

# BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 06 (Session 06)

Tên chủ đề: CTF Final Test

GVHD: Đoàn Minh Trung

Ngày báo cáo: 29/05/2024

Nhóm: 07

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.021.ATCL

STT	Họ và tên	MSSV	Email
1	Nguyễn Tân Phát	21522447	21522447@gm.uit.edu.vn
2	Nguyễn Đình Bảo Long	21522303	21522303@gm.uit.edu.vn
3	Đào Vĩnh Thịnh	21522632	21522632@gm.uit.edu.vn
4	Ngô Minh Thiên	21522623	21522623@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Thực hiện	Kết quả tự đánh giá
1	Memory	Memory.dmp Dump.raw	100%
2	Network	Tìm IP của web server: Hoàn thành Tìm username và password của một tài khoản sử dụng server: Hoàn thành Hacker tấn công từ đâu: Hoàn thành Tìm lỗ hổng hacker khai thác: Hoàn thành Tìm tài khoản hacker đã login: Hoàn thành Tìm Server hacker dùng để test: Hoàn thành Tìm mật khẩu của admin: Hoàn thành Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao? Hoàn thành	100%
3	Android	Bypass_login	100%
4	Steganography	DecaovsDatg	0%

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành,

## BÁO CÁO CHI TIẾT

## 1. Memory

## Câu Memory.dmp

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ strings memory.dmp | grep -i "distrib_description="
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
DISTRIB_DESCRIPTION=
DISTRIB_DESCRIPTION=%s
DISTRIB_DESCRIPTION=
DISTRIB_DESCRIPTION=%s
DISTRIB_DESCRIPTION=
DISTRIB_DESCRIPTION=%s
```

## Kiểm tra linux version.

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ strings memory.dmp | grep -i "linux version"
o The intent is to make the tool independent of Linux version dependencies,
o The intent is to make the tool independent of Linux version dependencies,
MESSAGE:Linux version 5.13.0-39-generic (build@lcy02-amd64-080) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 2022 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (build@lcy02-amd64-080) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 20
22 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (build@lcy02-amd64-080) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 20
22 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
o The intent is to make the tool independent of Linux version dependencies,
Linux version 5.13.0-39-generic (build@lcy02-amd64-080) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 20
22 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (build@lcy02-amd64-080) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 20
22 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (build@lcy02-amd64-080) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 20
22 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
```

Thực hiện cài đặt Ubuntu20.04.01 rồi cài đặt linux-mage-5.13.0.39-generic lên đó và sử dụng.

```
[+] root@ubuntu: /home/lixsong/Downloads  
root@ubuntu:/home/lixsong/Downloads# uname -r  
5.13.0-39-generic  
root@ubuntu:/home/lixsong/Downloads#
```

#### Cài đặt thêm các gói cần thiết

```
sudo apt install dwarfdump build-essential libelf-dev zip
```

## Clone repo Volatility

```
git clone https://github.com/volatilityfoundation/volatility.git
```

Generate the profile

cd volatility/tools/linux

make

Zip lại tất cả mọi thứ

```
sudo zip $(lsb_release -i -s)_$(uname -r)_profile.zip module.dwarf /boot/System.map-$(uname -r)
```

```
root@ubuntu:/home/lixsong/Downloads/volatility/plugins/overlays/linux# file Ubuntu_5.13.0-39-generic_profile.zip
Ubuntu_5.13.0-39-generic_profile.zip: Zip archive data, at least v2.0 to extract
root@ubuntu:/home/lixsong/Downloads/volatility/plugins/overlays/linux#
```

python2 vol.py --info | grep Ubuntu

```
root@ubuntu:/home/lixsong/Downloads/volatility# python2 vol.py --info | grep Ubuntu
Volatility Foundation Volatility Framework 2.6.1
LinuxUbuntu_5_13_0-39-generic_profilex64 - A Profile for Linux Ubuntu_5.13.0-39-generic_profile x64
root@ubuntu:/home/lixsong/Downloads/volatility#
```

Vì đề hint là linux\_bash nên ta dùng câu lệnh này để check linux\_bash

python2 vol.py -f ./memory.dmp --profile=LinuxUbuntu\_5\_13\_0-39-generic\_profilex64  
linux\_bash

```
root@ubuntu:/home/lixsong/Downloads/volatility# python2 vol.py -f ./memory.dmp --profile=LinuxUbuntu_5_13_0-39-generic_profilex64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getuids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
-----
```

Pid	Name	Command	Time	Command
109633	bash	2022-04-10 05:49:10 UTC+0000	echo "aW5zZWNsYWJ7dzNsYzBtM190MF9tM20wcllfZjByM25zMWM1fQ==" > Un33dt0r3@dth1s.txt	
109633	bash	2022-04-10 05:49:10 UTC+0000	chmod 755 avml	
109633	bash	2022-04-10 05:49:10 UTC+0000	sudo rm ~/.bash_history	
109633	bash	2022-04-10 05:49:18 UTC+0000	sudo ./avml memory.dmp	

Decode đoạn base64 này

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ echo "aW5zZWNsYWJ7dzNsYzBtM190MF9tM20wcllfZjByM25zMWM1fQ==" | base64 --decode
inseclab{w3lc0m3_t0_m3m0rY_f0r3ns1c5}
```

Flag: inseclab{w3lc0m3\_t0\_m3m0rY\_f0r3ns1c5}

Câu Dump.raw

Dùng Volatility check profile của dump.raw

## Session 01: Memory Forensics

Nhóm 01

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/lixsong/Downloads/volatility/dump.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800029f2110L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff800029f3d00L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2022-04-08 19:05:12 UTC+0000 (Managing Linux kernel modules)
Image local date and time : 2022-04-08 12:05:12 -0700
Links for linux-image-5.13.0-39-generic
No screenshot available. Sorry.
```

Dùng option pslist để xem thử các tiến trình

PID	PPID	Process Name	State	Priority	Threads	Start Address	End Address	CreateTime	LastWriteTime
844	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
888	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
924	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
980	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
384	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
1048	456	spoolsv.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
1084	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
1204	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
1272	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:23 UTC+0000	2022-04-08 17:44:23 UTC+0000
1372	456	cyrus-sasl.dll	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1420	456	VGAAuthService.exe	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1452	456	vm3dservice.exe	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1476	456	vmtoolsd.exe	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1484	1452	vm3dservice.exe	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1520	456	wlms.exe	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1664	1372	cyrus-sasl.dll	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1680	340	conhost.exe	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1696	1664	ssh.exe	Running	0	0	0	0	2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
1840	456	sppsvc.exe	Running	0	0	0	0	2022-04-08 17:44:25 UTC+0000	2022-04-08 17:44:25 UTC+0000
1872	616	WmiPrvSE.exe	Running	0	0	0	0	2022-04-08 17:44:25 UTC+0000	2022-04-08 17:44:25 UTC+0000
1968	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:44:25 UTC+0000	2022-04-08 17:44:25 UTC+0000
324	456	dllhost.exe	Running	0	0	0	0	2022-04-08 17:44:26 UTC+0000	2022-04-08 17:44:26 UTC+0000
2100	456	msdtc.exe	Running	0	0	0	0	2022-04-08 17:44:28 UTC+0000	2022-04-08 17:44:28 UTC+0000
2440	456	taskhost.exe	Running	0	0	0	0	2022-04-08 17:44:39 UTC+0000	2022-04-08 17:44:39 UTC+0000
2512	844	dwm.exe	Running	0	0	0	0	2022-04-08 17:44:39 UTC+0000	2022-04-08 17:44:39 UTC+0000
2528	2504	explorer.exe	Running	0	0	0	0	2022-04-08 17:44:39 UTC+0000	2022-04-08 17:44:39 UTC+0000
2916	2884	GoogleCrashHandler.exe	Running	0	0	0	1	2022-04-08 17:44:40 UTC+0000	2022-04-08 17:44:40 UTC+0000
2924	2884	GoogleCrashHandler.exe	Running	0	0	0	0	2022-04-08 17:44:41 UTC+0000	2022-04-08 17:44:41 UTC+0000
1336	456	SearchIndexer.exe	Running	0	0	0	0	2022-04-08 17:44:45 UTC+0000	2022-04-08 17:44:45 UTC+0000
1732	2528	vmtoolsd.exe	Running	0	0	0	0	2022-04-08 17:44:47 UTC+0000	2022-04-08 17:44:47 UTC+0000
2840	456	svchost.exe	Running	0	0	0	0	2022-04-08 17:46:26 UTC+0000	2022-04-08 17:46:26 UTC+0000
3228	456	taskhost.exe	Running	0	0	0	0	2022-04-08 18:44:26 UTC+0000	2022-04-08 18:44:26 UTC+0000
2332	2528	chrome.exe	Running	0	0	0	1	2022-04-08 19:02:52 UTC+0000	2022-04-08 19:05:17 UTC+0000
1756	1336	SearchProtocol.exe	Running	0	0	0	0	2022-04-08 19:05:04 UTC+0000	2022-04-08 19:05:04 UTC+0000
4172	1336	SearchFilterHost.exe	Running	0	0	0	0	2022-04-08 19:05:04 UTC+0000	2022-04-08 19:05:04 UTC+0000
4512	2332	DumpIt.exe	Running	0	0	0	1	2022-04-08 19:05:10 UTC+0000	2022-04-08 19:05:10 UTC+0000
4352	404	conhost.exe	Running	0	0	0	0	2022-04-08 19:05:10 UTC+0000	2022-04-08 19:05:10 UTC+0000
1656	924	WMIADAP.exe	Running	0	0	0	0	2022-04-08 19:05:25 UTC+0000	2022-04-08 19:05:25 UTC+0000
4380	616	WmiPrvSE.exe	Running	0	0	0	0	2022-04-08 19:05:25 UTC+0000	2022-04-08 19:05:25 UTC+0000

Ta dump thử tiến trình explorer.exe và chrome.exe để phân tích

## Session 01: Memory Forensics

Nhóm 01

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 memdump --dump-dir=./ -p 2528
```

Strings from the dump file:

```
$ strings ./2332.dmp | grep insec
insecLab.edu.vn
insecLab.edu.vn
insecLab.edu.vn
insecLab.edu.vn
TinsecLab.edu.vn
insecLab.edu.vn
https://insecLab.edu.vn/
insecLab.edu.vn
65a244ca-7b2d-4288-8eba-029304f1131ad0https://insecLab.edu.vn/nghien-cuu-ung-dung-phuong-phap-hoc-lien-ket-vao-viec-xay-dung-ids-trong-mang-kha-lap-trinh-sdn-duoc-chap-nhan-dang-tai-ky-yeu-hoi-nghi-khoa-hoc-quoc-te-nics-2021/V
77ba0e4c-96d0-b965-44f1546ec01d0https://www.google.com/search?q=insec&sourceid=chrome&ie=UTF-8
a0d906ff-c460-499e-8c52-dac3067c69a8dowhttps://insecLab.edu.vn/nghien-cuu-ung-dung-phuong-phap-hoc-lien-ket-vao-viec-xay-dung-ids-trong-mang-kha-lap-trinh-sdn-duoc-chap-nhan-dang-tai-ky-yeu-hoi-nghi-khoa-hoc-quoc-te-nics-2021/W
A boolean value that specifies if security should be enabled with insecure transports.
_keyhtps://insecLab.edu.vn/theme/js/jquery.min.js
_keyhtps://insecLab.edu.vn/theme/js/bootstrap.min.js
_keyhtps://insecLab.edu.vn/theme/js/bootstrap-table.min.js
_keyhtps://insecLab.edu.vn/includes/js/wp-emoji-release.min.js
insecLab\w3lcom3_t0
insecLab\w3lcom3_t0
insecLab\w3lcom3_t0
_keyhtps://insecLab.edu.vn/RCRD(
_keyhtps://insecLab.edu.vn/theme/is/waypoints.min.js
_keyhtps://insecLab.edu.vn/theme/is/minimal.lightbox.js
_keyhtps://insecLab.edu.vn/theme/is/jquery.flexslider.js
_keyhtps://insecLab.edu.vn/theme/is/resumable.js
Ntf9\insecLab\
insecLab
s://insecLab
upgrade-insecure-requests
Vad$InsecLab
upgrade-insecure-requests
upgrade-insecure-requests
upgrade-insecure-requests
```

Ubuntu Software Center details for Package: linux-image-5.13.0-39-generic:

- Version: 5.13.0-39-generic
- Description: Linux kernel version 5.13.0-39
- Architecture: amd64
- File size: 4.8 GB (4.04 GiB)
- Source package: linux-signed-hwe-5.13
- Links for linux-image-5.13.0-39-generic
- No screenshot available. Sorry.
- Ubuntu Resources:
  - Bug Reports
  - Ubuntu Changes
  - Copyfile File
- Download Source Package: linux-signed-hwe-5.13
- Maintainer: Canonical, Ltd.

Tìm được 1 phần của flag: inseclab{w3lcom3\_t0}

Tiếp tục dùng options filescan để tìm thông tin về inseclab

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 filescan | grep -i "insecLab"
```

Volatility Foundation Volatility Framework 2.6.1

```
0x0000000007167800 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Windows Live\Windows Live Mail.url
0x00000000071f38c0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Links\Suggested Sites.url
0x0000000013d8f8d40 16 0 -r-w \Device\HarddiskVolume1\Windows\Temp\vmware-vmtoolsd-NHK-InsecLab.log
0x0000000013d900590 33 1 -W-rw \Device\HarddiskVolume1\Windows\Temp\vmware-vmusr-NHK-InsecLab.log
0x0000000013d942590 33 1 -W-rw \Device\HarddiskVolume1\Windows\Temp\vmware-vmusr-NHK-InsecLab.log
0x0000000013d984590 33 1 -W-rw \Device\HarddiskVolume1\Windows\Temp\vmware-vmusr-NHK-InsecLab.log
0x0000000013d9c6590 33 1 -W-rw \Device\HarddiskVolume1\Windows\Temp\vmware-vmusr-NHK-InsecLab.log
0x0000000013da13070 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Help.lnk
0x0000000013da131c0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\On-Screen Keyboard.lnk
0x0000000013dab9070 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Software Store.url
0x0000000013dbebf860 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Links\Web Slice Gallery.url
0x0000000013d7eff20 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\WM4081UV\desktop.ini
0x0000000013d7f70040 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TAUH6A52\desktop.ini
0x0000000013d7f712a0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\NTISEAS26\desktop.ini
0x0000000013d7f71bc0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\50N5M0CM\desktop.ini
0x0000000013d7f729b0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\desktop.ini
0x0000000013d7f74590 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\50N5M0CM\desktop.ini
0x0000000013fc18860 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\computer.lnk
0x0000000013fc18a40 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WinRAR\What is new in the latest version.lnk
0x0000000013fc18c20 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\Contacts.lnk
0x0000000013fc1fd00 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\System32.lnk
0x0000000013fc263f0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Temp\Guest.bmp
0x0000000013fc2bfa0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\MSN Websites\MSN Entertainment.url
0x0000000013fc30070 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Desktop\flag.txt
0x0000000013fc31990 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Microsoft Websites\Microsoft At Work.url
0x0000000013fc371a0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
0x0000000013fc388a0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\NHK.contact.lnk
0x0000000013fc3cb1c0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Links for United States\USA.gov.url
0x0000000013fc3b740 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\MSN Websites\MSN Money.url
0x0000000013fc3bb90 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Microsoft Websites\IE Add-on site.url
0x0000000013fc3cc40 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Microsoft Websites\Microsoft At Home.url
0x0000000013fc3ed10 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Link for United States\Gobierno USA.gov.url
0x0000000013fc45350 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk
0x0000000013fc456b0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Contacts\NHK.contact
0x0000000013fc66660 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Pictures\Untitled.png
0x0000000013fc67d10 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\Microsoft Websites\IE site on Microsoft.com.url
0x0000000013fc68370 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Links\Desktop.lnk
0x0000000013fc68850 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\MSN Websites\MSNBC News.url
0x0000000013fc68bb0 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\MSN Websites\MSN Autos.url
0x0000000013fc69460 16 0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Favorites\MSN Websites\MSN Autos.url
```

Ta thấy có file flag.txt thử dumpfiles và cat flag.txt thử nhưng vẫn ra phần đầu của flag

## Session 01: Memory Forensics

Nhóm 01

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x0000000013fc30070 -D .

Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
DataSectionObject 0x13fc30070 None \Device\HarddiskVolume1\Users\NHK-InsecLab\Desktop\flag.txt

(lixsong㉿kali)-[~/Downloads/volatility]
$ ls
2916.pcap  CHANGELOG.txt  LEGAL.txt  MANIFEST.in  PKG-INFO  build  dump.raw
AUTHORS.txt  CREDITS.txt  LICENSE.txt  Makefile  README.txt  contrib  file.None.0xfffffa8003f

(lixsong㉿kali)-[~/Downloads/volatility]
$ cat file.None.0xfffffa8003f10350.dat
insecelab{w3lcom3_t0

(lixsong㉿kali)-[~/Downloads/volatility]
$
```

Check lại trong scan thì thấy có từ fl4g nên grep thử fl4g

```
0x0000000013fe7070 16 0 RW=rwu \Device\HarddiskVolume1\Users\TEMP\Temporary Internet Files\Content.IE5\77SMUUV\41-0bee62-68ddb2ab
0x0000000013fdffa70 16 0 -W=rwd \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\77SMUUV\41-0bee62-68ddb2ab
0x0000000013fdfd730 16 0 -W=rw- \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Google\Chrome\User Data\Default\Extension Scripts\MANIFEST-000001
0x0000000013fe4f9e0 16 0 RWD— \Device\HarddiskVolume1\Users\TEMP\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.lnk
0x0000000013fe5a4c0 16 0 RWD— \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Microsoft\Windows Mail\Stationery\Desktop.ini
0x0000000013feac700 16 0 RW=rwd \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ea714a333759727_0
0x0000000013feacd00 16 0 -W=rw- \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Temp\4080_487837860\CO
0x0000000013feb1ae0 16 0 R=rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini
0x0000000013feb6a20 16 0 R=rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
0x0000000013feb7f20 16 0 R=rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\fl4g.rar.lnk
0x0000000013febe2b0 16 0 RW=rwd \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\875c3b986209d0db_0
0x0000000013febe8d0 16 0 R=r-r-d \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Temp\IEUser.bmp
0x0000000013febea20 16 0 R=rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows_Exp
0x0000000013fed0880 16 0 R=rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Links\RecentPlaces.lnk
0x0000000013fed55e0 14 0 R=rwd \Device\HarddiskVolume1\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_1
0x0000000013fed7e60 13 0 R=rwd \Device\HarddiskVolume1\Users\IEUser\Downloads\ChromeSetup.exe
0x0000000013fedb8e0 15 0 R=rwd \Device\HarddiskVolume1\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
0x0000000013fed570 12 0 R=rwd \Device\HarddiskVolume1\Users\IEUser\Downloads\winrar-x64-611.exe
0x0000000013fee0b0 16 0 R=rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Local\Microsoft\Feeds Cache\desktop.ini
0x0000000013fee1400 16 0 RW—— \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Microsoft\CryptnetUrlCache\MetaData\F2DDCD2B5F37625B82E81F4976CEE400_B2C2817625
3BBB
0x0000000013fee8710 16 0 RW=rwd \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e28c9fea264bdee_0
0x0000000013feed30 16 0 RW=rwd \Device\HarddiskVolume1\Users\TEMP\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ac7645be3ef23f2_0
```

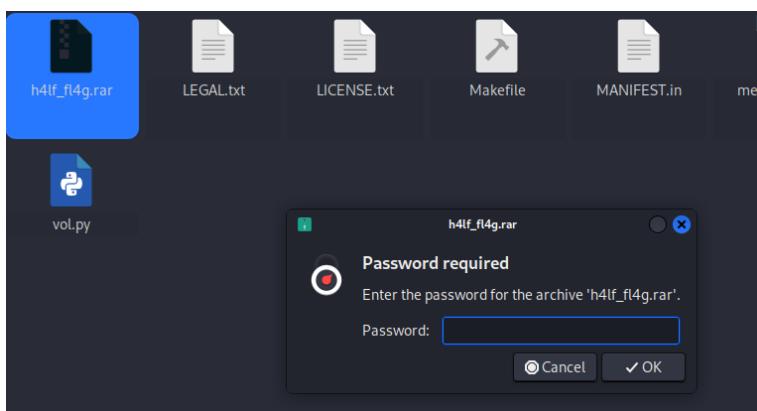
Ta tìm được file h4lf-fl4g.rar

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 filescan | grep -i "fl4g"

Volatility Foundation Volatility Framework 2.6.1
0x00000000071f3a10 16 0 RW—— \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
0x0000000013f804e20 16 0 RW=rw- \Device\HarddiskVolume1\Users\TEMP\AppData\Roaming\Microsoft\Windows\Recent\h4lf-fl4g.lnk
0x0000000013feb7f20 16 0 R=rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\fl4g.rar.lnk

(lixsong㉿kali)-[~/Downloads/volatility]
$
```

Dumpfiles này ra và extract ra nhưng thấy nó có password



Dùng tool rar2john online với đầu vào và file h4lf\_fl4g.rar và đưa vào file key.txt

Extract hashes from encrypted .zip or .rar or .7z files (1.1 GB max)

**Result**

⚠ Pay professionals to decrypt your remaining lists  
<https://hashes.com/en/escrow/view>

We can attempt to decrypt these hashes for free  
Enter a valid email address and we will message you if we are successful. You must click the link we send you to confirm your email address so we can attempt to decrypt your remaining lists.

Email

\$rar5\$16\$7a3f367e550900d03550fdaaa0937470\$15\$6cff83d489ca5fef8c6ae8fc7abd4168\$8\$2948156db3e079b9

```
Place( (root㉿kali)-[~/home/lixsong/Downloads/volatility]
└─# cat keyy.txt
h4lf_fl4g.rar:$rar5$16$7a3f367e550900d03550fdaaa0937470$15$6cff83d489ca5fef8c6ae8fc7abd4168$8$2948156db3e079b9
Place( (root㉿kali)-[~/home/lixsong/Downloads/volatility]
└─# john keyy.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 512/512 AVX512BW 16x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
r0cky0u          (h4lf_fl4g.rar)
1g 0:00:00:07 DONE (2024-05-31 22:25) 0.1297g/s 1959p/s 1959c/s 1959C/s drowssap1..lovemike
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

Place( (root㉿kali)-[~/home/lixsong/Downloads/volatility]
└─# )
```

Dùng tool john với wordlists rockyou.txt để crack password

Password tìm được là r0cky0u. Dùng password này để extract file h4lg\_fl4g.rar ta thu được nửa còn lại của flag.

```
Place( (root㉿kali)-[~/home/lixsong/Downloads/volatility]
└─# cat h4lf-fl4g.txt
_th3_w0rld_NHK}

Place( (root㉿kali)-[~/home/lixsong/Downloads/volatility]
└─# )
```

Flag hoàn chỉnh là: inseclab{w3lcom3\_t0\_th3\_w0rld\_NHK}

## Session 01: Memory Forensics

## Nhóm 01

Yêu cầu 2: Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra: + Liệu họ có để lại những dấu vết trên trình duyệt web?.

Đầu tiên, dùng plugins pslist để xem các process mà máy nạn nhân đang sử dụng để tìm các trình duyệt sử dụng

```
python2 vol.py -f dump.raw --profile=Win7SP1x64 pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64 Start	Exit
0xfffffa8003c71b10	System	4	0	91	546	—	0 2022-04-08 17:44:21 UTC+0000	
0xfffffa8005343620	smsvc.exe	264	4	2	29	—	0 2022-04-08 17:44:21 UTC+0000	
0xfffffa800584d060	csrss.exe	340	332	9	502	0	0 2022-04-08 17:44:22 UTC+0000	
0xfffffa800cdfc570	wininit.exe	392	332	3	76	0	0 2022-04-08 17:44:22 UTC+0000	
0xfffffa800b0bdfa80	cssrss.exe	404	384	16	279	1	0 2022-04-08 17:44:22 UTC+0000	
0xfffffa8005a1cb10	services.exe	456	392	7	223	0	0 2022-04-08 17:44:22 UTC+0000	
0xfffffa8005a276f0	lsass.exe	464	392	7	598	0	0 2022-04-08 17:44:22 UTC+0000	
0xfffffa8005a1f750	lsm.exe	472	392	9	157	0	0 2022-04-08 17:44:22 UTC+0000	
0xfffffa8005a248f0	winlogon.exe	496	384	3	110	1	0 2022-04-08 17:44:22 UTC+0000	
0xfffffa8005a6db10	svchost.exe	616	456	10	356	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005ab5b10	svchost.exe	684	456	8	274	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005ae69c0	svchost.exe	736	456	19	437	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005b1bb10	svchost.exe	844	456	17	425	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005b64870	svchost.exe	888	456	18	633	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005a86b10	svchost.exe	924	456	29	937	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005b96b10	svchost.exe	980	456	6	136	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005c04870	svchost.exe	384	456	15	482	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005c9d8f0	spoolsv.exe	1048	456	13	270	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005cd9870	svchost.exe	1084	456	17	310	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005d1b320	svchost.exe	1204	456	13	334	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005cd8060	svchost.exe	1272	456	12	218	0	0 2022-04-08 17:44:23 UTC+0000	
0xfffffa8005ceb060	cyrgrunsrv.exe	1372	456	6	99	0	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005d82060	VGAuthService.	1420	456	3	87	0	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005e11b10	vm3dservice.exe	1452	456	4	58	0	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005e4db10	vmtoolsd.exe	1476	456	13	293	0	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005e29b10	vm3dservice.exe	1484	1452	2	52	1	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005e53b10	wlms.exe	1520	456	4	45	0	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005e8b10	cyrgrunsrv.exe	1664	1372	0	—	0	0 2022-04-08 17:44:24 UTC+0000	2022-04-08 17:44:24 UTC+0000
0xfffffa8005eee8c0	conhost.exe	1680	340	2	33	0	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005fe6c0	sshd.exe	1696	1664	4	99	0	0 2022-04-08 17:44:24 UTC+0000	
0xfffffa8005bfb4c0	sppsvc.exe	1840	456	4	152	0	0 2022-04-08 17:44:25 UTC+0000	
0xfffffa8005f6b350	WmiPrvSE.exe	1872	616	10	203	0	0 2022-04-08 17:44:25 UTC+0000	
0xfffffa8005f917b0	svchost.exe	1968	456	5	95	0	0 2022-04-08 17:44:25 UTC+0000	
0xfffffa8004fe29c0	dllhost.exe	324	456	13	192	0	0 2022-04-08 17:44:26 UTC+0000	
0xfffffa80060713f0	msdtc.exe	2100	456	12	145	0	0 2022-04-08 17:44:28 UTC+0000	
0xfffffa8006135b10	taskhost.exe	2440	456	9	244	1	0 2022-04-08 17:44:39 UTC+0000	
0xfffffa8006150900	dwm.exe	2512	844	5	74	1	0 2022-04-08 17:44:39 UTC+0000	
0xfffffa8006156b10	explorer.exe	2528	2504	25	937	1	0 2022-04-08 17:44:39 UTC+0000	
0xfffffa8006265060	GoogleCrashHan	2916	2884	5	90	0	1 2022-04-08 17:44:40 UTC+0000	
0xfffffa80062689c0	GoogleCrashHan	2924	2884	5	83	0	0 2022-04-08 17:44:41 UTC+0000	
0xfffffa800629e060	SearchIndexer.	1336	456	13	712	0	0 2022-04-08 17:44:45 UTC+0000	
0xfffffa80063ff600	vmtoolsd.exe	1732	2528	8	278	1	0 2022-04-08 17:44:47 UTC+0000	
0xfffffa80061375c0	svchost.exe	2840	456	14	384	0	0 2022-04-08 17:46:26 UTC+0000	
0xfffffa800629a600	taskhost.exe	3228	456	5	141	1	0 2022-04-08 18:44:26 UTC+0000	
0xfffffa8004220060	chrome.exe	2332	2528	0	—	1	0 2022-04-08 19:02:52 UTC+0000	2022-04-08 19:05:17 UTC+0000
0xfffffa80053f6a10	SearchProtocol	1756	1336	8	282	0	0 2022-04-08 19:05:04 UTC+0000	
0xfffffa8004eebb10	SearchFilterHo	4172	1336	5	101	0	0 2022-04-08 19:05:04 UTC+0000	
0xfffffa8005461700	DumpIt.exe	4512	2332	5	46	1	1 2022-04-08 19:05:10 UTC+0000	
0xfffffa80062eab10	conhost.exe	4352	404	2	52	1	0 2022-04-08 19:05:10 UTC+0000	
0xfffffa80061e3b10	WMIADAP.exe	1656	924	6	769	—	0 2022-04-08 19:05:25 UTC+0000	

Ta thấy có sử dụng chrome, internet explorer. Ta thử kiểm tra chrome.

Ở đây ta cài thêm 2 file chromehistory.py và sqlite\_help.py để chạy được plugin chromehistory

```
python2 vol.py --plugins=/home/lixsong/Downloads/4Chrome/ -f dump.raw
chromehistory
```

## Session 01: Memory Forensics

Nhóm 01

```
(lixsong@kali):~/Downloads/volatility
$ python2 vol.py --plugins=/home/lixsong/Downloads/4Chrome/ -f dump.raw chromehistory

Volatility Foundation Volatility Framework 2.6.1
** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.malware.keys (ImportError: No module named distorm3)
** Failed to import volatility.plugins.all_shells (ImportError: No module named distorm3)
** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)

Index URL Title Visits Typed Last Visit Time Hidden Favicon ID
32 https://www.google.com/search?q=downlao ... 3015.501bj0j76sourceid=chrome0ie=UTF-8 download dumpit - Google 搜尋 6 0 2022-04-08 19:08:24.443945 N/A
29 https://www.google.com/search?q=downlao ... 3017.1911j0j76sourceid=chrome0ie=UTF-8 how to pass digital forensics - Google 搜尋 0 2022-04-08 19:08:24.443945 N/A
25 https://www.google.com/search?q=inscclab ... 4ymEAoAEBAEAEWmEBGsl1mzg-wiz inscclab - Google 搜尋 2 0 2022-04-08 19:08:32.823397 N/A
19 https://www.google.com/search?q=inscclab ... 4ymEAoAEBAEAEWmEBGsl1mzg-wiz inscclab - Google 搜尋 3 0 2022-04-08 19:08:32.823397 N/A
18 https://www.google.com/search?q=romano ... 61512.897j0j76sourceid=chrome0ie=UTF-8 ronan - Google 搜尋 2 0 2022-04-08 19:08:25.836168 N/A
16 https://www.google.com/search?q=downlao ... 3017.1911j0j76sourceid=chrome0ie=UTF-8 download hxxp - Google 搜尋 2 0 2022-04-08 18:58:06.184801 N/A
9 https://www.google.com/search?q=downlao ... 8130.4374j0j76sourceid=chrome0ie=UTF-8 download hidden tear - Google 搜尋 2 0 2022-04-08 18:47:57.622508 N/A
6 https://www.google.com/search?q=q+golate ... 58.216279j0j96sourceid=golate-hidden-tear: ransomware open-sources (github.com) - Google 搜尋 2 0 2022-04-08 18:44:39.388108 N/A
5 https://www.google.com/search?q=q+adq=a ... 1601.2.189j0j96sourceid=chrome0ie=UTF-8 a - Google 搜尋 2 0 2022-04-08 18:41:05.127338 N/A
26 https://www.google.com/search?q=q+downlao ... 1219.3638j0j76sourceid=chrome0ie=UTF-8 downloadRAR - Google 搜尋 2 0 2022-04-08 18:40:45.492725 N/A
7 https://pastebin.com/ CTFtime.org / All about CTF (Capture The Flag) 1 0 2022-04-08 18:40:15.851134 N/A
7 https://pastebin.com/ Pastebin.com - #1 paste tool since 2002! 2 1 2022-04-08 18:45:55.500915 N/A
4 https://github.com/ GitHub: Where the world builds software - GitHub 1 1 2022-04-08 18:40:41.704202 N/A
39 https://github.com/thimbleweed/All-In-U ... lob/master/utilities/DumpIt/DumpIt.exe All-In-USB/DumpIt.exe at master · thimbleweed/All-In-USB · GitHub 2 0 2022-04-08 19:05:01.392413 N/A
34 https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt All-In-USB/DumpIt.exe at master · thimbleweed/All-In-USB · GitHub 4 0 2022-04-08 19:05:00.838389 N/A
36 https://windowsden.uk/1559294512/dumpit DumpIt for PC - Free Download | WindowsDen (Win 10/8/7) 2 0 2022-04-08 19:04:21.436776 N/A
38 https://windowsden.uk/get/1559294512 Download DumpIt Apk for PC 1 0 2022-04-08 19:04:19.636482 N/A
37 https://windowsden.uk/1559294512/dumpit#google_vignette Download DumpIt Apk for PC 1 0 2022-04-08 19:04:19.636482 N/A
35 https://dumpitsoft32.com/ Download DumpIt 1 0 2022-04-08 19:03:18.030699 N/A
33 https://down10.software/download-dumpit/ Download Free Download for Windows 11, 10, 7, 8/8.1 | Down10.Software 1 0 2022-04-08 19:03:02.450150 N/A
31 https://securityscorcard.com/solutions ... J0F9w1VmplBR2BLwZKEAAYASAAEgJLxPD_BwE 1 0 2022-04-08 19:02:45.423898 N/A
30 https://googleleadservices.com/pagead ... okX3AhWVH7cAHUJNCeQ0Qx6BaAgEAE8dct=1 1 0 2022-04-08 19:02:45.423898 N/A
28 https://ctftime.org/stats/2022?page=2 CTFtime.org / CTF teams 1 0 2022-04-08 19:02:16.829102 N/A
27 https://ctftime.org/stats/ CTFtime.org / CTF teams 1 0 2022-04-08 19:02:00.114201 N/A
24 https://inseclab.uit.edu.vn/nghien-cuu ... information-security-and-applications The UIT Information Security Laboratory 0 0 2022-04-08 19:01:13.500097 N/A
28 https://inseclab.uit.edu.vn/nghien-cuu ... u-hoi-nghi-khoa-hoc-quoc-te-nics-2021/ The UIT Information Security Laboratory 1 0 2022-04-08 19:01:13.500097 N/A
22 https://inseclab.uit.edu.vn/Cong-trinh- ... u-hoi-nghi-khoa-hoc-quoc-te-nics-2021/ The UIT Information Security Laboratory 1 0 2022-04-08 19:01:10.016493 N/A
21 https://inseclab.uit.edu.vn/bai-hao-igh ... eu-noi-hinghi-khoa-hoc-quoc-te-nics-2021/ The UIT Information Security Laboratory 1 0 2022-04-08 19:01:07.350574 N/A
20 https://inseclab.uit.edu.vn/ The UIT Information Security Laboratory 5 0 2022-04-08 19:01:14.015259 N/A
17 https://mh-nexus.de/en/hxd/ HxD - Frenware Hex Editor and Disk Editor | mh-nexus 1 0 2022-04-08 19:01:08.704246 N/A
15 https://github.com/golate/hidden-tear/ ... -tear/bin/Debug/hidden-tear.vshost.exe hidden-tear/hidden-tear.vshost.exe at master · golate/hidden-tear · GitHub 1 0 2022-04-08 18:51:31.159613 N/A
14 https://github.com/golate/hidden-tear/ ... ster/hidden-tear/hidden-tear/bin/Debug hidden-tear/hidden-tear/hidden-tear/bin/*ster · golate/hidden-tear · GitHub 2 0 2022-04-08 18:51:33.424394 N/A
13 https://github.com/golate/hidden-tear/ ... ter/hidden-tear/hidden-tear/Properties hidden-tear/hidden-tear/hidden-tear/Properties · golate/hidden-tear · GitHub 2 0 2022-04-08 18:51:33.424394 N/A
12 https://github.com/golate/hidden-tear/ ... tree/master/hidden-tear/hidden-tear hidden-tear/hidden-tear/hidden-tear at master · golate/hidden-tear · GitHub 5 0 2022-04-08 18:51:33.914445 N/A
11 https://github.com/golate/hidden-tear/ ... tree/master/hidden-tear hidden-tear/hidden-tear at master · golate/hidden-tear · GitHub 0 0 2022-04-08 18:51:35.373730 N/A
10 https://github.com/golate/hidden-tear/ ... GitHub - golate/hidden-tear: ransomware open-sources 4 0 2022-04-08 18:51:13.257215 N/A
8 https://pastebin.com/k2HuWZmp https://drive.google.com/file/d/1TxvMNB...RWJD7wZc/Viewusp=shari - Pastebin.com 1 0 2022-04-08 18:46:46.246539 N/A
9 https://www.win-rar.com/download.html?L=0 WinRAR download free and support: WinRAR Download Latest Version 1 0 2022-04-08 18:05:17.080333 N/A
2 https://www.win-rar.com/download.html WinRAR download free and support: WinRAR Download Latest Version 1 0 2022-04-08 18:05:17.080333 N/A
```

Ta phân tích thì thấy user này có vào 1 trang pastebin - pastebin là một trang giúp cho mọi người lưu trữ và chia sẻ text. Thủ đi vào đường dẫn này thử thì thấy có dẫn đến một link google drive.

The screenshot shows a Pastebin.com page with a single text file. The file content is a Google Drive link: <https://drive.google.com/file/d/1TxvMNB...RWJD7wZc/Viewusp=shari>. The page has a dark theme with various UI elements like sharing buttons (Facebook, Twitter), a login/signup button, and a sidebar listing other public pastes.

Ta vô trang drive



Thấy bảo là nothing here, but in here ta thử bôi đen thì thấy file còn kéo dài



→ Tải về và dùng xxd xem thử

```
(lixsong㉿kali)-[~/Downloads]
$ xxd empty.txt
00000000: 6e6f 7468 696e 6720 6865 7265 2c20 6275  nothing here, bu
00000010: 7420 6974 2068 6572 6509 2020 2020 0920  t it here.
00000020: 0920 2009 0920 2020 0920 2020 2020 200a  .
00000030: 2020 2020 2020 0920 2020 2009 2020 2020  .
00000040: 2020 2009 2020 0920 0920 0920 2020 0920  .
00000050: 0920 2020 2020 0920 0a20 2020 2009  .
00000060: 0909 2020 0909 2020 2009 2020 2020 2020  ..
00000070: 2009 2020 2020 2009 2020 2020 2020 2009  .
00000080: 2020 2020 2020 200a 2020 2020 0920 2020  .
00000090: 2020 0920 0920 2009 2009 2020 2009 2020  .
000000a0: 2020 0920 2020 2020 0920 2020 2020 2020  ..
000000b0: 0920 2020 2020 2020 0a09 0920 2020 2009  .
000000c0: 2020 0920 2020 2020 0920 2020 2009 2020  .
000000d0: 0920 2020 2020 0920 2020 2020 0920 2020  ..
000000e0: 2020 2020 0a20 2020 2020 2020 0920 2020  ..
000000f0: 2009 2020 0920 0920 2020 2020 0920 2020  ..
00000100: 0920 2020 2020 0920 2020 2009 2020 2020  ..
00000110: 2009 2020 200a 2020 2020 2009 2020 2020  ..
00000120: 0920 2020 0920 2020 2020 0920 200a  . . . .
```

Sau khi tìm hiểu thì tìm tool stegsnow để giải mã.

```
(lixsong㉿kali)-[~/Downloads]
$ stegsnow -C empty.txt
inseclab{y0u_c4n_s33_fl4g}
```

Flag: inseclab{y0u\_c4n\_s33\_fl4g}

Yêu cầu 3: Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra: Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK. Hãy tìm password đó.

BỘ MÔN

AN TOÀN THÔNG TIN

## Session 01: Memory Forensics

Thử nghiệm lấy thông tin mật khẩu.

Ở đây ta dùng hivelist để lấy ra trườnng địa chỉ bắt đầu trọng bộ nhớ của nơi lưu trữ thông tin đăng ký và quản lý về tài khoản người dùng Windows.

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined) 9-
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Virtual Physical Name
0xffff8a0012a6010 0x00000000e18b010 \??\C:\Users\sshd_server\ntuser.dat
0xffff8a0012bb270 0x00000004829e270 \??\C:\Users\sshd_server\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffff8a0017f4010 0x000000019cda010 \??\C:\Users\TEMP\ntuser.dat
0xffff8a001882410 0x000000021a41410 \??\C:\Users\TEMP\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffff8a0032eb010 0x000000011ff7a010 \??\C:\Windows\AppCompat\Programs\Amcache.hve
0xffff8a00484c010 0x00000000a8ca5010 \Device\HarddiskVolume1\Boot\BCD
0xffff8a004ecd010 0x00000000529bb010 \SystemRoot\System32\Config\DEFAULT
0xffff8a004ed7010 0x0000000052913010 \SystemRoot\System32\Config\SAM
0xffff8a00000e010 0x00000000a9537010 [no name]
0xffff8a000024010 0x00000000a9742010 \REGISTRY\MACHINE\SYSTEM
0xffff8a000063010 0x00000000a9683010 \REGISTRY\MACHINE\HARDWARE
0xffff8a0005dc010 0x0000000054799010 \SystemRoot\System32\Config\SECURITY
0xffff8a0005e6010 0x0000000013a00010 \SystemRoot\System32\Config\SOFTWARE
0xffff8a000e2b010 0x00000000a4cc8010 \??\C:\System Volume Information\Syscache.hve
0xffff8a000e61010 0x000000000dc00010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffff8a000ef1010 0x000000004b8d9010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
```

Sau đó ta trích xuất mã băm mật khẩu vào một tập tin text để tiện quan sát

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 hashdump -y 0xffff8a000024010 -s 0xffff8a004ed7010 > pwhashes.txt
Volatility Foundation Volatility Framework 2.6.1
Linux kernel extra modules for version 5.13.0 on 64 bit x86 SMP
Ubuntu Resource
```

Mật khẩu đã được hash và thông tin chỉ được lưu lại ở dạng hash.

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ cat pwhashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
NHK-InsecLab:1000:aad3b435b51404eeaad3b435b51404ee:141be588e38b145c4e1f274b646898eb:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16fcfc061c3359db455d00ec27035:::
```

Đã thử dùng hashcat và tool hashes online nhưng ko ra kết quả pass ở dạng plaintext.

Thử dùng plugin lsadump để xem pass nhưng ko có

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
NL$KM
0x00000000 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 @.....
0x00000010 ef 8e 01 77 ad a5 85 29 da 7c 46 c4 d1 5b a7 d4 ...w...).|F..[..
0x00000020 10 38 2d d7 b5 84 7d 93 45 5d 7b e7 28 5f e9 c1 .8-...}E]{.(..
0x00000030 fe be 9e 6a 42 d8 a5 6b 47 99 30 67 fc a7 5c 6c ...jB..KG.0g..\l
0x00000040 49 ea 4c 1e 2b 89 21 56 a2 33 01 bd e6 71 fa 4d I.L.+.!V.3...q.M
0x00000050 90 36 4c e1 5f a5 29 5a 13 12 08 90 4d 7c 15 67 .6L_.)Z....M|.g

DefaultPassword
0x00000000 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010 50 00 61 00 73 00 73 00 77 00 30 00 72 00 64 00 P.a.s.s.w.0.r.d.
0x00000020 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 !.....
SC OpenSSHD
0x00000000 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010 44 00 40 00 72 00 6a 00 33 00 33 00 6c 00 31 00 D.@.r.j.3.l.1.
0x00000020 6e 00 67 00 00 00 00 00 00 00 00 00 00 00 00 00 n.g.....
DPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,.....
0x00000010 01 00 00 00 4a b5 78 3e 9b 1a 62 d6 52 08 75 86 ....J.x>..b.R.u.
0x00000020 13 a2 3b 36 3c 96 ad 6e 74 1e 31 1d bf e1 89 85 ..;6<..nt.1....
0x00000030 49 ac 51 cf ca 28 97 2d 8d c6 a4 b6 00 00 00 00 I.Q..(.-.....

```

Tải và cài đặt plugins mimikatz để tìm password

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f dump.raw --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Module User Domain Password
-----
```

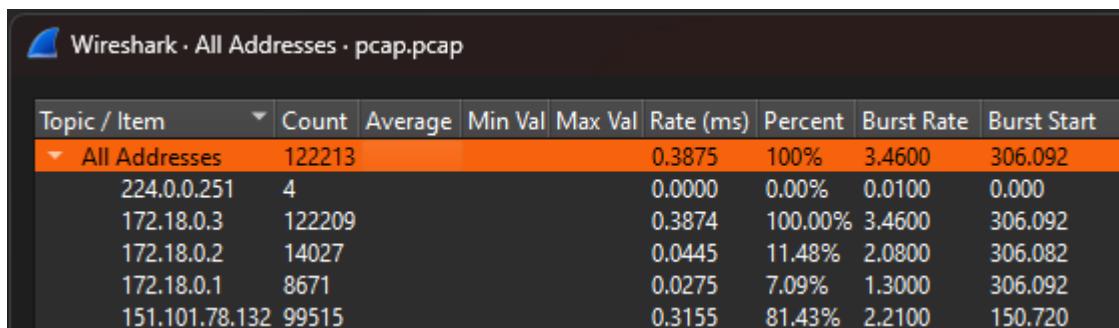
Module	User	Domain	Password
wdigest	NHK-InsecLab	IEWIN7	AntinHK
wdigest	sshd_server	IEWIN7	D@rj33l1ng
wdigest	IEWIN7\$	WORKGROUP	

Flag: inseclab{AntiNHK}

## 2. Network

### a. Tìm IP của web server.

Sử dụng Statistics cho Ipv4 thì ta thấy tổng số packet của IP 224.0.0.251 và 172.18.0.3 bằng 122213, tổng số packet của 3 IP còn lại cũng bằng 122213



## Session 01: Memory Forensics

Nhóm 01

Xem qua vài packet thì thấy địa số là IP 172.18.0.3 response, 172.18.0.2 thì response các gói tin qua giao thức MySQL nên có thể đây là database của server, 172.18.0.1 có thể là default gateway. Vậy mô hình mạng theo em suy đoán thì hacker sử dụng máy có IP 151.101.78.132. IP của server là 172.18.0.3

19964 85.295431	172.18.0.3	172.18.0.2	TCP	74 33992 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=3228849465 TSecr=0 WS=128
19965 85.295462	172.18.0.2	172.18.0.3	TCP	74 3306 → 33992 [SYN, ACK] Seq=0 Ack=1 Win=32128 Len=0 MSS=1460 SACK_PERM TStamp=797336374 TSecr=3228849465 WS=128
19966 85.295469	172.18.0.3	172.18.0.2	TCP	66 33992 → 3306 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=3228849465 TSecr=797336374
19967 85.295690	172.18.0.2	172.18.0.3	MySQL	143 Server Greeting proto=10 version=8.3.0
19968 85.295698	172.18.0.3	172.18.0.2	TCP	66 33992 → 3306 [ACK] Seq=1 Ack=78 Win=32128 Len=0 TStamp=3228849465 TSecr=797336374
19969 85.295715	172.18.0.3	172.18.0.2	MySQL	206 Login Request user=root db=chall
19970 85.295723	172.18.0.2	172.18.0.3	TCP	66 3306 → 33992 [ACK] Seq=78 Ack=141 Win=31872 Len=0 TStamp=797336374 TSecr=3228849465
19971 85.295749	172.18.0.2	172.18.0.3	MySQL	72 Caching_sha2_password fast_auth_success
19972 85.295797	172.18.0.2	172.18.0.3	MySQL	77 Response OK
19973 85.295801	172.18.0.3	172.18.0.2	TCP	66 33992 → 3306 [ACK] Seq=141 Ack=95 Win=32128 Len=0 TStamp=3228849465 TSecr=797336374
19974 85.295873	172.18.0.3	172.18.0.2	MySQL	126 Request Query
19975 85.296151	172.18.0.2	172.18.0.3	MySQL	248 Response TABULAR Response
19976 85.296228	172.18.0.3	172.18.0.2	MySQL	71 Request Quit
19977 85.296238	172.18.0.3	172.18.0.2	TCP	66 33992 → 3306 [FIN, ACK] Seq=206 Ack=277 Win=32000 Len=0 TStamp=3228849465 TSecr=797336374
19978 85.296253	172.18.0.2	172.18.0.3	TCP	66 3306 → 33992 [FIN, ACK] Seq=277 Ack=207 Win=31872 Len=0 TStamp=797336374 TSecr=3228849465
19979 85.296257	172.18.0.3	172.18.0.2	TCP	66 33992 → 3306 [ACK] Seq=207 Ack=278 Win=32000 Len=0 TStamp=3228849465 TSecr=797336374

- b. Tìm username và password của một tài khoản sử dụng server. NHK nghe nói anh ta là một đặc vụ mật.

Sử dụng Ctrl+F tìm string “login”, gói tin 3786 có hiện thông tin username là ‘agentp’ và password là "perrytheplatypu"

3786 20.317082	172.18.0.1	172.18.0.3	HTTP	60 34068 → 80 [ACK] Seq=1 ACK=1 Win=32120 Len=0 TStamp=21071494894 TSecr=300177304
3786 20.317082	172.18.0.1	172.18.0.3	HTTP	614 POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3787 20.317080	172.18.0.2	172.18.0.1	TCP	cc 60 → 33060 [ACK] Seq=1 ACK=1 Win=32120 Len=0 TStamp=21071494894 TSecr=300177304
Source Address:	172.18.0.1			
Destination Address:	172.18.0.3			
Transmission Control Protocol, Src Port:	34068	Dst Port:	80	Seq: 1, Ack: 1, Len: 548
Source Port:	34068			
Destination Port:	80			
[Stream index: 1]				
[Conversation completeness: Complete, WITH_DATA (31)]				
[TCP Segment Len: 548]				
Sequence Number: 1 (relative sequence number)				
Sequence Number (raw): 2107149488				
[Next Sequence Number: 549 (relative sequence number)]				
Acknowledgment Number: 1 (relative ack number)				
Acknowledgment number (raw): 2896418520				
1000 .... = Header Length: 32 bytes (8)				
> Flags: 0x01 (PSH, ACK)				
Window: 251				
[Calculated window size: 32128]				
[Window size scaling factor: 128]				
Checksum: 0x5a73 [unverified]				
[Checksum Status: Unverified]				
Urgent Pointer: 0				
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps				
> [Timestamps]				
> [SEQ/ACK analysis]				
TCP payload (548 bytes)				
Hypertext Transfer Protocol				
HTML Form URL Encoded: application/x-www-form-urlencoded				
> Form item: "username" = "agentp"				
> Form item: "password" = "perrytheplatypus"				
0000 02 42 ac 12 00 03 02 42 eb 1f c6 4a 08 00 45 00 B.....B...J..E..				
0001 02 58 69 f9 40 00 40 06 76 7e ac 12 00 01 01 ac 12 Xi:@@.v~.....				
0020 00 03 85 14 00 50 7d 98 8c b0 ac a3 d6 88 18 .....P}.....				
0030 00 fb 5a 73 00 00 01 01 08 0a 5a 91 b1 2d 5e ..Zs.....Z.....^				
0040 69 98 58 4f 53 54 20 2f 6c 6f 67 69 6e 2e 70 68 i-POST / login.ph				
0050 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 p HTTP / /login.ph				
0060 3a 20 61 73 38 37 34 32 2e 64 75 63 6b 64 73 : as8742 .duckdns				
0070 2e 6f 72 67 3a 32 38 30 38 0d 0a 55 73 65 72 2d .org:288 8 -User-				
0080 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: Mozilla/5				
0090 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 .0 (X11; Linux x				
00a0 38 36 5f 36 34 3b 20 72 76 3a 31 32 31 2e 30 29 86_64; r : v12.0)				
00b0 20 47 65 63 6b 6f 2f 32 30 31 30 31 30 31 20 Gecko/201001				
00c0 46 69 72 65 66 6f 78 2f 31 32 31 2e 30 0d 0a 41 Firefox/121.0 -A				
00d0 63 65 70 74 3a 20 74 6f 78 74 2f 68 74 6d 6c ccept: t ext/html				
00e0 2c 61 70 78 6c 69 63 61 74 6f 6e 2f 78 68 74 ,application/xht				
00f0 6c 62 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml, applicati				
0100 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml; q = 0.9, ima				
0110 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 ge/avif, image/we				
0120 62 70 2c 2a 2f 3b 71 3d 30 2e 38 0d 0a 41 63 bp,*/*;q = 0.8 -Ac				
0130 63 65 70 74 2d 4c 61 6e 67 75 61 65 3a 20 65 cept-Lan guage: e				
0140 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 n-US,en; q = 0.5 -A				
0150 63 65 65 70 2d 45 6e 63 6f 64 69 66 67 3a 20 ccept-En coding:				
0160 67 7a 69 70 2c 2b 64 65 66 6c 61 74 65 0d 0a 43 gzip, de flate -C				
0170 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 ontent-type: app				
0180 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 2d 66 location /x-www-f				
0190 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a Content- Length:				
01a0 43 6f 66 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 40 -Onig in: http				
01b0 34 30 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 ::/as8742 .duckdn				
01c0 3a 2f 6f 2f 61 73 38 37 34 32 2e 64 75 63 6b 64 6e s.org:288 08 -Conn				
01d0 73 2e 6f 72 67 3a 32 38 30 38 0d 0a 43 6f 6e 6e action: keep-al				
01e0 65 63 64 69 6f 6e 3a 20 6b 65 70 2d 61 6c 69 76 65 72 3a 20 68 74 74 ve -Referer: htt				

pcap.pcap

Packets: 122232 · Displayed: 122232 (100%)

- c. Hacker tấn công từ bên ngoài mạng hay là từ bên trong mạng.

Theo câu a thì hacker tấn công từ bên ngoài mạng

- d. Lỗ hổng là hacker dùng để khai thác là gì?

Trong file pcap có rất nhiều packet có payload giống như sau, vậy nên attacker khai thác lỗ hổng SQL injection

4928 26.017854	172.18.0.1	172.18.0.3	TCP	66 57126 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=1519495165 TSecr=308:
4929 26.017907	172.18.0.1	172.18.0.3	HTTP	676 POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4930 26.017914	172.18.0.3	172.18.0.1	TCP	66 80 → 57126 [ACK] Seq=1 Ack=611 Win=31872 Len=0 TStamp=308183005 TSecr=15:
Frame 4929: 676 bytes on wire (5408 bits), 676 bytes captured (5408 bits)				
Ethernet II, Src: 02:42:ab:1f:c6:4a (02:42:ab:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)				
Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3				
Transmission Control Protocol, Src Port: 57126, Dst Port: 80, Seq: 1, Ack: 1, Len: 610				
Hypertext Transfer Protocol				
HTML Form URL Encoded: application/x-www-form-urlencoded				
> Form item: "username" = "agentp"				
> Form item: "password" = "perrytheplatypus"				
[Community ID: 1:URNMxz164CVtRNFTN0/G6oieuxo=]				

Packet 7073 cũng có 1 POST request gửi với username và password là admin

7071 33.102293	172.101.78.132	172.18.0.3	TCP	2240 00 → 70734 [PSH, ACK] Seq=10328504 Win=1-452 Len=2000 TSval=5014
7072 33.103027	172.18.0.3	151.101.78.132	TCP	66 36794 → 80 [ACK] Seq=3013 Ack=10323844 Win=793216 Len=0 TSval=5014
7073 33.105063	172.18.0.1	172.18.0.3	HTTP	655 POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
7074 33.106430	172.18.0.3	172.18.0.2	TCP	74 58040 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=5014
7075 33.106497	172.18.0.2	172.18.0.3	TCP	74 3306 → 58040 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_

```

Frame 7073: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits)
Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
Transmission Control Protocol, Src Port: 57126, Dst Port: 80, Seq: 1468, Ack: 1200, Len: 589
Hypertext Transfer Protocol
  HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "username" = "admin"
    Form item: "password" = "admin"
[Community ID: 1:URNWxz164CVtRNFTN0/G6oieuoxo=]

```

f. Server mà hacker dùng để test là gì?

Ở đây server hacker dùng để test là MySQL Database server

7071 33.102293	172.101.78.132	172.18.0.3	TCP	00 00 → 3306
95616 252.403070	172.18.0.3	172.18.0.2	TCP	74 45156 → 3306
95617 252.403158	172.18.0.2	172.18.0.3	TCP	74 3306 → 45156
95618 252.403179	172.18.0.3	172.18.0.2	TCP	66 45156 → 3306
95619 252.403705	172.18.0.2	172.18.0.3	MySQL	143 Server G
95620 252.403730	172.18.0.3	172.18.0.2	TCP	66 45156 → 3306
95621 252.403851	172.18.0.3	172.18.0.2	MySQL	206 Login Re
95622 252.403866	172.18.0.2	172.18.0.3	TCP	66 3306 → 45156
95623 252.403962	172.18.0.2	172.18.0.3	MySQL	72 Caching_
95624 252.404087	172.18.0.2	172.18.0.3	MySQL	77 Response
95625 252.404098	172.18.0.3	172.18.0.2	TCP	66 45156 → 3306
95626 252.404348	172.18.0.3	172.18.0.2	MySQL	234 Request
95627 252.405751	172.18.0.2	172.18.0.3	MySQL	257 Response
95628 252.406172	172.18.0.3	172.18.0.2	MySQL	71 Request
95629 252.406199	172.18.0.3	172.18.0.2	TCP	66 45156 → 3306
95630 252.406219	172.18.0.2	172.18.0.3	TCP	66 3306 → 45156
95631 252.406226	172.18.0.3	172.18.0.2	TCP	66 45156 → 3306
95632 252.406226	172.18.0.2	172.18.0.1	HTTP	412 HTTP/1.1

Như câu a thì ta đoán IP của hacker là 151.101.78.132 nên ta có thể thử dùng curl và nmap để thử xác định server của hacker

```
(lixsong㉿kali)-[~/Downloads/volatility]
$ curl -I 151.101.78.132
HTTP/1.1 500 Domain Not Found
Connection: keep-alive
Content-Length: 249
Server: Varnish
Retry-After: 0
content-type: text/html
Cache-Control: private, no-cache
X-Served-By: cache-hkg17930-HKG
Accept-Ranges: bytes
Date: Wed, 29 May 2024 16:18:23 GMT
Via: 1.1 varnish

(lixsong㉿kali)-[~/Downloads/volatility]
$ curl -I 172.18.0.1
^C

(lixsong㉿kali)-[~/Downloads/volatility]
$ nmap -sV 151.101.78.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 23:19 +07
Nmap scan report for 151.101.78.132
Host is up (0.048s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Varnish
443/tcp   open  ssl/https Varnish
2 services unrecognized despite returning data. If you know the service/version,
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
SF-Port80-TCP:V=7.94SVN%I=7%D=5/29%T=665755F3%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,1F0,"HTTP/1.\1\x20500\x20Domain\x20Not\x20Found\r\nConnection
SF::\x20close\r\nContent-Length:\x20221\r\nServer:\x20Varnish\r\nRetry-Aft
SF:er:\x200\r\nContent-Type:\x20text/html\r\nCache-Control:\x20private,\x20boot loader
SF:0no-cache\r\nX-Served-By:\x20cache-hkg17926-HKG\r\nAccept-Ranges:\x20by
SF:tes\r\nDate:\x20Wed,\x2029\x20May\x202024\x2016:21:07\x20GMT\r\nVia:\x20
SF:01.\1\x20varnish\r\n\r\n<html>\n<head>\n<title>Fastly\x20error:\x20un
SF:known\x20domain\x20</title>\n</head>\n<body>\n<p>Fastly\x20error:\x20un
SF:known\x20domain:\x20.\x20Please\x20check\x20that\x20this\x20domain\x20
SF:has\x20been\x20added\x20to\x20a\x20service.</p>\n<p>Details:\x20cache-
SF:hkg17926-HKG</p></body></html>"%r(HTTPOptions,1F0,"HTTP/1.\1\x20500\x2
Linux kernel specific documentation for version 5.13.0-39-generic

```

Có thể thấy service ở đây là Varnish.

Theo tìm hiểu thì Varnish hoạt động như một reverse proxy, đứng giữa người dùng và server backend. Các yêu cầu từ người dùng sẽ được gửi tới Varnish trước, sau đó Varnish sẽ quyết định có nên trả về nội dung từ cache hay chuyển tiếp yêu cầu tới server backend.

Do vậy hacker đã dùng Varnish để che giấu đi server của hacker thật sự nên chưa thể tìm ra.....

- Có vẻ là hacker đã lấy được mật khẩu của admin. Nhưng có người lại bảo là chưa. Vậy hacker đã lấy được mật khẩu của admin chưa? Mật khẩu của admin là gì? Hacker đã lấy được gì?

Từ khoảng packet thứ 87000 trở đi em thấy có rất nhiều packet có payload như sau

```
Frame 87086: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits)
Ethernet II, Src: 02:42:eb:1f:6:4a (02:42:eb:1f:6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
Transmission Control Protocol, Src Port: 41410, Dst Port: 80, Seq: 1, Ack: 1, Len: 380
HTTP/1.1 Transfer Protocol
GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27admin%27%29%2C1%2C1%29%3D%27a%27%2Csleep%284%29%2Csleep%280%29%2C2%27a%27+--+ HTTP/1.1\r\n
Host: as8742.duckdns.org:28080\r\n
User-Agent: python-requests/2.31.0\r\n
Accept-Encoding: gzip, deflate\r\n
Accept: */*\r\n
Connection: keep-alive\r\n
Cookie: PHPSESSID=fdd6853a47ea490bfe69cc82954439b8d\r\n
\r\n
[Full request URI: http://as8742.duckdns.org:28080/news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27admin%27%29%2C1%2C1%29%3D%27a%27%2Csleep%284%29%2Csleep%280%29%2C2%27a%27+--+ HTTP request 1/1]
[Response in frame: 87104]
[Community ID: 1:EP1VvyRShGxJ5glCpOhs0KtwGo=]
```

Thử dùng chatgpt với prompt “convert this payload to readable string for me” để hiểu payload dùng để làm gì

```
GET /news.php?name=" UNION SELECT IF(
    SUBSTR(
        (SELECT password FROM users WHERE username='admin'), 1, 1
    ) = '@',
    sleep(4),
    sleep(0)
), 'a' --
HTTP/1.1\r\n
```

1. **GET /news.php?name=**: This is the URL being requested, where `name` is a query parameter.
2. **\*\*\* UNION SELECT IF(..), 'a' -- \*\***: This is the SQL injection payload inserted into the `name` parameter.
  - `": The closing quote of the `name` parameter, potentially terminating any existing SQL query.
  - **UNION SELECT**: Combines the result of this SELECT statement with the result of any existing query.
  - **IF(condition, true\_value, false\_value)**: Conditional function in SQL.
    - **SUBSTR((SELECT password FROM users WHERE username='admin'), 1, 1)**: Retrieves the first character of the password for the user 'admin'.
    - **= '@'**: Checks if this first character is the `@` symbol.
    - **sleep(4)**: Causes a 4-second delay if the condition is true.
    - **sleep(0)**: Causes no delay if the condition is false.
  - **'a'**: The second part of the UNION SELECT statement, returning 'a'.
  - **--**: SQL comment marker to ignore the rest of the SQL query.
3. **HTTP/1.1\r\n**: The HTTP version used in the request.

Chatgpt còn giải thích giúp thêm về payload, thì em hiểu payload sẽ so sánh kí tự đầu tiên của password cho user 'admin' có phải là '@' hay không, nếu đúng thì sẽ sleep 4s. Lúc này em sẽ đi tìm những khoảng thời gian hacker gửi payload tấn công tới server và bị ngắt khoảng 4s không gửi payload tấn công nữa.

89377	330.867814	172.18.0.3	151.101.78.132	TCP	66 36794 + 80 [ACK] Seq=228044 Ack=137733138 Win=14074440 Len=0 TSval=501008113 TScer=1402774997
89378	330.893829	172.18.0.1	172.18.0.3	TCP	74 42132 + 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1408 PERM TSval=15109700041 TScer=15109700041 WS=128
89379	330.893836	172.18.0.3	151.101.78.132	TCP	74 42132 + 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1408 PERM TSval=15109700041 TScer=15109700041 WS=128
89380	330.893835	172.18.0.3	172.18.0.3	TCP	74 42132 + 80 [ACK] Seq=1 Win=32120 Len=0 MSS=1408 PERM TSval=15109700041 TScer=15109700041 WS=128
89381	330.893836	172.18.0.3	172.18.0.3	HTTP	448 36794 + 80 [GET] Seq=1 Win=32120 Len=0 MSS=1408 PERM TSval=15109700041 TScer=15109700041 WS=128
89382	330.893979	172.18.0.3	172.18.0.1	TCP	66 80 + 42132 [ACK] Seq=1 Ack=383 Win=31872 Len=0 TSval=308387881 TScer=15109700041
89383	330.894778	172.18.0.3	172.18.0.2	TCP	74 43188 + 3308 [SYN] Seq=0 Win=32120 Len=0 MSS=1408 PERM TSval=3228995864 TScer=803228995864 WS=128
89384	330.894780	172.18.0.3	172.18.0.2	TCP	74 43188 + 3308 [ACK] Seq=1 Win=32120 Len=0 TSval=3228995864 TScer=803228995864 WS=128
89385	330.894860	172.18.0.3	172.18.0.2	TCP	66 43188 + 3308 [ACK] Seq=1 Win=32120 Len=0 MSS=1408 PERM TSval=797481973 TScer=3228995864 WS=128
89386	330.895177	172.18.0.2	172.18.0.3	MySQL	143 Server Greeting greeting_proto->version=8.3.0
89387	330.895185	172.18.0.3	172.18.0.2	TCP	66 43188 + 3308 [ACK] Seq=1 Ack=78 Win=32120 Len=0 TSval=3228995864 TScer=97481973
89388	330.895203	172.18.0.3	172.18.0.2	MySQL	206 Login Request user=>root db=>null
89389	330.895205	172.18.0.3	172.18.0.2	TCP	66 43188 + 3308 [ACK] Seq=1 Ack=141 Win=321872 Len=0 TSval=797481973 TScer=3228995864
89390	330.895245	172.18.0.2	172.18.0.3	MySQL	72 Caching_sha2_password_fast_auth_success
89391	330.895308	172.18.0.2	172.18.0.3	MySQL	77 Response OK
89392	330.895312	172.18.0.2	172.18.0.3	TCP	66 43188 + 3308 [ACK] Seq=141 Ack=95 Win=32128 Len=0 TSval=3228995065 TScer=797481973
89393	330.895313	172.18.0.2	172.18.0.3	MySQL	79 Query OK
89394	330.895346	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89395	330.898662	172.18.0.3	151.101.78.132	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137736018 Win=1407440 Len=0 TSval=501008144 TScer=1402775015
89396	330.909672	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89397	330.910001	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137736098 Win=1407440 Len=0 TSval=501008155 TScer=1402775022
89398	330.919380	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89399	330.919341	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137741778 Win=1437440 Len=0 TSval=501008165 TScer=1402775035
89400	330.936475	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89401	330.936476	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137744659 Win=1437440 Len=0 TSval=501008162 TScer=140277504
89402	330.942163	172.18.0.2	172.18.0.3	TCP	66 3308 + 43188 [ACK] Seq=99 Win=31872 Len=0 TSval=797482021 TScer=3228995865
89403	331.004664	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89404	331.004678	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137741778 Win=1437440 Len=0 TSval=501008165 TScer=140277512
89405	331.004680	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89406	331.004689	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=1377447538 Win=1437440 Len=0 TSval=501008550 TScer=140277512
89407	331.004693	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89408	331.004697	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137744659 Win=1437440 Len=0 TSval=501008162 TScer=1402775054
89409	331.004700	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89410	331.004730	172.18.0.3	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137761938 Win=1424384 Len=0 TSval=501008550 TScer=1402775132
89411	331.004743	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89412	331.004945	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137763378 Win=14402456 Len=0 TSval=501008648 TScer=1402775415
89413	331.023463	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89414	331.023464	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137764818 Win=1438884 Len=0 TSval=501008669 TScer=1402775549
89415	331.025784	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89416	331.025804	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137767698 Win=1437440 Len=0 TSval=501008671 TScer=1402775545
89417	331.044321	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89418	331.044322	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137767698 Win=1437440 Len=0 TSval=501008672 TScer=1402775546
89419	331.045943	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89420	331.045947	151.101.78.132	172.18.0.3	TCP	66 36794 + 80 [ACK] Seq=22804 Ack=137773458 Win=1437440 Len=0 TSval=501008705 TScer=1402775593

Em tìm được rất nhiều packet như trên và sử dụng chatgpt để chuyển đổi payload thành dạng dễ đọc hơn. Sau đó em ghép các kí tự lại với nhau thì được chuỗi "@dm1n\_3r37\_!@#~" nhưng bị thiếu kí tự thứ 7 và 9.

Lúc này em đi search lại string ‘password’ ở các packet injection đầu tiên xem có bõ sót gì không thì gặp packet 49482, packet này rất khác các packet trên, em xem thử các packet response thì packet 49495 trả về tabular

Packet list		Narrow & Wide	Case sensitive	String	password	
o.	#	Time	Source	Destination	Protocol	Length Info
-	49476	130.152375	172.18.0.3	151.101.78.132	TCP	66 36794 → 80 [ACK] Seq=15771 Ack=78084285 Win=1106816 Len=0 TSval=501507398 TSecr=1402674319
-	49477	130.159104	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
-	49478	130.159181	172.18.0.3	151.101.78.132	TCP	66 36794 → 80 [ACK] Seq=15771 Ack=78088165 Win=1106816 Len=0 TSval=501507404 TSecr=1402674326
-	49479	130.160284	172.18.0.1	172.18.0.3	TCP	74 50164 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1519599307 TSecr=0 WS=128
-	49488	130.160314	172.18.0.3	172.18.0.1	TCP	74 80 → 50164 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=308287148 TSecr=1519599308
-	49481	130.160343	172.18.0.1	172.18.0.3	TCP	66 50164 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1519599308 TSecr=308287148
-	49482	130.160465	172.18.0.1	172.18.0.3	HTTP	538 GET /news.php?name=%22%20union%20select%20username,password%20from%20users---+ HTTP/1.1
-	49483	130.160490	172.18.0.3	172.18.0.1	TCP	66 80 → 50164 [ACK] Seq=1 Ack=473 Win=31872 Len=0 TSval=308287148 TSecr=1519599308
-	49484	130.162207	172.18.0.3	172.18.0.2	TCP	74 57410 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3228894331 TSecr=0 WS=128
-	49485	130.162248	172.18.0.2	172.18.0.3	TCP	74 3306 → 57410 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=797381240 TSecr=3228894332
-	49486	130.162257	172.18.0.3	172.18.0.2	TCP	66 57410 → 3306 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3228894331 TSecr=797381240
-	49487	130.162775	172.18.0.2	172.18.0.3	MySQL	143 Server Greeting proto=10 version='8.3.0'
-	49488	130.162795	172.18.0.3	172.18.0.2	TCP	66 57410 → 3306 [ACK] Seq=1 Ack=78 Win=32128 Len=0 TSval=3228894332 TSecr=797381241
-	49489	130.162858	172.18.0.3	172.18.0.2	MySQL	206 Login Request user=root db=chall
-	49490	130.162867	172.18.0.2	172.18.0.3	TCP	66 3306 → 57410 [ACK] Seq=78 Ack=141 Win=31872 Len=0 TSval=797381241 TSecr=3228894332
-	49491	130.162941	172.18.0.2	172.18.0.3	MySQL	72 Caching_sha2_password fast_auth_success
-	49492	130.163129	172.18.0.2	172.18.0.3	MySQL	77 Response OK
-	49493	130.163137	172.18.0.3	172.18.0.2	TCP	66 57410 → 3306 [ACK] Seq=141 Ack=95 Win=32128 Len=0 TSval=3228894332 TSecr=797381241
-	49494	130.163525	172.18.0.3	172.18.0.2	MySQL	169 Request Query
-	49495	130.164202	172.18.0.2	172.18.0.3	MySQL	347 Response TABULAR Response
-	49496	130.164409	172.18.0.3	172.18.0.2	MySQL	71 Request Quit
-	49497	130.164422	172.18.0.3	172.18.0.2	TCP	66 57410 → 3306 [FIN, ACK] Seq=249 Ack=376 Win=31872 Len=0 TSval=3228894334 TSecr=797381242
-	49498	130.164437	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
-	49499	130.164446	172.18.0.2	172.18.0.3	TCP	66 3306 → 57410 [FIN, ACK] Seq=376 Ack=250 Win=31872 Len=0 TSval=797381243 TSecr=3228894334

Mở ra xem thử thì có toàn bộ username và password luôn

No.	Time	Source	Destination	Protocol	Length	Info	
49495	130.164202	172.18.0.2	172.18.0.3	MySQL	347	Response TABULAR Response	password
Length: 16000 Type: FIELD_TYPE_BLOB (252) Flags: 0x0010 Decimals: 0							
MySQL Protocol - intermediate EOF Packet Length: 5 Packet Number: 4 Response Code: EOF Packet (0xfe) EOF marker: 254 Warnings: 0 Server Status: 0x0022							
MySQL Protocol - row packet Packet Length: 23 Packet Number: 5 text text: Science news text text: 1 + 1 = 3							
MySQL Protocol - row packet Packet Length: 55 Packet Number: 6 text text: More science news text text: 88 + 22 is not equal to 100 ???:???:???:???							
MySQL Protocol - row packet Packet Length: 23 Packet Number: 7 text text: admin text text: @dm1n_s3cr37_!@#							
MySQL Protocol - row packet Packet Length: 24 Packet Number: 8 text text: agentp text text: perrytheplatypus							
MySQL Protocol - row packet Packet Length: 22 Packet Number: 9 text text: doofenshmirtz text text: noooooo							
MySQL Protocol - row packet Packet Length: 13 Packet Number: 10 text text: guest text text: 123456							
MySQL Protocol - response EOF Packet Length: 5 Packet Number: 11 Response Code: EOF Packet (0xfe) EOF marker: 254 Warnings: 0 Server Status: 0x0022							
Ready to load or capture							

Vậy hacker đã lấy được mật khẩu admin là "@dm1n\_s3cr37\_!@#"

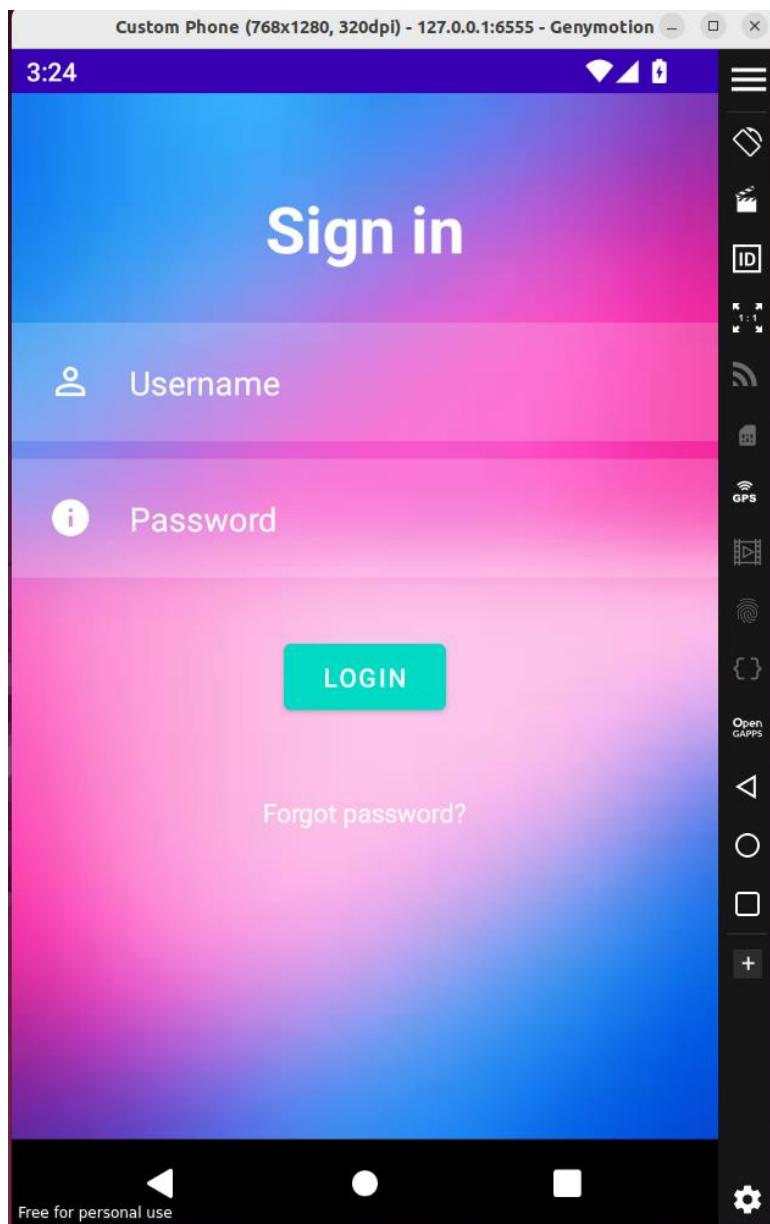
h. Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao?

Theo em thì hacker không phải Agent P, hacker không biết pass admin nên không phải là người get TABULAR ở packet 49495, nếu đã biết account thì không cần attack, thêm 1 tí bằng chứng ngoài lề là Agent P là đặc vụ giữ an toàn cho khu vực Tri-State Area nên khá chắc đặc vụ không làm việc này.

### 3. Android

Mở app thấy giao diện như này

Có vẻ yêu cầu ta Login thành công sẽ có flag



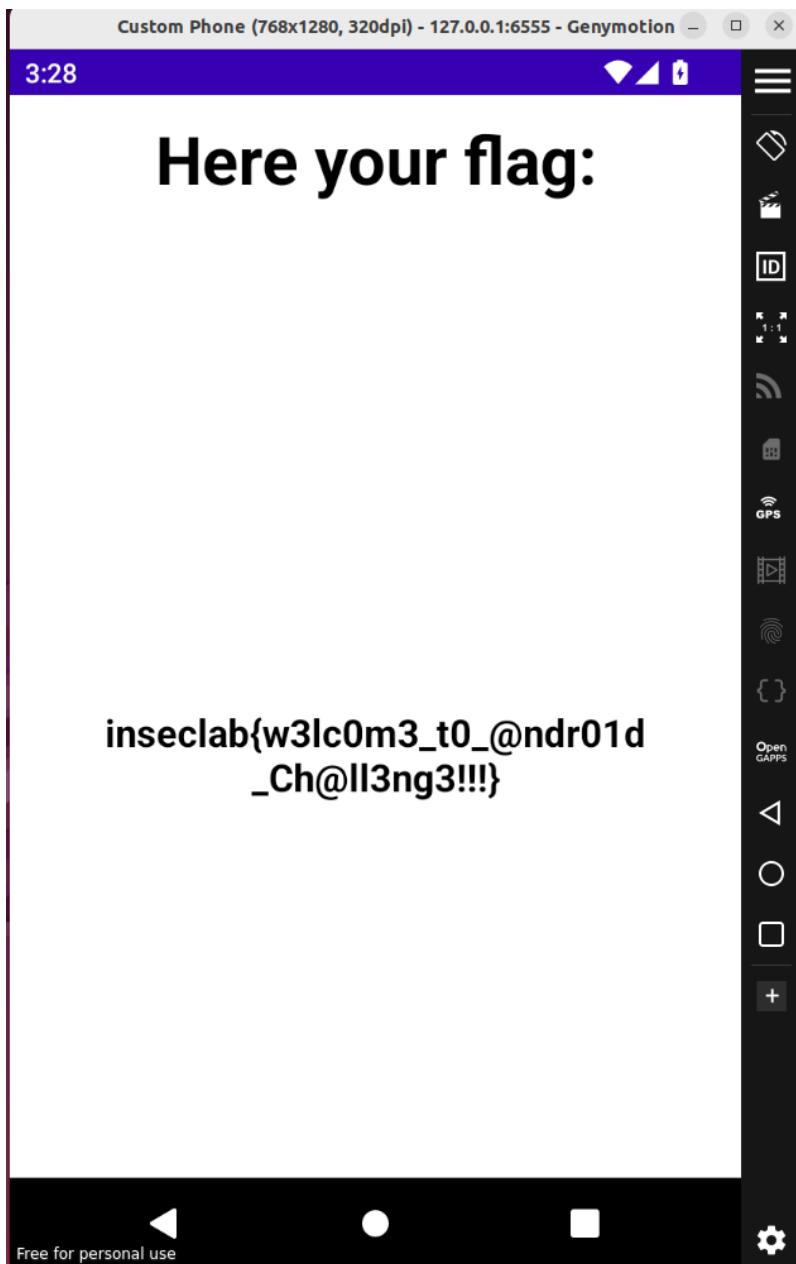
Dùng ByteCode-Viewer để đọc code.

Đọc và phân tích code hàm MainActivity

The screenshot shows the FernFlower Decomplier interface with the file 'com/example/trungquyenapp/MainActivity.class' open. The code is as follows:

```
1 package com.example.trungquyenapp;
2
3 import android.content.Intent;
4 import android.os.Bundle;
5 import android.view.View;
6 import android.widget.TextView;
7 import android.widget.Toast;
8 import androidx.appcompat.app.AppCompatActivity;
9 import com.google.android.material.button.MaterialButton;
10
11 public class MainActivity extends AppCompatActivity {
12     // $FF: synthetic method
13     public void lambda$onCreate$0(com_example_trungquyenapp_MainActivity var1, TextView var2, View var3) {
14         if (var1.getText().toString().equals("admin") && var2.getText().toString().equals("admin")) {
15             Toast.makeText(this, "LOGIN SUCCESSFUL", 0).show();
16             this.startActivity(new Intent(this, User.class));
17         } else {
18             Toast.makeText(this, "LOGIN FAILED !!!", 0).show();
19         }
20     }
21
22     protected void onCreate(Bundle var1) {
23         super.onCreate(var1);
24         this.setContentView(2131427356);
25         TextView var2 = (TextView)this.findViewById(2131231157);
26         TextView var3 = (TextView)this.findViewById(2131231021);
27         ((MaterialButton)this.findViewById(2131230938)).setOnClickListener(new .ExternalSyntheticLambda0(this, var2, var3));
28     }
29 }
30
31 }
```

Ta thấy username và password là admin thì login thành công.



Ta có được flag: inseclab{w3lc0m3\_t0\_@ndr01d\_Ch@ll3ng3!!!}

Đoạn mã bạn cung cấp chứa một số lỗi bảo mật nghiêm trọng liên quan đến việc xử lý thông tin đăng nhập và bảo vệ thông tin nhạy cảm. Dưới đây là phân tích về các lỗi và biện pháp khắc phục:

Lỗi bảo mật

1. Thông tin đăng nhập cứng (Hard-coded credentials):

- Thông tin đăng nhập `admin` được mã hóa cứng trong mã nguồn. Điều này có nghĩa là bất kỳ ai có quyền truy cập vào mã nguồn đều có thể dễ dàng nhìn thấy thông tin đăng nhập này.

```
if (var1.getText().toString().equals("admin") && var2.getText().toString().equals("admin")) {
```

2. So sánh chuỗi không an toàn:

## Session 01: Memory Forensics

- So sánh chuỗi sử dụng phương thức `equals` mà không có biện pháp bảo vệ trước các tấn công thời gian (timing attacks).
- Điều này có thể bị lợi dụng để đoán mật khẩu dựa trên thời gian phản hồi của ứng dụng.

### Biện pháp khắc phục

#### 1. Loại bỏ thông tin đăng nhập cứng:

- Không bao giờ lưu trữ thông tin đăng nhập hoặc thông tin nhạy cảm trực tiếp trong mã nguồn. Thay vào đó, sử dụng cơ sở dữ liệu hoặc các dịch vụ xác thực bên ngoài.

- Sử dụng các phương pháp xác thực an toàn như OAuth, JWT, hoặc các phương pháp xác thực hai yếu tố (2FA).

#### 2. Sử dụng các hàm băm và mã hóa an toàn:

- Mật khẩu nên được lưu trữ dưới dạng băm (hash) với một salt ngẫu nhiên và sử dụng các thuật toán băm mạnh như bcrypt, Argon2, hoặc PBKDF2.

- Khi người dùng đăng nhập, so sánh mật khẩu đã băm của họ với mật khẩu đã băm được lưu trữ.

#### 3. Sử dụng biện pháp bảo vệ trước các tấn công thời gian:

- Sử dụng các thư viện bảo mật đã được kiểm chứng để so sánh các chuỗi an toàn, như thư viện `MessageDigest` hoặc `SecretKeySpec` trong Java.

### Đề xuất mã sửa đổi

Dưới đây là một ví dụ về cách cải thiện đoạn mã đăng nhập:

```

public class MainActivity extends AppCompatActivity {

    private UserService userService; // Giả định có một lớp dịch vụ người dùng để xử lý xác thực

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main); // Sử dụng tên tài nguyên rõ ràng
        TextView usernameTextView = findViewById(R.id.username);
        TextView passwordTextView = findViewById(R.id.password);
        MaterialButton loginButton = findViewById(R.id.login_button);

        userService = new UserService(); // Khởi tạo dịch vụ người dùng

        loginButton.setOnClickListener(view -> {
            String username = usernameTextView.getText().toString();
            String password = passwordTextView.getText().toString();
            handleLogin(username, password);
        });
    }

    private void handleLogin(String username, String password) {
        boolean loginSuccess = userService.authenticate(username, password);
        if (loginSuccess) {
            Toast.makeText(this, "LOGIN SUCCESSFUL", Toast.LENGTH_SHORT).show();
            startActivity(new Intent(this, UserActivity.class));
        } else {
            Toast.makeText(this, "LOGIN FAILED !!!", Toast.LENGTH_SHORT).show();
        }
    }
}

```

### Tóm tắt

- Loại bỏ thông tin đăng nhập cứng khỏi mã nguồn.
- Sử dụng cơ sở dữ liệu để lưu trữ thông tin người dùng và mật khẩu đã băm.
- Sử dụng các thư viện băm mạnh và so sánh chuỗi an toàn.
- Triển khai các biện pháp bảo mật như xác thực hai yếu tố (2FA) để tăng cường bảo mật.

### 4. Steganography

---

**Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này**

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [NT101.H11.1]-Session1\_Group3.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](http://courses.uit.edu.vn).

**Đánh giá:** Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**