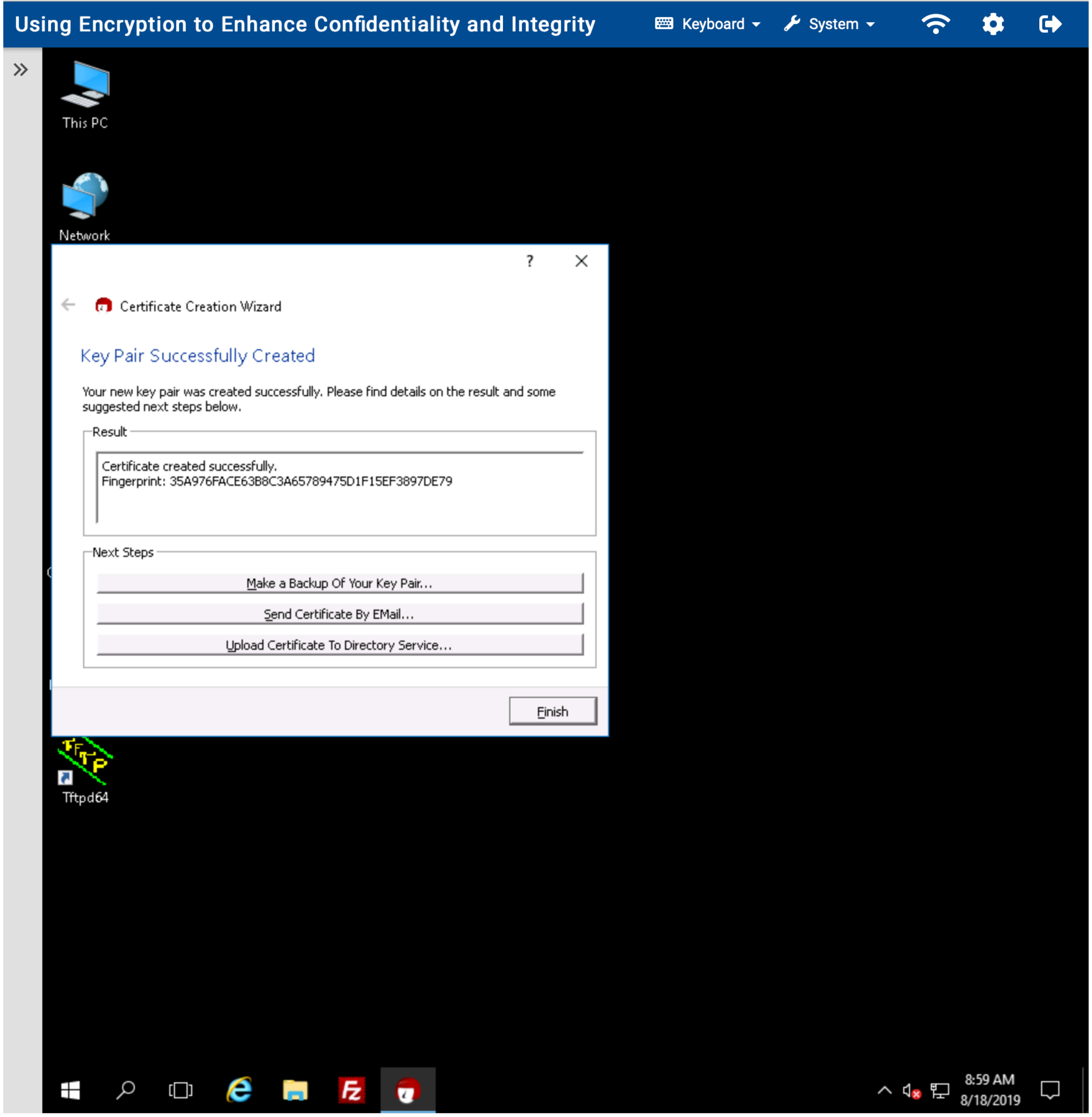
Lab #2: Using Encryption to Enhance Confidentiality and Integrity
Tool: GPG4Win—Kleopatra

Part 1: Create a Public and Private Key Pair for the Sender

Step #11


Using Encryption to Enhance Confidentiality and Integrity
Keyboard
System
This PC
Network
Certificate Creation Wizard
Make a Backup Of Your Key Pair...
Send Certificate By EMail...
Upload Certificate To Directory Service...
Finish
Tftpd64
8:59 AM
8/18/2019

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

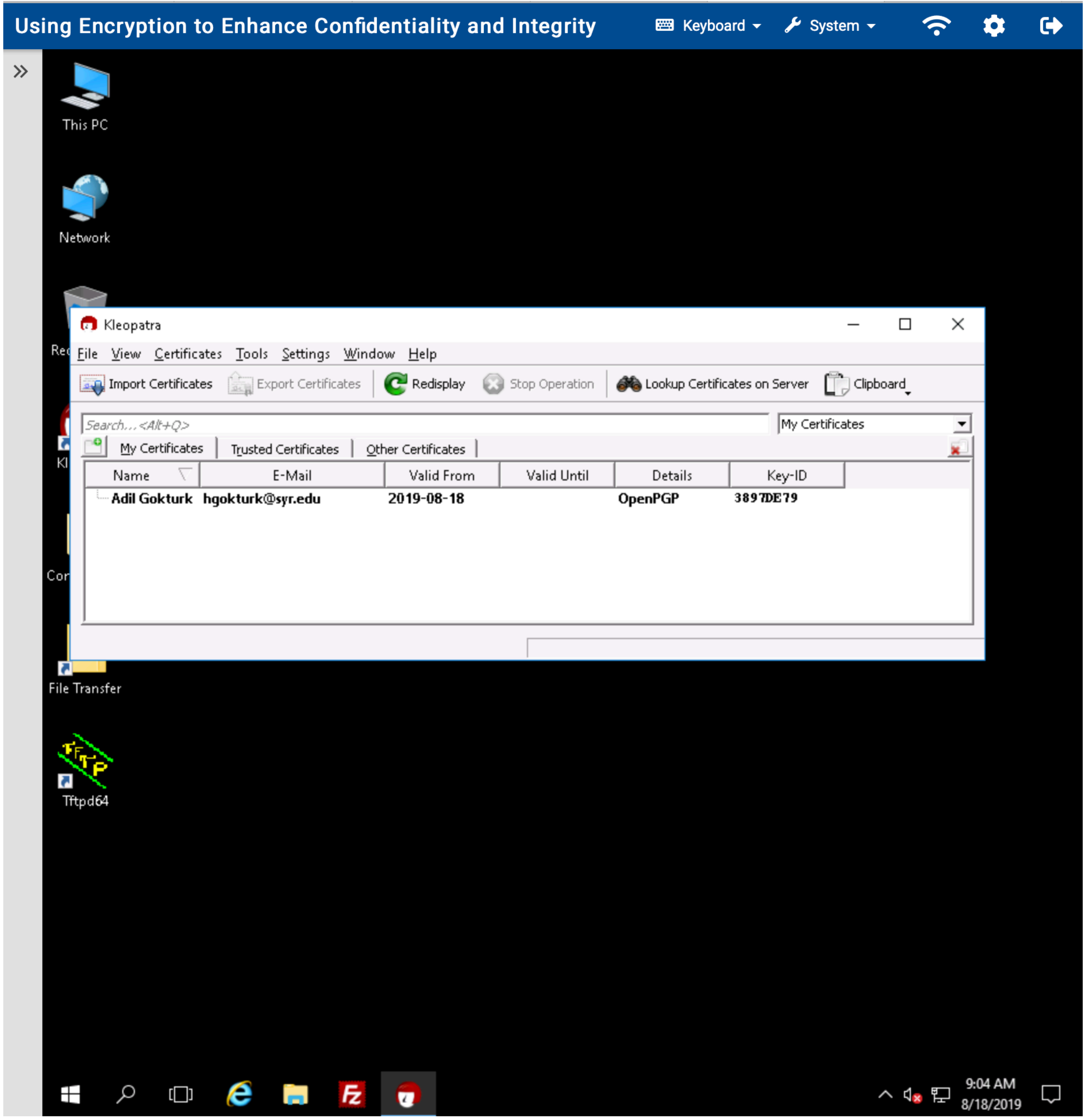
Result

Certificate created successfully.
Fingerprint: 35A976FACE63B8C3A65789475D1F15EF3897DE79

Next Steps

Part 1: Create a Public and Private Key Pair for the Sender

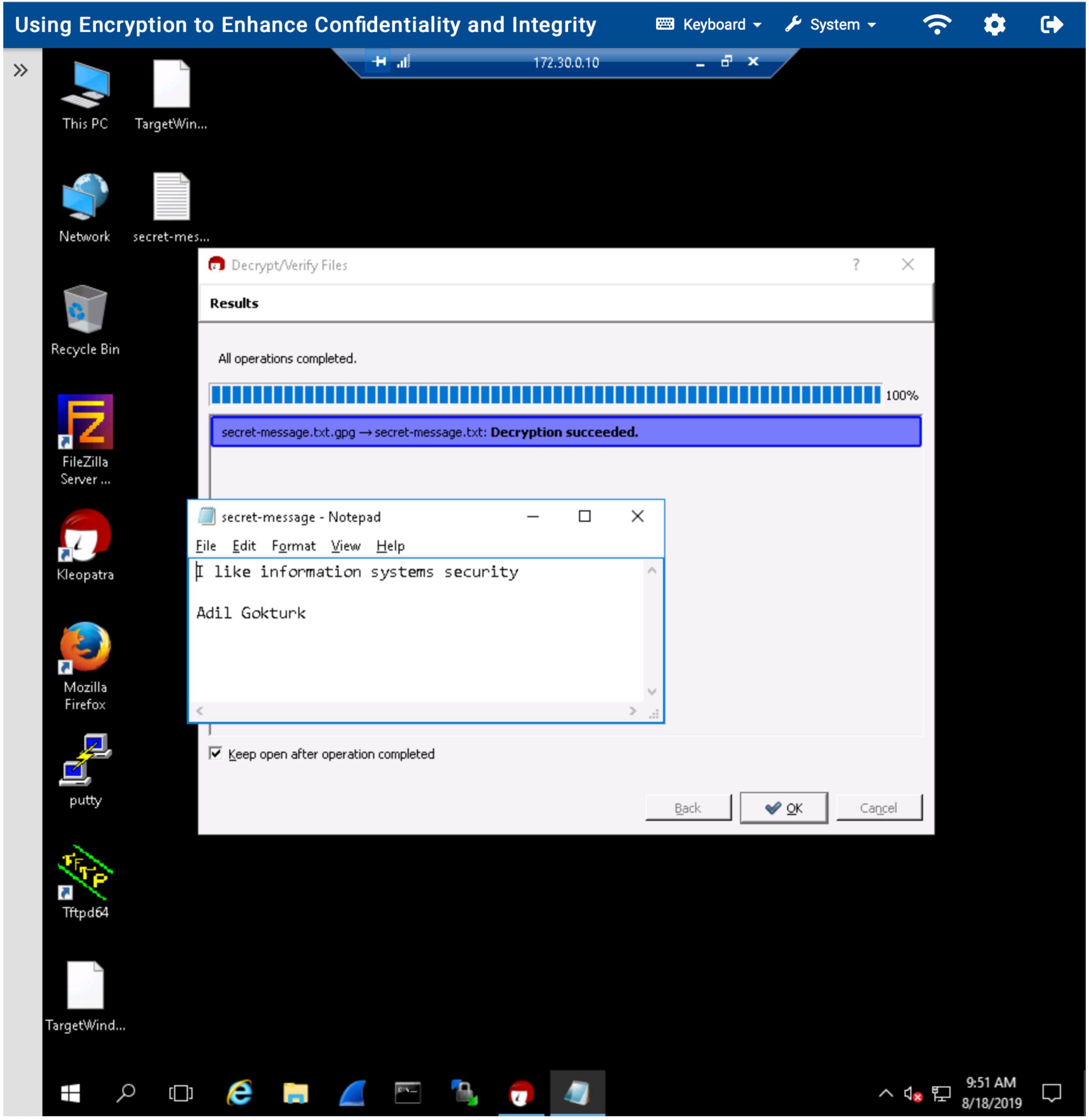
Step #17



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Adil Gokturk	hgokturk@syr.edu	2019-08-18		OpenPGP	3897DE79

Part 4: Encrypt and Decrypt a File from the Sender

Step #22



All operations completed.

secret-message.txt.gpg → secret-message.txt: **Decryption succeeded.**

```
I like information systems security

Adil Gokturk
```

☑ Keep open after operation completed

Part 5: Challenge Question

What is the difference and tradeoffs between X.509 and PGP certificate types? (Discuss them in 200 words.)

OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every individual creates a personal web of Trust by certifying other users' key pairs with their own certificate.

X.509 key pairs are also created locally, but certified centrally by a certification authority—CA. CAs can certify other CAs, creating a central, hierarchical chain of trust. X.509 is actually a format standard for public key.

The CA will send the verifier a digital certificate. Digital certificates follow the X.509 syntax. A digital certificate contains a number of fields. Most importantly, the digital certificate contains the name of the true party in the Subject field and the true party's public key. The verifier looks up the digital certificate of the true party, and then uses this public key in the digital certificate to test the digital signature of the supplicant.

The trade off between OpenPGP and X.509 is level of security. For instance, If you trust X, and if X trusts Y, then you may trust Y. This is dangerous because if misplaced trust is present anywhere in the system, bogus public key/name pairs may circulate widely. PGP has had most success in person-to-person communication without corporate control, where X.509 preferred mostly in enterprises. OpenPGP is a simple, cost efficient and relatively less safe and faster than X.509. The complex verification protocol of X.509 makes it the safest way of encryption application.