



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
Кафедра Інформаційної Безпеки

Зворотна розробка та аналіз шкідливого програмного забезпечення

---

Лабораторна робота №4

Системи віддаленого керування

**Мета:**

Отримати навички аналізу та моделювання систем віддаленого керування.

Перевірив:

\_\_\_\_\_

Виконав:

студент III курсу

групи ФБ-01

Сахній Н.Р.

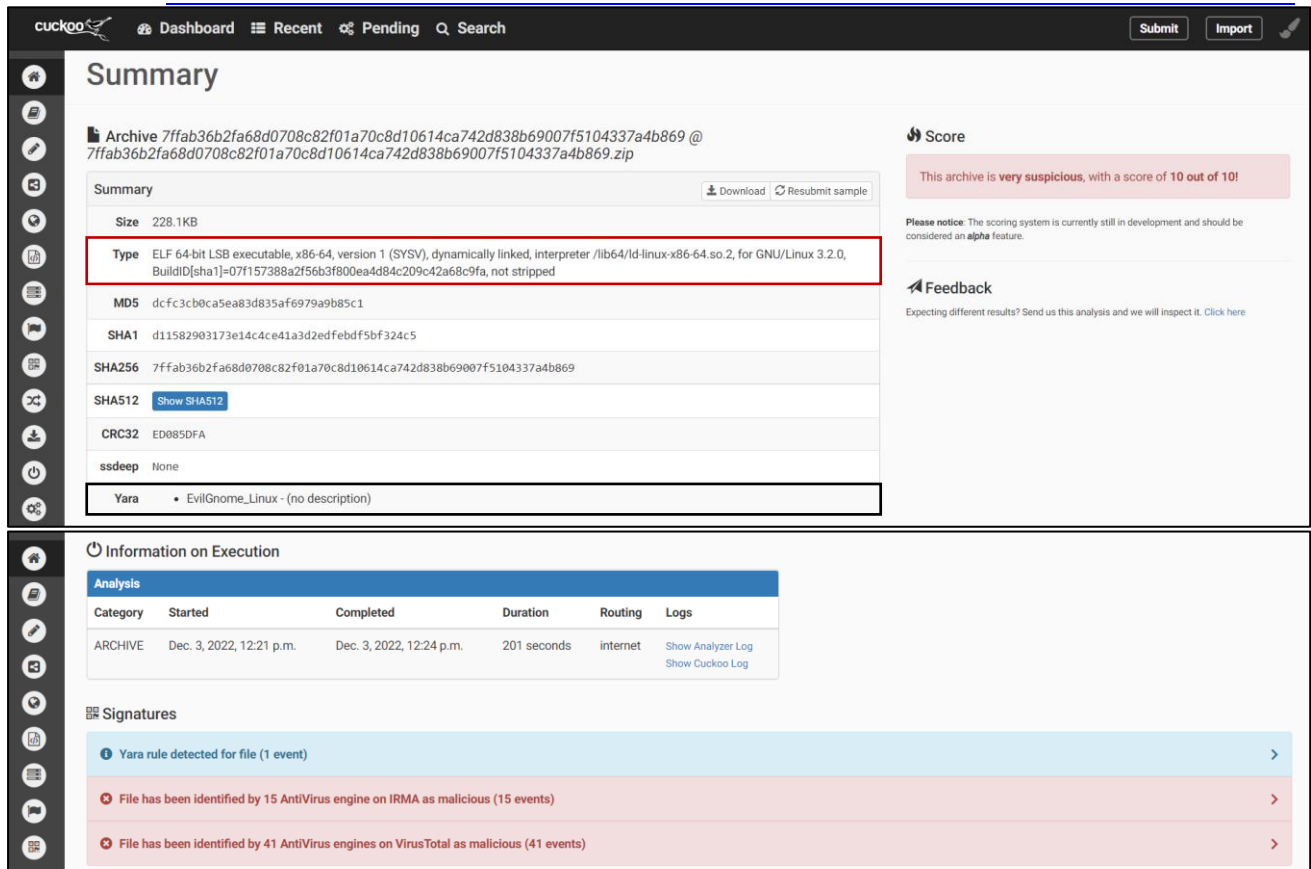
Київ 2022

## Завдання для виконання:

### 1. Аналіз зразків [EvilGnome](#)

#### – Cuckoo Sandbox

➤ [7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869](#)



The screenshot shows the Cuckoo Sandbox web interface. The top navigation bar includes 'Dashboard', 'Recent', 'Pending', and 'Search'. The main content area is titled 'Summary' and displays details for an archive file. The file's size is 228.1KB. The 'Type' field is highlighted with a red box, indicating it is an 'ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=07f157388a2f56b3f800ea4d84c209c42a68c9fa, not stripped'. The 'MD5' hash is 'dcfc3cb0ca5ea83d835af6979a9b85c1'. The 'SHA1' hash is 'd11582903173e14c4ce41a3d2efebdf5bf324c5'. The 'SHA256' hash is '7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869'. The 'SHA512' hash is 'Show SHA512'. The 'CRC32' hash is 'ED085DFA'. The 'ssdeep' hash is 'None'. The 'Yara' rule is 'EvilGnome\_Linux - (no description)'. On the right, the 'Score' section indicates the archive is 'very suspicious' with a score of 10 out of 10. A 'Feedback' section is also present.

**Summary**

Archive 7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869 @ 7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869.zip

Download Resubmit sample

Size 228.1KB

Type ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=07f157388a2f56b3f800ea4d84c209c42a68c9fa, not stripped

MD5 dcfc3cb0ca5ea83d835af6979a9b85c1

SHA1 d11582903173e14c4ce41a3d2efebdf5bf324c5

SHA256 7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869

SHA512 Show SHA512

CRC32 ED085DFA

ssdeep None

Yara EvilGnome\_Linux - (no description)

**Score**

This archive is very suspicious, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

**Feedback**

Expecting different results? Send us this analysis and we will inspect it. Click here

**Information on Execution**

Analysis

Category	Started	Completed	Duration	Routing	Logs
ARCHIVE	Dec. 3, 2022, 12:21 p.m.	Dec. 3, 2022, 12:24 p.m.	201 seconds	internet	Show Analyzer Log Show Cuckoo Log

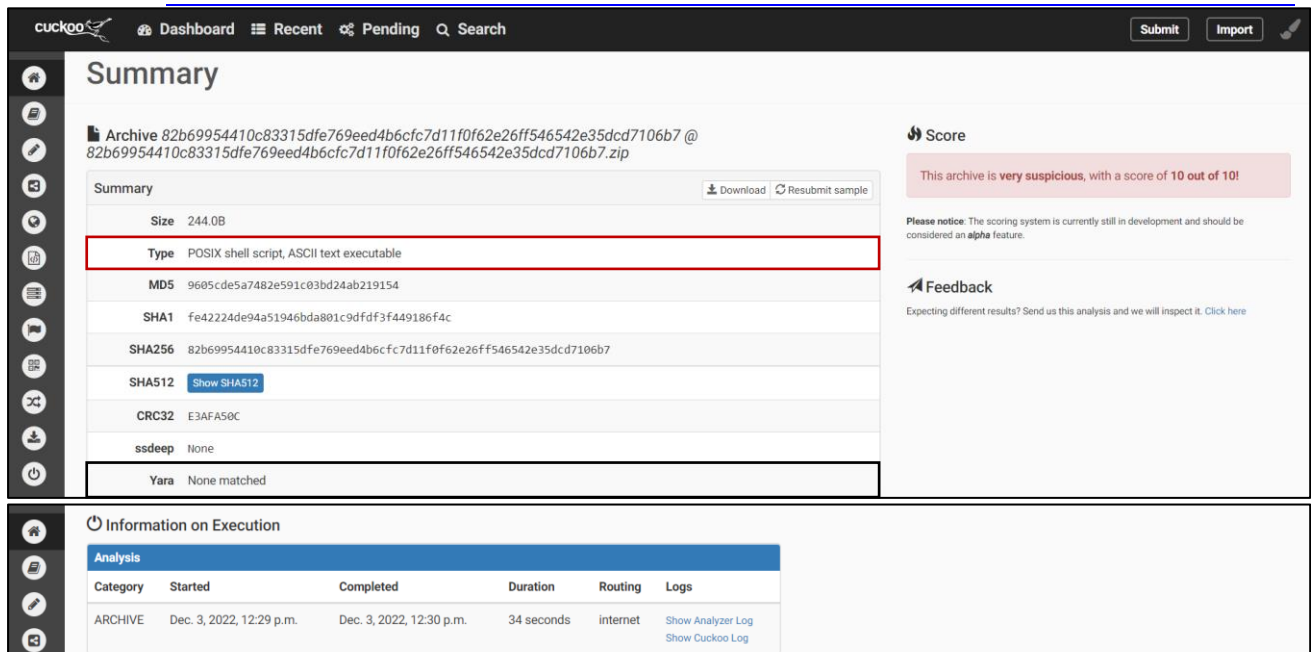
**Signatures**

Yara rule detected for file (1 event)

File has been identified by 15 AntiVirus engine on IRMA as malicious (15 events)

File has been identified by 41 AntiVirus engines on VirusTotal as malicious (41 events)

➤ [82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7](#)



The screenshot shows the Cuckoo Sandbox web interface for a different file. The file's size is 244.0B. The 'Type' field is highlighted with a red box, indicating it is a 'POSIX shell script, ASCII text executable'. The 'MD5' hash is '9605cde5a7482e591c03bd24ab219154'. The 'SHA1' hash is 'fe42224de94a51946bda801c9dfdf3f449186f4c'. The 'SHA256' hash is '82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7'. The 'SHA512' hash is 'Show SHA512'. The 'CRC32' hash is 'E3AF50C'. The 'ssdeep' hash is 'None'. The 'Yara' rule is 'None matched'. On the right, the 'Score' section indicates the archive is 'very suspicious' with a score of 10 out of 10. A 'Feedback' section is also present.

**Summary**

Archive 82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7 @ 82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7.zip

Download Resubmit sample

Size 244.0B

Type POSIX shell script, ASCII text executable

MD5 9605cde5a7482e591c03bd24ab219154

SHA1 fe42224de94a51946bda801c9dfdf3f449186f4c

SHA256 82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7

SHA512 Show SHA512

CRC32 E3AF50C

ssdeep None

Yara None matched

**Score**

This archive is very suspicious, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

**Feedback**

Expecting different results? Send us this analysis and we will inspect it. Click here

**Information on Execution**

Analysis

Category	Started	Completed	Duration	Routing	Logs
ARCHIVE	Dec. 3, 2022, 12:29 p.m.	Dec. 3, 2022, 12:30 p.m.	34 seconds	internet	Show Analyzer Log Show Cuckoo Log

Просто для прикладу продемонструємо на цьому зразку ШПЗ, які антивіруси на IRMA детектують його шкідливим, розгорнувши відповідник список у Signatures↓

Signatures	
File has been identified by 11 AntiVirus engine on IRMA as malicious (11 events)	
Avast Core Security (Linux)	BV:Agent-BGL [Trj]
Kaspersky Antivirus (Win)	HEUR:Trojan-Spy.Shell.EvilGnm.a
ESET NOD32 Antivirus (Linux)	Linux/EvilGnome.A trojan
GData (Windows)	Virus: Trojan.Linux.EvilGnome.A (Engine A)
eScan Antivirus (Linux)	Trojan.Linux.EvilGnome.A(DB)
McAfee CLI scanner (Linux)	Linux/EvilGnome trojan
Sophos Anti-Virus (Linux)	Linux/EvilGnm-A
DrWeb Antivirus (Linux)	Linux.EvilGnome.1
ClamAV (Linux)	Unix.Malware.Agent-7062664-0
Bitdefender Antivirus (Linux)	Trojan.Linux.EvilGnome.A
Emsisoft Commandline Scanner (Windows)	Trojan.Linux.EvilGnome.A (B)

Аналогічно детектування VirusTotal на шкідливість цього зразку ШПЗ ↓

File has been identified by 29 AntiVirus engines on VirusTotal as malicious (29 events)	
Lionic	Trojan.Shell.EvilGnm.ltc
MicroWorld-eScan	Trojan.Linux.EvilGnome.A
ALYac	Trojan.Linux.EvilGnome
Sangfor	Malware.Generic-Script.Save.ba282
Arcabit	Trojan.Linux.EvilGnome.A
Cyren	Unix/EvilGnome.A
Symantec	Trojan Horse
ESET-NOD32	Linux/EvilGnome.A
TrendMicro-HouseCall	Trojan.SH.GNOMEX.A
Avast	BV:Agent-BGL [Trj]
ClamAV	Unix.Malware.Agent-7062664-0
Kaspersky	HEUR:Trojan-Spy.Shell.EvilGnm.a
BitDefender	Trojan.Linux.EvilGnome.A
Tencent	Win32.Trojan-spy.Evilgnm.Hquv
Ad-Aware	Trojan.Linux.EvilGnome.A
Sophos	Linux/EvilGnm-A
Comodo	Malware@#xivn0tqyvrf
DrWeb	Linux.EvilGnome.1
VIPRE	Trojan.Linux.EvilGnome.A
TrendMicro	Trojan.SH.GNOMEX.A
McAfee-GW-Edition	Linux/EvilGnome
FireEye	Trojan.Linux.EvilGnome.A
Emsisoft	Trojan.Linux.EvilGnome.A (B)
Antiy-AVL	Trojan/Generic.ASSuf.2A942
GData	Trojan.Linux.EvilGnome.A
McAfee	Linux/EvilGnome
Ikarus	Trojan.Linux.Evilgnome
Fortinet	Linux/EvilGnome.Altr
AVG	BV:Agent-BGL [Trj]

➤ [a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032](https://cuckoo.sh/analysis/a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032)

Dashboard
Recent
Pending
Search
Submit
Import

Archive a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032 @ a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032.zip
Download
Resubmit sample

Summary

Size754.0B
TypePOSIX shell script, ASCII text executable
MD5997a43976b11604836798045827648a6
SHA1b3d07c5f9c2181c9e828b5f87240a46e20c2b67f
SHA256a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032
SHA512Show SHA512
CRC322FAE3F97
ssdeepNone
YaraNone matched

Score

This archive is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback
Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
ARCHIVE	Dec. 3, 2022, 12:38 p.m.	Dec. 3, 2022, 12:38 p.m.	25 seconds	internet	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

Signatures

File has been identified by 13 AntiVirus engine on IRMA as malicious (13 events)

File has been identified by 28 AntiVirus engines on VirusTotal as malicious (28 events)

## – Антивірусна лабораторія

Detection	7ffab3...7a4b86	82b699...d7106b	a21acb...7e8032
AV0 Windows Defender	Trojan:Linux/EvilGnome.B!MTB	0 threats found	Trojan:Linux/EvilGnome.A!MTB
AV1 Avira Free Security	LINUX/Dldr.Agent.wqskh	0 threats found	0 threats found
AV2 Avast Free Antivirus	BV:Agent-BGL [Trj]	BV:Agent-BGL [Trj]	BV:Agent-BGL [Trj]
AV3 360 Total Security	No threats found	No threats found	No threats found
AV4 AVG AntiVirus FREE	No malware found	No malware found	No malware found
AV5 Bitdefender Antivirus Free	Infected file detected an hour ago	Infected file detected an hour ago	Infected file detected an hour ago

## 2. Розробка систему віддаленого керування:

- Продемонструємо роботу системи віддаленого керування для наглядності

```
Run: server X
"D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Server\venv\Scripts\python.exe"

Hello! This is simple Remote Control System ☺
[>] Прослуховування на :25254
[>] З'єднано з 192.168.43.214:49830
[>] Під'єднано до Windows ОС
```

- Довідкове меню із доступних команд для віддаленого виконання на ОС клієнта

```
Run: server X
D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client> help
Доступні команди:
♣ Інтерфейс командного рядка для даної ОС
• download/upload {file} -> завантаження та вивантаження файлу
• screenshot -> знімок екрану в даний момент часу
• photo -> зробити 1 фотографію за допомогою веб-камери
• video -> зробити 5с відеозапис із веб-камери
• audio -> зробити 10с аудіозапис за допомогою мікрофона
• exit -> вийти із сервера та клієнта
• help -> переглянути довідкове меню
```

- Переглянемо вміст поточної папки користувача та деякого цікавого файлу ʘ

```
D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client> dir
Volume in drive D is K@ўл® B@~
Volume Serial Number is 526D-D7D8

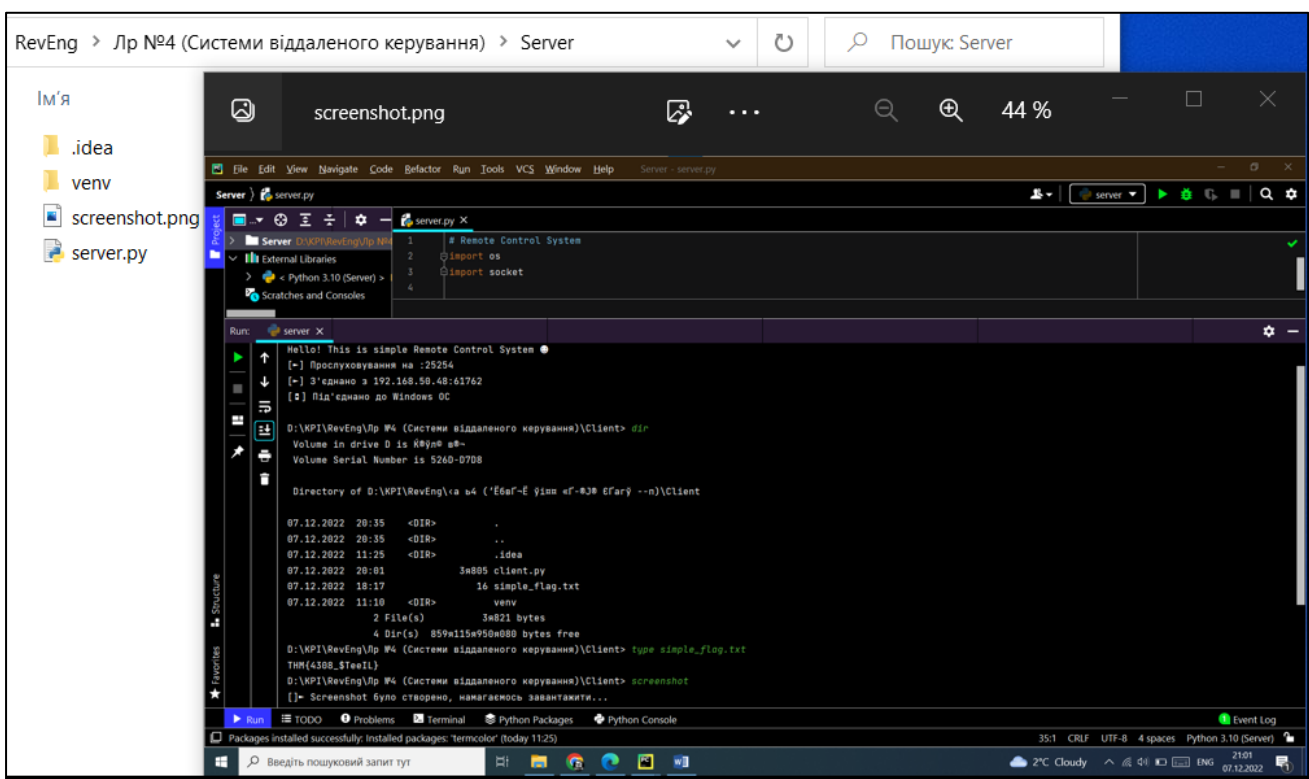
Directory of D:\KPI\RevEng\Лр №4 ('Ё6вГ-Ё ўм« «Г-®J® ЁГарў --n)\Client

07.12.2022  19:52    <DIR>          .
07.12.2022  19:52    <DIR>          ..
07.12.2022  11:25    <DIR>          .idea
07.12.2022  19:50                3я806 client.py
07.12.2022  18:17                16 simple_flag.txt
07.12.2022  11:10    <DIR>          venv
                2 File(s)                3я822 bytes
                4 Dir(s)  859я123я822я592 bytes free
D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client> type simple_flag.txt
TMM{4308_$TeeIL}
```

- Виконаємо команду, яка зробить знімок екрану

```
D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client> screenshot
[]- Screenshot було створено, намагаємось завантажити...
[]- Завантаження файлу: screenshot.png
[]- Розмір файлу: 237717
[*]- Завантажується...
[] Запис у файл -> screenshot.png
[*]- Завантажується...
[] Запис у файл -> screenshot.png
```

```
[*]- Завантажується...
[]- Завантаження завершено!
[]- Screenshot було видалено із ОС клієнта
```



screenshot.png

- Отримаємо зображення з веб-камери

```
D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client> photo
[]- Photo було створено, намагаємось завантажити
[]- Завантаження файлу: photo.jpg
[]- Розмір файлу:
[*]- Завантажується...
[] Запис у файл -> photo.jpg
[*]- Завантажується...
[] Запис у файл -> photo.jpg
```

```
[*]─ Завантажується...
[ ]─ Завантаження завершено!
[]─ Photo було видалено із ОС клієнта
```

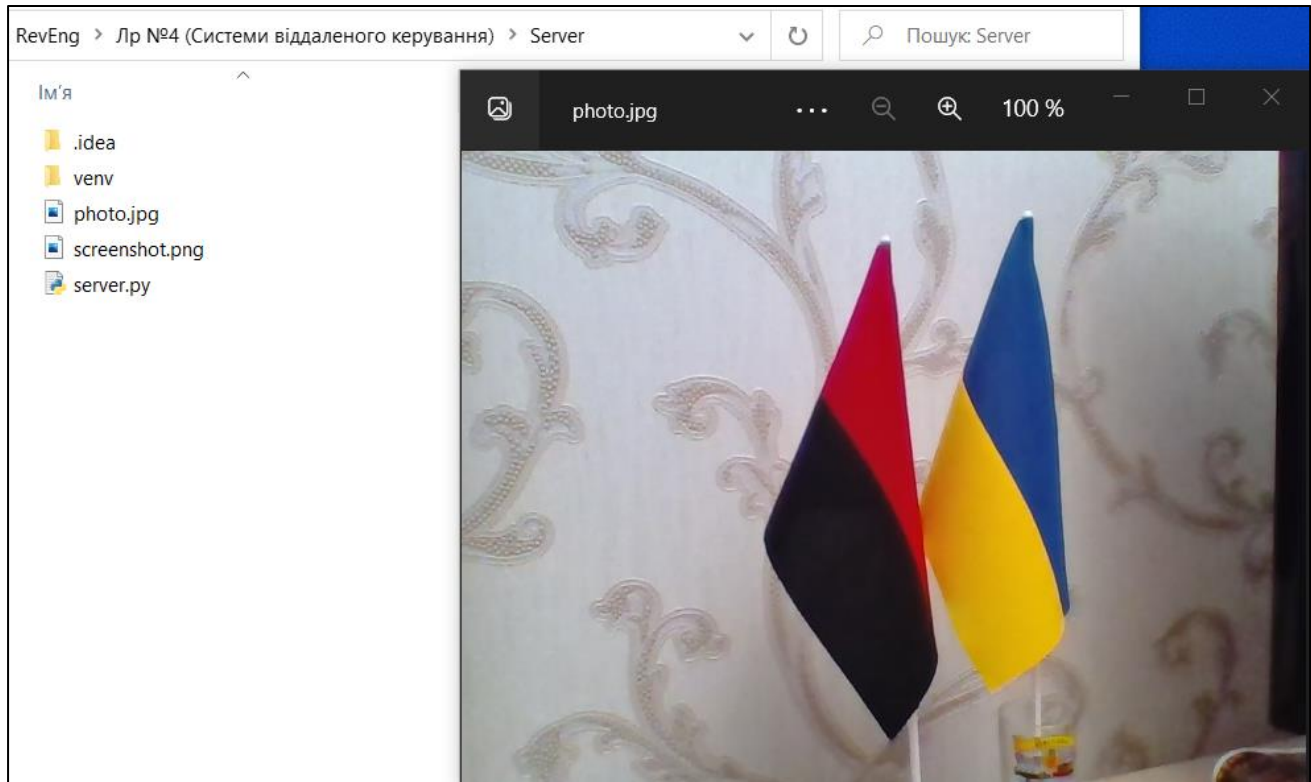
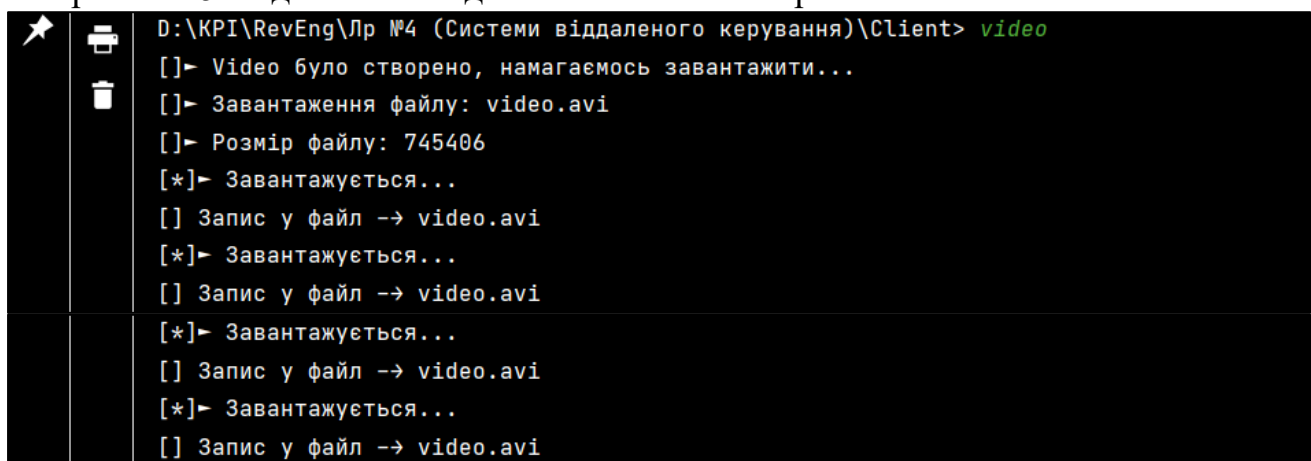


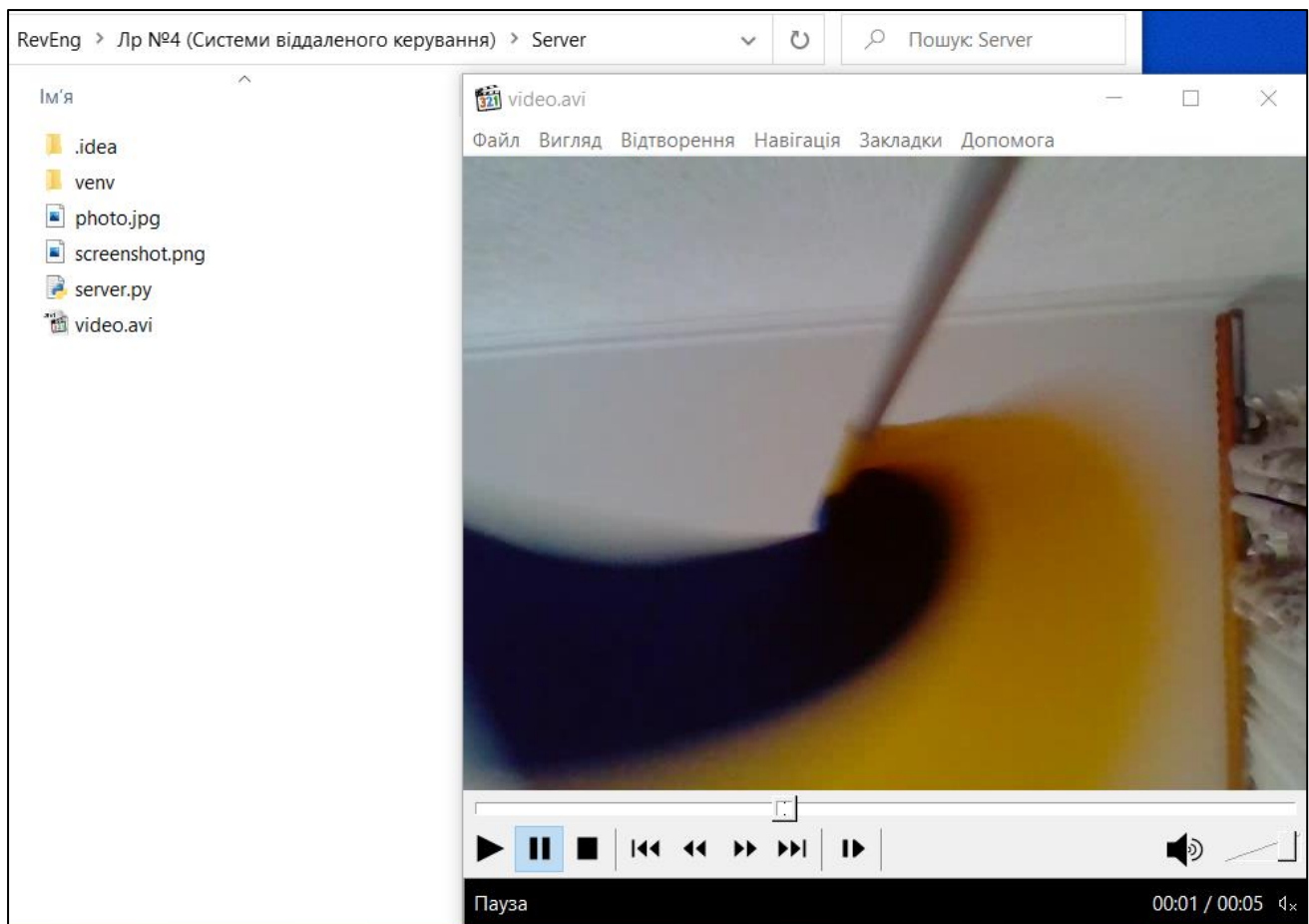
photo.jpg

- Зробимо 5с відеозапис за допомогою веб-камери



```
[*]─ Завантажується...
[ ]─ Завантаження завершено!
[]─ Video було видалено із ОС клієнта
```





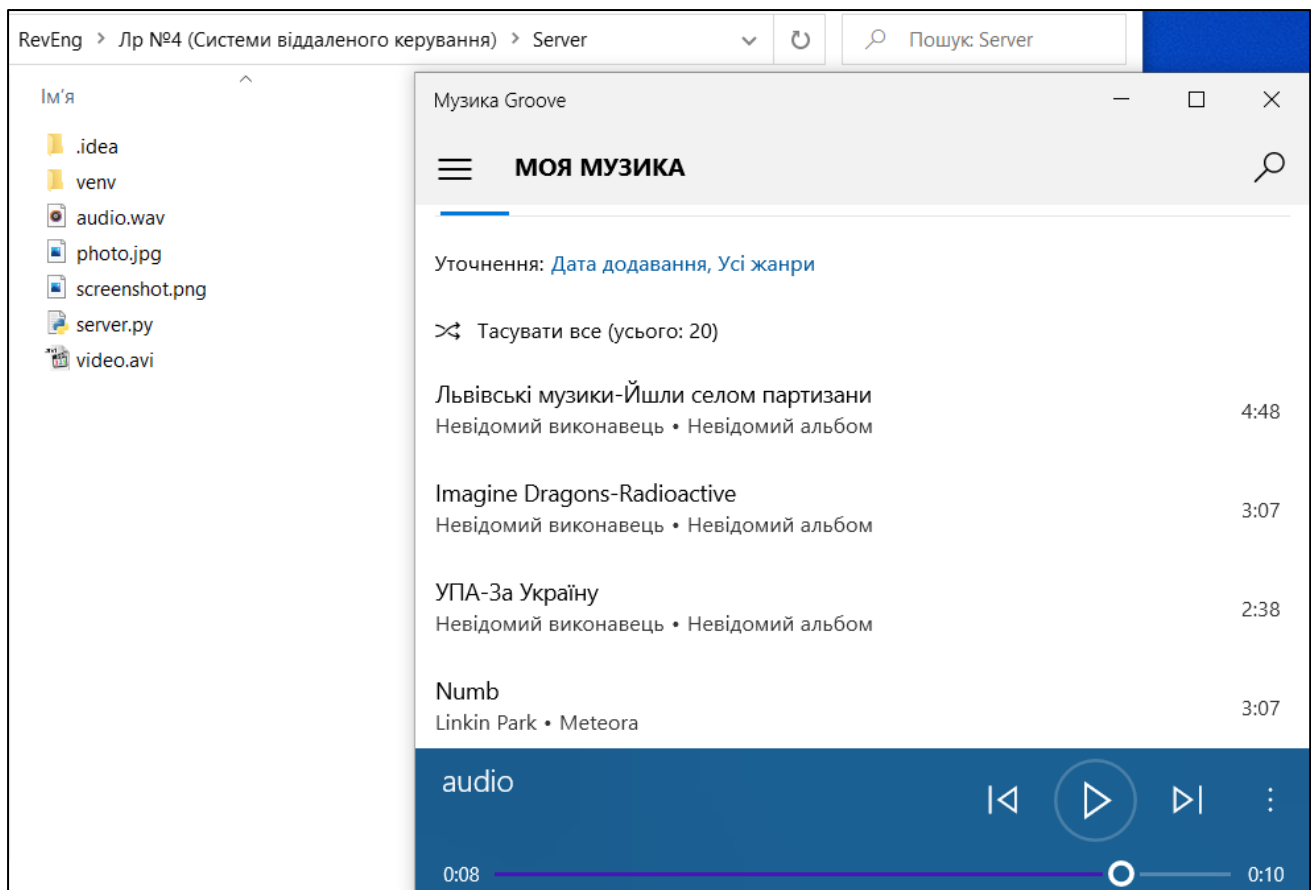
video.avi

- Отримаємо 10с аудіозапис за допомогою мікрофона

```

D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client> audio
[ ]> Audio було створено, намагаємось завантажити...
[ ]> Завантаження файлу: audio.wav
[ ]> Розмір файлу: 3528058
[*]> Завантажується...
[ ] Запис у файл -> audio.wav
[*]> Завантажується...
[ ] Запис у файл -> audio.wav
[*]> Завантажується...
[ ] Запис у файл -> audio.wav
[*]> Завантажується...
[ ] Запис у файл -> audio.wav
[*]> Завантажується...
[ ] Запис у файл -> audio.wav
[*]> Завантажується...
[ ]> Завантаження завершено!
[ ]> Audio було видалено із ОС клієнта
  
```





audio.wav

- Продемонструємо, що вміст папки клієнта ніяким чином не змінився ↓

```
Directory of D:\KPI\RevEng\ка ь4 ('ЁбвГ-Ё їищ «Г-@J@ ёГарґ --п)\Client
07.12.2022  21:04    <DIR>          .
07.12.2022  21:04    <DIR>          ..
07.12.2022  11:25    <DIR>          .idea
07.12.2022  21:04                3я809 client.py
07.12.2022  18:17                16 simple_flag.txt
07.12.2022  11:10    <DIR>          venv
                2 File(s)        3я825 bytes
                4 Dir(s)   859я113я091я072 bytes free
```

- А також команда, яка дозволить завершити з'єднання між клієнтом та сервером

```
Run: server X
D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client> exit
Process finished with exit code 0
```

```
Run: client X
"D:\KPI\RevEng\Лр №4 (Системи віддаленого керування)\Client\venv\Scripts\python.exe"
Process finished with exit code 0
```

На стороні клієнта програма все виконувала у фоновому режимі (без "слідів")

### 3. Аналіз отриманого зразка в системах поведінкового аналізу ШПЗ: – Cuckoo Sandbox

The screenshot displays the Cuckoo Sandbox web interface. The top navigation bar includes 'Dashboard', 'Recent', 'Pending', and 'Search'. The main content area is titled 'Summary' and shows details for a file named 'client.py'. The file's size is 3.7KB, and its type is 'Python script, UTF-8 Unicode text executable, with CRLF line terminators'. The MD5 hash is 'bf8fc2a3dc620ccb3fde6a66601b6ca'. The SHA1 hash is '7c3dccc78bf7a0123364df8bbd1d9ba89969e0a18'. The SHA256 hash is 'fe2b497d3547f11971f9b5f416a0688d87ba43518a2043430308f4482eb8faf3'. The SHA512 hash is '80326E61'. The CRC32 hash is '80326E61'. The ssdeep value is 'None'. The Yara rule is 'None matched'. On the right, a 'Score' section indicates a score of 0.0 out of 10, with a note that the scoring system is still in development. Below the summary, there is a table for 'Information on Execution' with columns for Category, Started, Completed, Duration, Routing, and Logs. The table shows one execution record for the file 'client.py'.

### – Антивірусна лабораторія

Detection	client.py
AV0 Windows Defender	0 threats found
AV1 Avira Free Security	0 threats found
AV2 Avast Free Antivirus	<b>Шкідливих програм не знайдено</b>
AV3 360 Total Security	No threats found
AV4 AVG AntiVirus FREE	<b>No malware found</b>
AV5 Bitdefender Antivirus Free	<b>Your system is clean!</b>

### Висновки:

У цій лабораторній роботі досліджувалися технології побудови ШПЗ та систем віддаленого керування шляхом моделювання. Для цього мною було реалізовано програмний код серверної та клієнтської сторони, що при запуску буде забезпечувати віддалене з'єднання з системою керування.

Як можна було впевнитись: детектування зразка для клієнтської сторони відсутнє як і в Cuckoo Sandbox, так і в антивірусній лабораторії, а отже, програма без проблем може бути запущена на виконання, т.б. буде встановлено з'єднання.