

Hands-on Tasks (due by 6 feb 5:35pm)

(A) Malware Behavior Analysis

For this we use a tool Qu1cksc0pe: <https://github.com/CYB3RMX/Qu1cksc0pe>

```
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop] $ git clone https://github.com/CYB3RMX/Qu1cksc0pe
Cloning into 'Qu1cksc0pe' ...
remote: Enumerating objects: 4122, done.
remote: Counting objects: 100% (199/199), done.
remote: Compressing objects: 100% (106/106), done.
remote: Total 4122 (delta 122), reused 116 (delta 93), pack-reused 3923 (from 3)
Receiving objects: 100% (4122/4122), 109.87 MiB | 672.00 KiB/s, done.
Resolving deltas: 100% (2671/2671), done.
```

After installation we will setup this

```
kali:kali: ~/Desktop/Qu1cksc0pe
File Actions Edit View Help
Certificate added: C=US, S=Arizona, L=Scottsdale, O="Starfield Technologies, Inc.", CN=Starfield Root Certificate Authority - G2
Certificate added: C=US, S=Arizona, L=Scottsdale, O="Starfield Technologies, Inc.", CN=Starfield Services Root Certificate Authority - G2
Certificate added: C=CH, O=SwissSign AG, CN=SwissSign Gold CA - G2
Certificate added: C=CH, O=SwissSign AG, CN=SwissSign Silver CA - G2
Certificate added: C=PL, O=Krajowa Izba Rozliczeniowa S.A., CN=SZAFIR ROOT CA2
Certificate added: C=FI, O=Telia Finland Oyj, CN=Telia Root CA v2
Certificate added: O=TeliaSonera, CN=TeliaSonera Root CA v1
Certificate added: C=CN, O="TrustAsia Technologies, Inc.", CN=TrustAsia Global Root CA G3
Certificate added: C=CN, O="TrustAsia Technologies, Inc.", CN=TrustAsia Global Root CA G4
Certificate added: C=US, S=Illinois, L=Chicago, O="Trustwave Holdings, Inc.", CN=Trustwave Global Certification Authority
Certificate added: C=US, S=Illinois, L=Chicago, O="Trustwave Holdings, Inc.", CN=Trustwave Global ECC P256 Certification Authority
Certificate added: C=US, S=Illinois, L=Chicago, O="Trustwave Holdings, Inc.", CN=Trustwave Global ECC P384 Certification Authority
Certificate added: C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2
Certificate added: C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 3
Certificate added: C=TR, L=Gezbe - Kocaeli, O=Turktelekom Arastirma Kurumu - TUBITAK, OU=Kamu Sertifikasyon Merkezi - Kamu SM, CN=TUBITAK Kamu SM SSL Kok Se
rtifikasi - Surum 1
Certificate added: C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA
Certificate added: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Global Root CA
Certificate added: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Root Certification Authority
Certificate added: C=CN, O=UniTrust, CN=UCA Extended Validation Root
Certificate added: C=CN, O=UniTrust, CN=UCA Global G2 Root
Certificate added: C=US, S>New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority
Certificate added: C=US, S>New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
Certificate added: C=CN, O="iTrustChina Co.,Ltd.", CN=vTrust ECC Root CA
Certificate added: C=CN, O="iTrustChina Co.,Ltd.", CN=vTrust Root CA
Certificate added: C=US, O=www.xrampprofessional.com, O=XRamp Security Services Inc, CN=XRamp Global Certification Authority
Certificate added: C=ES, O=Firmaprofesional SA, OID.2.5.4.97-VATES-A62634068, CN=FIRMAPROFESIONAL CA ROOT-A WEB
Certificate added: C=JP, O="Cybertrust Japan Co., Ltd.", CN=SecureSign Root CA12
Certificate added: C=JP, O="Cybertrust Japan Co., Ltd.", CN=SecureSign Root CA14
Certificate added: C=JP, O="Cybertrust Japan Co., Ltd.", CN=SecureSign Root CA15
Certificate added: C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security TLS ECC Root 2020
Certificate added: C=DE, O=Deutsche Telekom Security GmbH, CN=Telekom Security TLS RSA Root 2023
Certificate added: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA CYBER Root CA
152 new root certificates were added to your trust store.
Import process completed.
Done
done.
Setting up mono-devel (6.12.0.199+dfsg-2.1) ...
update-alternatives: using /usr/bin/mono-csc to provide /usr/bin/cli-csc (c-sharp-compiler) in auto mode
update-alternatives: using /usr/bin/resgen to provide /usr/bin/cli-resgen (resource-file-generator) in auto mode
update-alternatives: using /usr/bin/al to provide /usr/bin/cli-al (assembly-linker) in auto mode
update-alternatives: using /usr/bin/sn to provide /usr/bin/cli-sn (strong-name-tool) in auto mode
Setting up mono-complete (6.12.0.199+dfsg-2.1) ...
Processing triggers for ca-certificates-java (20240118) ...
done.

[*] All done.
Friends Group 2
https://github.com/0xT3m0n/QuickScanner
(kali㉿kali)-[~/Desktop/Qu1cksc0pe]
$
```

After the setup we first

```
$ python quickscope.py --db_update  
use this command to setup database
```

After database initialization we scan the malware

```
└$ python quickscope.py --file ..\malware\wann.exe --hashscan
```

Checking for database state ...
Database State: Up to date.

```
>>> Total Hashes: 336595  
>>> File Name: .. /malware/wann.exe  
>>> Target Hash: 84c82835a5d21bbc75a61706d8ab549
```

Hash	Name
84c82835a5d21bbc75a61706d8ab549	Uds.Dangerousobject.Multi!c

Here ..//malware/warn.exe is the file location
And –hashscan is the tool which we are using

After scanning we conclude that one file is malicious which we can see in the image

For Identification of virus type we perform following steps
– > initialize api which we will get in the VirusTotal.com website

```
$ python qu1cksc0pe.py --key_init

    < This tool is very dangerous. Be careful >
    < while using it !! >
    < Mr. Virus >

[*] Enter your VirusTotal API key:
1e7895d4
[+] Your VirusTotal API key saved.
```

python quickscope.py --file .. /malware/see7. exe --sigcheck!

Using this command we can check which kind of file this is
this will give all the information about this file

python quickscope.py --file .. /malware/see7. exe --hashscan

Using this command we can scan whole file
this will give all the information about all the malicious files in this file

python quickscope.py --file .. /malware/see7. exe --analyze
This command analyzes the whole file

\$ python quicksc0pe.py --file ..//malware/infect.xls --doc
this command scans the whole document and analyzes that