL	gro.allizom.www.	NULL	WRUR4airB1c	47358034485371	NULL	1	
6	6	https://www.mozilla.org/en-US/about/	NULL	gro.allizom.www.	NULL	sKITB2OUIgh	47358774953055	NULL	1	
7	7	http://www.ubuntu.com/	NULL	moc.ubuntu.www.	NULL	XwC_2Hw9GjB	125508050257634	NULL	3	
8	8	http://wiki.ubuntu.com/	NULL	moc.ubuntu.kiw.	NULL	PQbhiQ_16-9	125511519733047	NULL	4	
9	9	https://answers.launchpad.net/ubuntu/+addquestion	NULL	ten.daphcnual.sre...	NULL	bwIXHbb7WNIF	47359338650210	NULL	5	
10	10	http://www.debian.org/	NULL	gro.naibed.www.	NULL	UXRyw7bbjs_c	125508165346216	NULL	6	
11	11	https://www.mozilla.org/en-US/firefox/central/	NULL	gro.allizom.www.	NULL	oX1r00k1b-1z	47356370932282	NULL	1	
12	12	https://www.dropbox.com/s/nf7c4k7uik11nb4/xfarma.zip?...	xfarma.zip	moc.xobpord.www.	1604827206508780	_XaIfR2UAxe2	47357382355080	Shared with Dropbox	7	
13	13	https://...	xfarma.zip	moc.tnetocresuxo...	1604827221729000	2DIZV5jUtpe	47357438756001	NULL	8	
14	14	http://161.107.169.17:3000/	Pharma Leaks   Wiki.js	71.961.701.161.	1604828523117801	_YQ3lqzeCXL	125510934541317	Leak what Big Pharma doesn't want us to know!	9	
15	15	http://161.107.169.17:3000/login	Login   Wiki.js	71.961.701.161.	1604828511112714	P9hOh4Xrahgd	125509488695933	NULL	9	
16	16	http://161.107.169.17:3000/register	Register   Wiki.js	71.961.701.161.	1604828404594848	Ghg5trvZAH8	12551179462539	NULL	9	
17	17	http://161.107.169.17:3000/en/leaks/xfarma_Secrets	New Page   Wiki.js	71.961.701.161.	1604828544331219	JTibGRUjB4Zm	125507611010971	NULL	9	
18	18	http://161.107.169.17:3000/en/leaks/xfarma_Secrets	xfarma Secrets   Wiki.js	71.961.701.161.	1604828661680543	WMmx5XXpJyB	12551111608076	What they don't want you to know!	9	
19	19	https://www.google.com/search?...	permanently and securely delete files ...	moc.elgoog.www.	1604829901473394	4c02gYkVn	47358501113144	NULL	10	
20	20	https://www.tecmint.com/permanently-and-securely-delet...	3 Ways to Permanently and Securely ...	moc.brimcet.www.	1604829910760993	XF_IDOASyReV	47358684199718	In this article, we will explain a number of ...	11	

Figure 11: Firefox History

```

File Actions Edit View Help
opty@opty:~/Documents/Lab_2$ ffind -o 0001052672 rick_disk.dd 284779
/home/rick/.local/share
opty@opty:~/Documents/Lab_2$ fls -o 0001052672 rick_disk.dd 284779
d/d 284780: tracker
d/d 448343: xorg
d/d 551612: ibus-table
d/d 551625: keyrings
d/d 312179: gnome-shell
d/d 312181: evolution
r/r 284781: session_migration-ubuntu
d/d 448380: applications
d/d 448383: sounds
d/d 448384: flatpak
d/d 448386: icc
d/d 312201: gnome-settings-daemon
d/d 312206: gvfs-metadata
d/d 448407: nautilus
r/r * 284699(realloc): recently-used.xbel.UAQPT0
r/r 284699: recently-used.xbel
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 284699 > recently-used.xbel
opty@opty:~/Documents/Lab_2$ md5sum recently-used.xbel
7af45076d5525a72b1dc7f1eea8d9972 recently-used.xbel
opty@opty:~/Documents/Lab_2$

```

Figure 12: Recently Used Files Log

```

File Actions Edit View Help
opty@opty:~/Documents/Lab_2$ ffind -o 0001052672 rick_disk.dd 136385
/home/rick/.bash_history
opty@opty:~/Documents/Lab_2$ icat -o 0001052672 rick_disk.dd 136385
sudo su
set -o | grep history
mkdir /data/xfarmadocs
mv /data/downloads/xfarma.zip /data/xfarmadocs/
evince /data/xfarmadocs/xfarma/xfarma-ceo-email.pdf
sudo su
echo $BACKUP_PASS
sudo su
sudo apt install srm
sudo apt install secure-delete
srm -vz /data/*
srm -rvz /data/*
opty@opty:~/Documents/Lab_2$ istat -o 0001052672 rick_disk.dd 136385
inode: 136385
Allocated
Group: 16
Generation Id: 426690121
uid / gid: 1000 / 1000
mode: rrw
Flags: Extents,
size: 278
num of links: 1

Inode Times:
Accessed: 2020-11-08 11:02:26.581560265 (GMT)
File Modified: 2020-11-08 11:02:26.581560265 (GMT)
Inode Modified: 2020-11-08 11:02:26.581560265 (GMT)
File Created: 2020-11-06 16:06:39.479448504 (GMT)

Direct Blocks:
558410
opty@opty:~/Documents/Lab_2$

```

Figure 13: Deletion Evidence



## 4 What can you tell about the identity of the person(s) responsible for leaking the files?

There are two persons responsible for leaking the files:

- N16H70WL: Who provided the leaked files by sending a link to its Dropbox to Rick Chick in the Mail Exchange. [Mail: N16H70WL\_services@protonmail.com] [Annex: Inbox] [Figure: 14]
- Rick Chick: Who made the Annotated Email PDF with its Comments and Highlights and uploaded it along with the Report downloaded from N16H70WL Dropbox to PharmaLeaks. [Mail: rick\_chick\_@outlook.com]

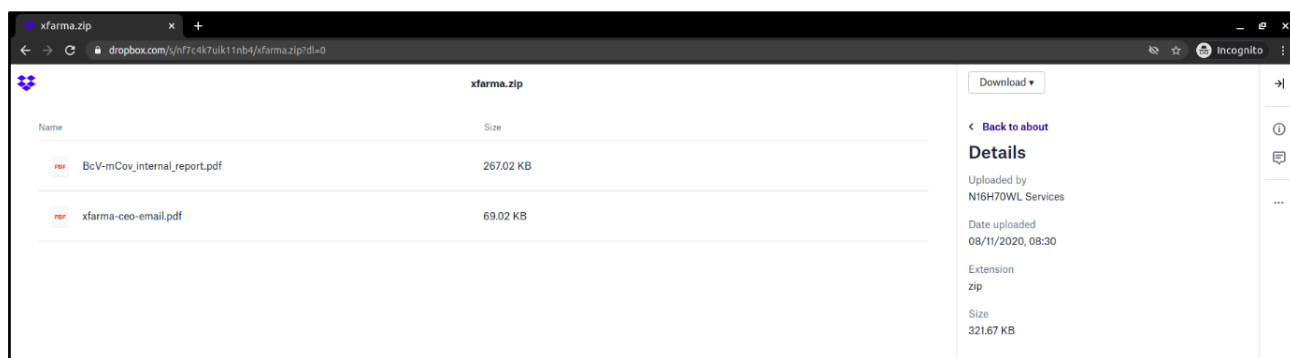


Figure 14: Dropbox Owner

## 5 Annexes:

**Note:** The Backups are not present in the *Annexes* folder along with the Report because it was not possible due to Size Constraints. However, it can be obtained following the commands below.

- *backup\_1604761201.zip*: Backup containing the *firefox\_cache* folder of the hard disk image of Rick's backup server at Nov 7 15:00.
  - **MD5:** 35dc3d5a455cbe5ad008a00060c57b58
  - **Command to Extract:** `icat -o 0000002048 backup_disk.dd 27007 > backup_1604761201.zip`
  - **Command to Unzip:** `unzip -P r1cK_7ru7h2020_CH1cK backup_1604761201.zip`
- *backup\_1604763001.zip*: Backup containing the *firefox\_cache* folder of the hard disk image of Rick's backup server at Nov 7 15:30.
  - **MD5:** de216611dd10fbd44b6328f6fd376d1
  - **Command to Extract:** `icat -o 0000002048 backup_disk.dd 27008 > backup_1604763001.zip`
  - **Command to Unzip:** `unzip -P r1cK_7ru7h2020_CH1cK backup_1604763001.zip`
- *backup\_1604827801.zip*: Backup containing the *downloads* folder, the *firefox\_cache* folder and the *xfarmadocs* folder of the hard disk image of Rick's backup server at Nov 8 09:30.
  - **MD5:** c8e0a92ccc6d09eaf8bd0e74bf9a61ff
  - **Command to Extract:** `icat -o 0000002048 backup_disk.dd 11760 > backup_1604827801.zip`
  - **Command to Unzip:** `unzip -P r1cK_7ru7h2020_CH1cK backup_1604827801.zip`

- *backup\_1604829601.zip*: Backup containing the *downloads* folder, the *firefox\_cache* folder and the *xfarmadocs* folder of the hard disk image of Rick's backup server at Nov 8 10:00.
  - **MD5**: 2a05c7471c5d518430ddea7441d1206
  - **Command to Extract**: `icat -o 0000002048 backup_disk.dd 35731 > backup_1604829601.zip`
  - **Command to Unzip**: `unzip -P r1cK_7ru7h2020_CH1cK backup_1604829601.zip`
- *backup\_1604831402.zip*: Backup containing the *downloads* folder, the *firefox\_cache* folder and the *xfarmadocs* folder of the hard disk image of Rick's backup server at Nov 8 10:30.
  - **MD5**: f5bf6e88c20e392d8a44902cdcf5f63a
  - **Command to Extract**: `icat -o 0000002048 backup_disk.dd 36025 > backup_1604831402.zip`
  - **Command to Unzip**: `unzip -P r1cK_7ru7h2020_CH1cK backup_1604831402.zip`
- *BcV-mCov\_internal\_report.pdf*: Report that was leaked to PharmaLeaks (Hashes matches), found in the hard disk image of Rick's backup server.
  - **MD5**: 8e5a62390ef3e86a40f91be4a7eff550]
  - **Present in**: Last three backups in *xfarmadocs/xfarma* folder.
- *xfarma-ceo-email.pdf*: Email that was used by Rick to create *xfarma-ceo-email\_annotated.pdf*, found in the hard disk image of Rick's backup server.
  - **MD5**: 87eca7a4b6ec8c47d2351172ab825a24
  - **Present in**: Last three backups in *xfarmadocs/xfarma* folder.
- *xfarma-ceo-email\_annotated.pdf*: Email that was leaked to PharmaLeaks (Hashes matches), found in the hard disk image of Rick's backup server.
  - **MD5**: dc1abdb8679d3ca10a7f40b5b6436a35
  - **Present in**: Last three backups in *xfarmadocs/xfarma* folder.
- *places.sqlite*: Contains the history of the browser as well as the downloads, which proves that *xfarma.zip* was downloaded from it and that he interacted with PharmaLeaks Website, found in the hard disk image of Rick's backup server.
  - **MD5**: 58690f087b47dcc17ff800d92177ce46
  - **Present in**: Last backup in *firefox\_cache* folder.
- *Inbox*: Contains relevant emails sent from N16H70W, found in the hard disk image of Rick's workstation.
  - **MD5**: ba4d14d3fd6e938e03adbaee1c224e18
  - **Command to Extract**: `icat -o 0001052672 rick_disk.dd 10703 > Inbox`
- *Sent*: Contains relevant emails sent to N16H70W, found in the hard disk image of Rick's workstation.
  - **MD5**: f734ddbbae63e1de47d4c072d00ec1793
  - **Command to Extract**: `icat -o 0001052672 rick_disk.dd 10874 > Sent`
- *recently-used.xbel*: Recently Used Files Logs, which shows that the emails were opened in Document Viewer and the browser used the leaked files on a suspicious moment, found in the hard disk image of Rick's workstation.
  - **MD5**: 7af45076d5525a72b1dc7f1eea8d9972
  - **Command to Extract**: `icat -o 0001052672 rick_disk.dd 284699 > recently-used.xbel`