School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

1

# CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

## WEEK 6.2

## CODE SIGNING

Last Updated: 9/10/2021

2

# Code Signing

# Install HashTab



- HashTab provides OS extensions to calculate file hashes and supports many hash algorithms such as MD5, SHA1, SHA2, RipeMD, HAVAL and Whirlpool.
- Visit
  - http://implbits.com/products/hashtab/
- Click on download now
- Download and install

# Software Download & Hash Check



- Go to the below link and download the testing file "advancedrun.zip"
  - https://www.nirsoft.net/hash_check/?software=advancedrun
- Take note the file's MD5 Hash and SHA1 Hash values.

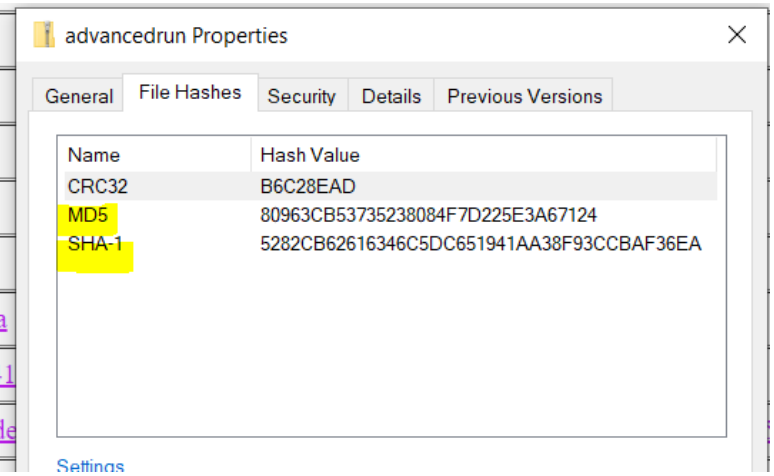
| | |
|---|---|
| Filename | advancedrun.zip |
| Download URL | https://www.nirsoft.net/utils/advancedrun.zip |
| File Size | 62624 Bytes |
| Update Time | August 03 2020 13:43:07 |
| MD5 Hash | 80963cb53735238084f7d225e3a67124 |
| SHA1 Hash | 5282cb62616346c5dc651941aa38f93ccbaf36ea |
| SHA256 Hash | e931c57f86248727c382c69f038eac4f419d2f141 |
| SHA512 Hash | d18e80e05ae0f15e63314daa43f21e4195202f5de |

# Software Download & Hash Check



- Right click on the downloaded file and select “Properties”
- Click on “File Hashes” tab in the “Properties” window
  - Copy and paste the MD5 Hash Value below
    - **????**
  - Compare the above value with the “MD5Hash” value that was sent to you via email by the HashTab website.
    - **Do they match: yes/no?**

| | |
|---|---|
| Filename | advancedrun.zip |
| Download URL | https://www.nirsoft.net/utils/advancedrun.zip |
| File Size | 62624 Bytes |
| Update Time | August 03 2020 13:43:07 |
| MD5 Hash | 80963cb53735238084f7d225e3a67124 |
| SHA1 Hash | 5282cb62616346c5dc651941aa38f93ccbaf36ea |
| SHA256 Hash | e931c57f86248727c382c69f038eac4f419d2f141 |
| SHA512 Hash | d18e80e05ae0f15e63314daa43f21e4195202f5de |



# HashTab



- What conclusions could you infer?
  - Do you think the file/software was indeed from the right source? Justify in your own words.
    - ????
  - Do you think the file/software was altered after it was published? Justify in your own words.
    - ????
  - Are you 100% sure that the file/software is from the right source and it was not altered? What could go wrong?
    - ????

# Code Signing



- Visit:
  - URL: https://msdn.microsoft.com/en-us/library/ms537361%28v=vs.85%29.aspx
- Watch:
  - https://www.youtube.com/watch?t=98&v=lr4tgiiDhBs
- Write a short summary to explain what code signing is and its purposes?
  - ????

# HashTab – Digital Signature

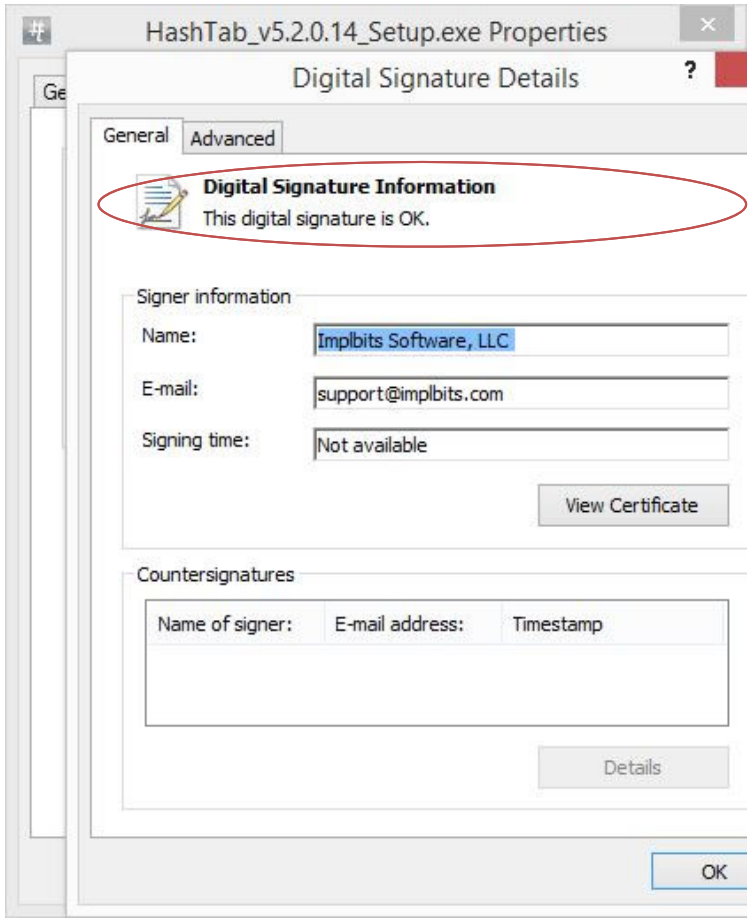


- Right click on the file “HashTab_v6.0.0.34_Setup.exe”
  - Click on “Digital Signatures” tab?
  - Select the “Name of Signer” in the “Signature List”
  - Click on “Details”

# HashTab – Signature Check



- First Check:
  - "This digital signature is OK"

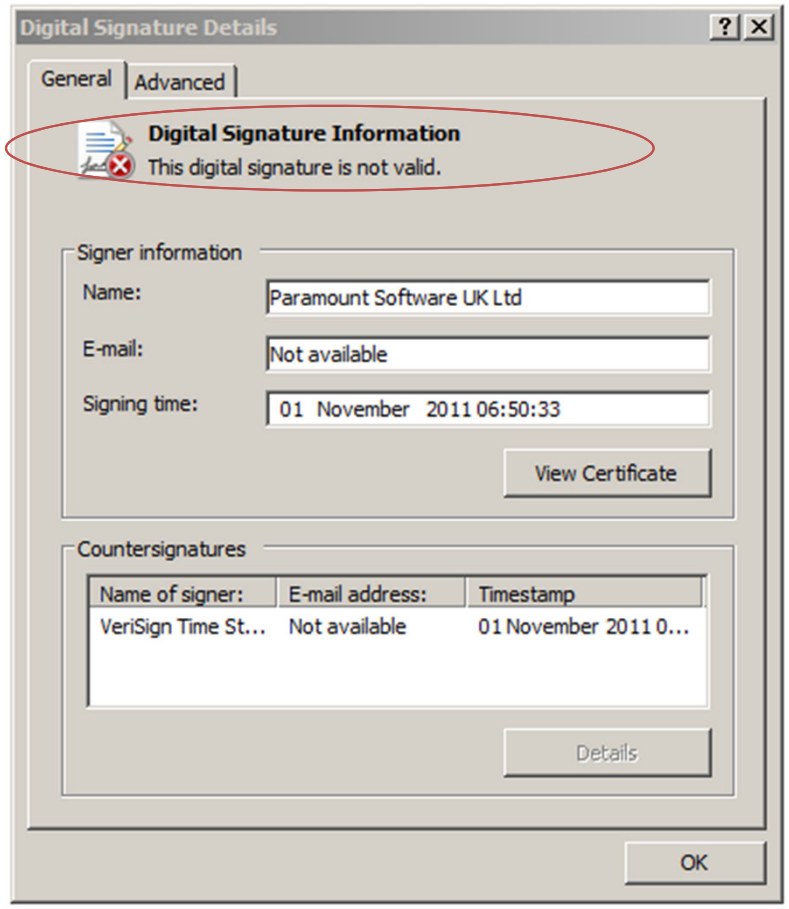


# Example: Signature Check Fail



- If the code is corrupted
  - The signature check will fail

Source: http://kb.macrium.com/KnowledgebaseArticle50213.aspx



# HashTab – View Certificate



- Now click on “View Certificate”
  - What are the two intended purposes of the certificate
    - ????
    - ????
  - Fill in the following details
    - Issued to
      - ????
    - Issued by
      - ????
    - Validty
      - From: ???
      - To: ????

# HashTab – View Certificate - Details



- Fill in the following details
  - Signature Algorithm
    - ????
  - Signature Hash Algorithm
    - ????
  - Size of the RSA Public Key
    - ???? Bits
    - First 6 bytes of the public key
      - ????

# HashTab – View Certificate - Details



- Fill in the following details
  - Thumbprint algorithm
    - ????
  - First 6 bytes of the thumbprint
    - ????
- What is thumbprint?
  - the hash of the entire certificate
- Click on “Copy to File” and save the certificate on the desktop as “hashtab.cer”
  - Right click on “hashtab.cer” and check its SHA1 hash value
  - Does it match the thumbprint?
    - Yes/No?

# HashTab – View Certificate – Certification Path



- Click on “Certification Path”
  - Who is the Root Certificate Authority (CA)
    - ????
  - Who is the Intermediate CA
    - ????

# HashTab – View Certificate – Certification Path



- In order to verify the code sign of HashTab the operating system (Win8.1) must also verify the signatures of both the Intermediate CA and the Root CA
- Type: “certmgr.msc” into the Win8.1 search and double click on the icon
- Explore all the folders inside “certmgr.msc”
  - In which two folders would you find the certificates of Root CA and Intermediate CA?
    - ????
    - ????

# Answer the following - 1



- Assume we are considering the following software and its publisher
  - Software: Flash player.exe
  - Publisher: Adobe
- Explain with a diagram, how the executable code/file is signed by the software publisher

# Answer the following - 2



- Explain how to “ensure software came from software publisher” can be achieved through the use of the certificate embedded in the executable file sent to you?

# Answer the following - 3



- Explain how the certificate can “protect software from alteration after publication”?

# Summary

Week 6.2

# You learnt about



- Code Signing
- Why code signing?
- Understanding details of Digital Certificate
- Certification Path
- Root Certificates