Reconsideration of public key fingerprints

Suga Yuji

Internet Initiative Japan

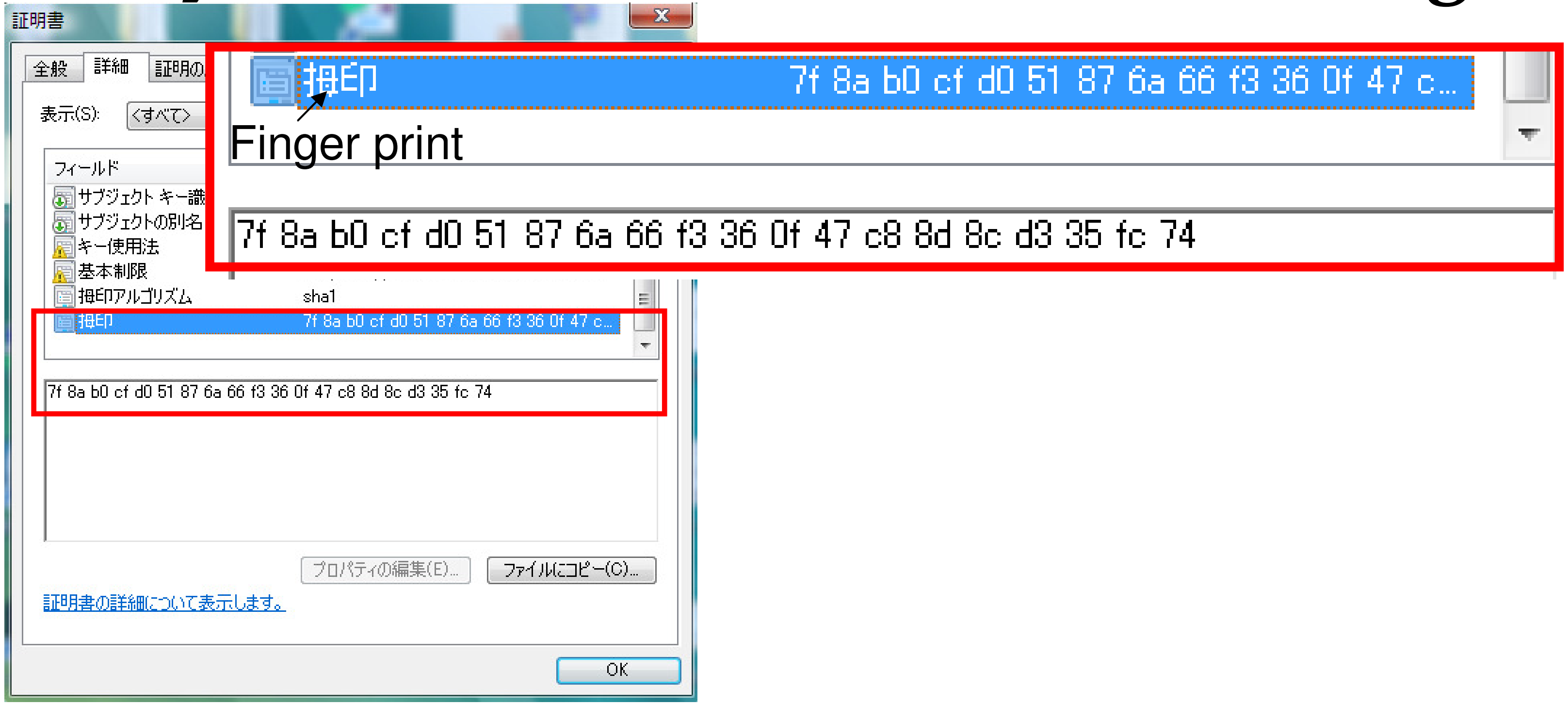
Fingerprint of an X.509 PKC

- A short sequence of bytes used to authenticate a public key.

- Created by applying a cryptographic hash function to a public key.
  - Commonly used today are based on (MD5 or) SHA-1.

Fingerprint of X.509 PKC

- **Install an X.509 self-signed certificate with <u>human inspection</u>.**
- **Usually encoded into hexadecimal strings.**



サブジェクト キー識
サブジェクトの別名
キー使用法
基本制限
拇印アルゴリズム sha1
拇印 7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c...

7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c8 8d 8c d3 35 fc 74

Human inspection

- Get a fingerprint via non-Internet channel.
  - Such as newspaper, official gazette.

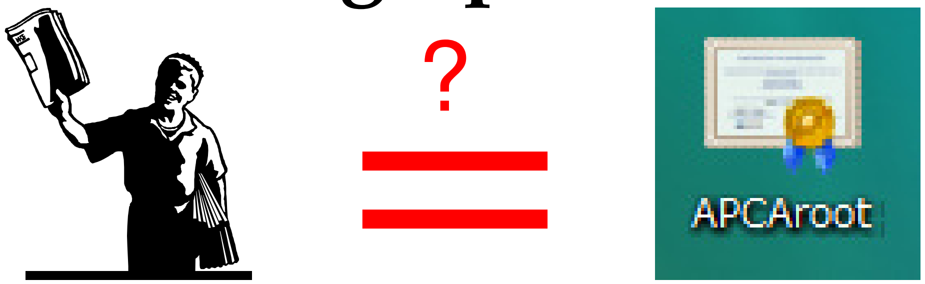
Human inspection

- Get a fingerprint via non-Internet channel.
  - Such as newspaper, official gazette.

- Download an X.509 cert via the Internet.
  - Usually self-signed CA certificate.

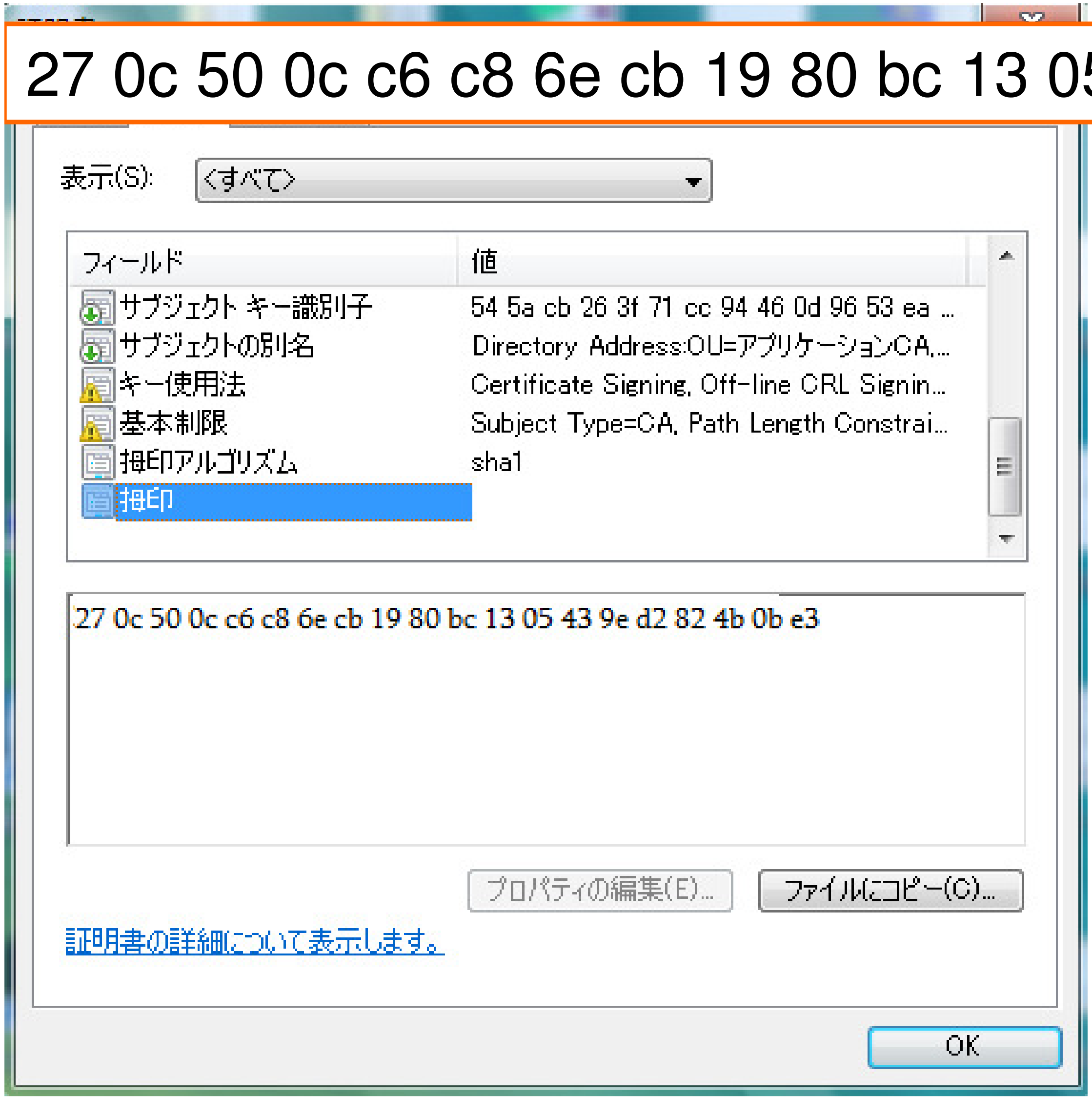
Human inspection

- Get a fingerprint via non-Internet channel.
  - Such as newspaper, official gazette.
- Download an X.509 cert via the Internet.
  - Usually self-signed CA certificate.
- Check these fingerprints.



Let’s try !!

27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3



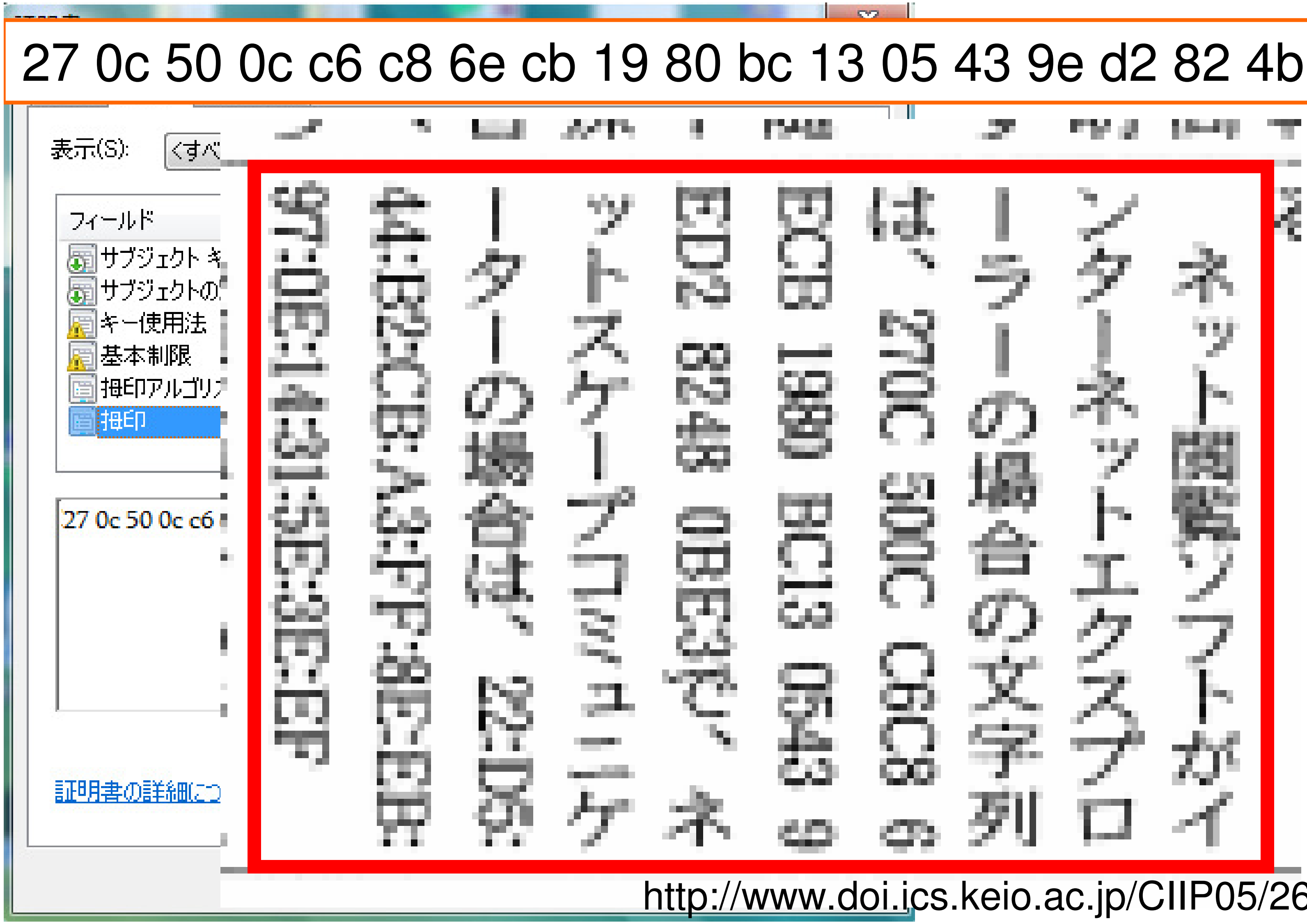
表示(S): <すべて>

フィールド	値
サブジェクト キー識別子	54 5a cb 26 3f 71 cc 94 46 0d 96 53 ea ...
サブジェクトの別名	Directory Address:OU=アプリケーションCA,...
キー使用法	Certificate Signing, Off-line CRL Signin...
基本制限	Subject Type=CA, Path Length Constrai...
拇印アルゴリズム	sha1
拇印	

27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3

Let’s try !!

27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3



27 0c 50 0c c6

ネット関係ソフトがインターネットエクスプローラーの場合の文字列は、270C 500C C6C8 6ECB 1980 BC13 0543 9ED2 824B 0BE3で、ネットスケープコミュニケーターの場合は、22:D8:44:B2:CB:A3:FF:3E:EB:97:0E:14:31:5E:3E:EF

http://www.doi.ics.keio.ac.jp/CIIP05/26/12-Takagi.pdf

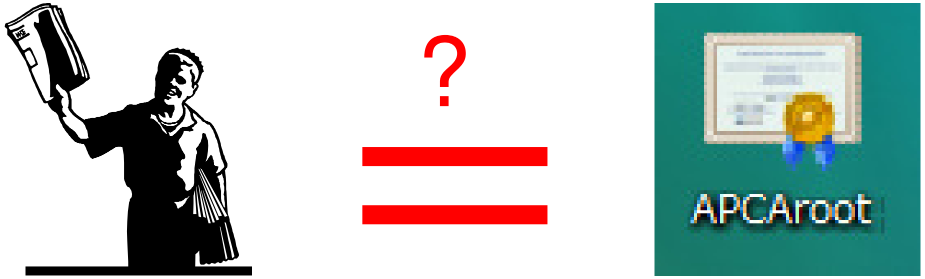
What’s wrong ?

- It is difficult for us to check it :
  - Case-sensitive problem
  - Different from separation of blocks
  - (Vertically problem)

- Trigger human errors…

Human inspection

- Get a fingerprint via non-Internet channel.
  - Such as newspaper, official gazette.
- Download an X.509 cert via the Internet.
  - Usually self-signed CA certificate.
- Check these fingerprints.



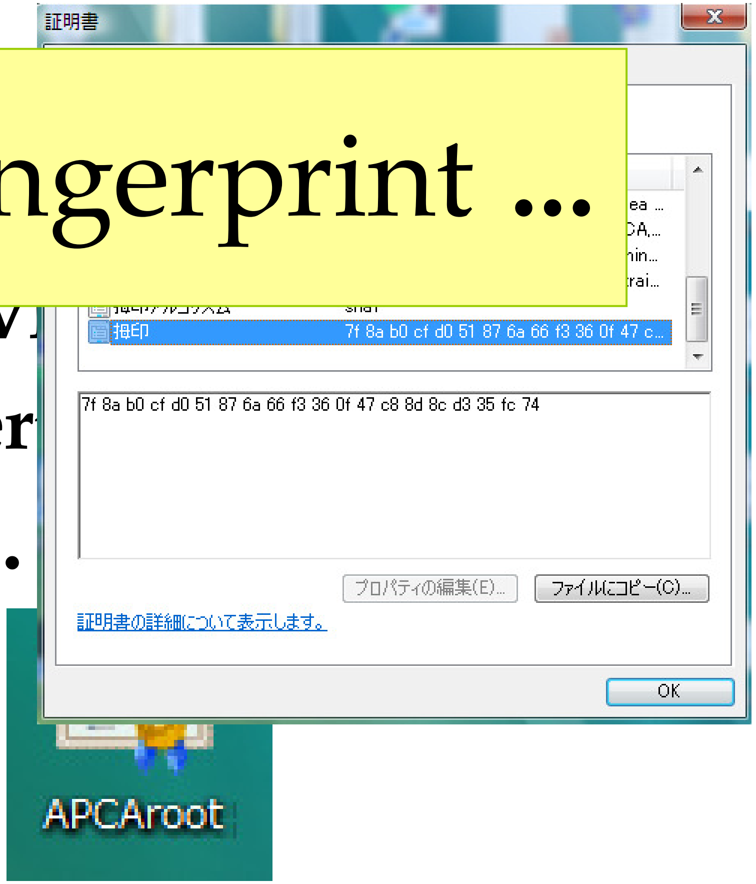
Human inspection

- G
  -
- Download an X.509 cert v
  - Usually self-signed CA cer
- Check these fingerprints.

Only display a fingerprint ...

?

=



	ea ...
	CA,...
	hin...
	rai...
拇印アルゴリズム	sha1
拇印	7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c...

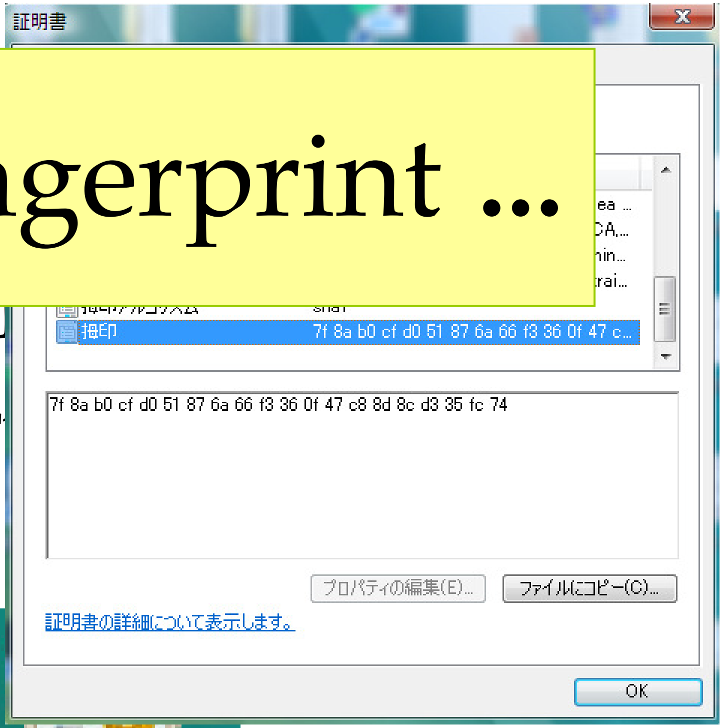
7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c8 8d 8c d3 35 fc 74

We can do interaction Human ~~inspection~~

- G
  -

Only display a fingerprint ...

- Download an X.509 cert vi
  - Usually self-signed CA cer
- Check these fingerprints.



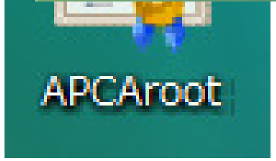
証明書

拇印アルゴリズム sha1

拇印 7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c...

7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c8 8d 8c d3 35 fc 74

$\overset{?}{=}$

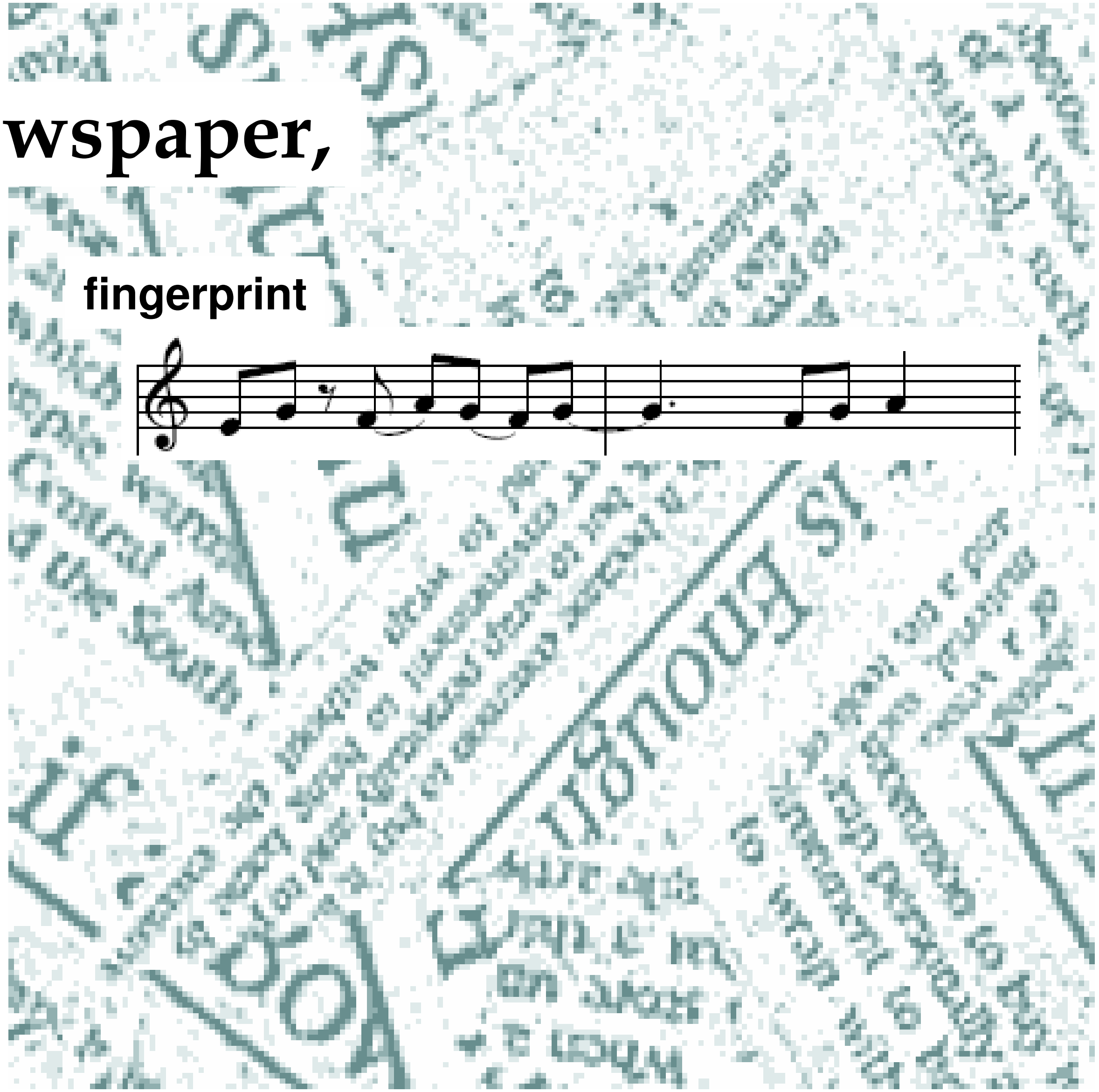


My proposal is simple

- **Users can do something**
  - **Passive mode**
    - **Basically check something.**
    - **Not only (boring) hex strings.**
  - **Active mode**
    - **Interactive to PCs.**

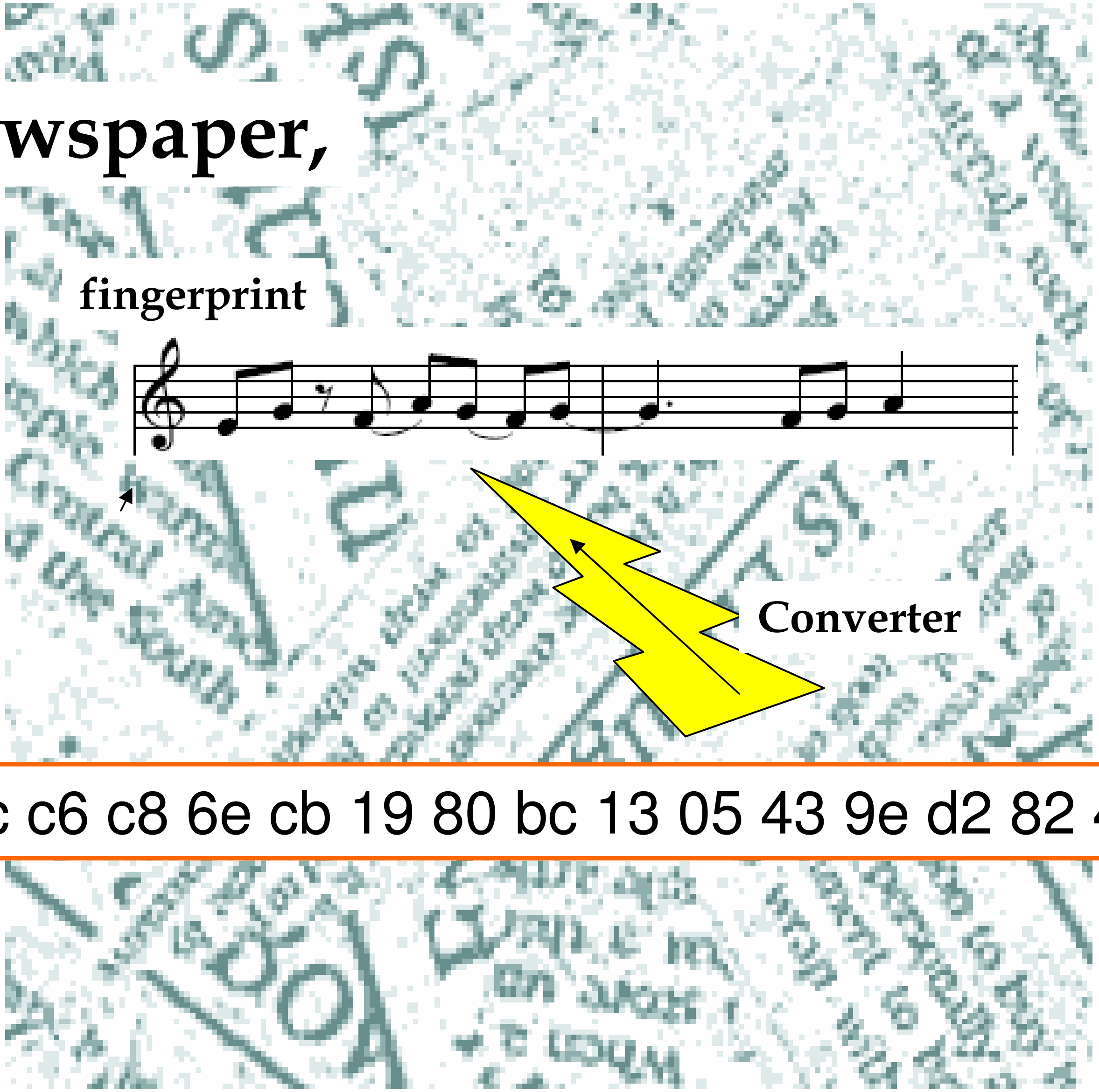
Example: Music scores

- **In a newspaper,**



Example: Music scores

- **In a newspaper,**



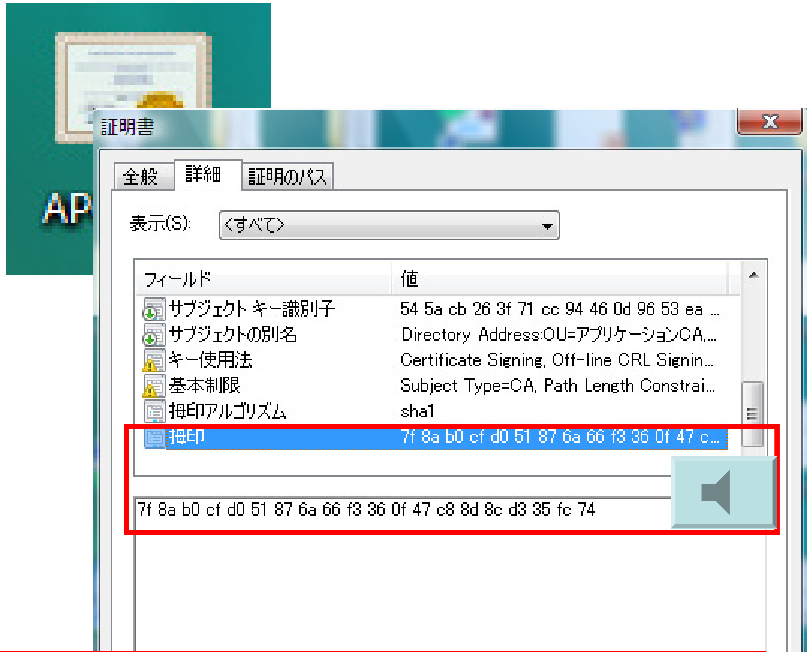
27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3

APCAroot

Example: Music scores

- Check these fingerprints.

≟

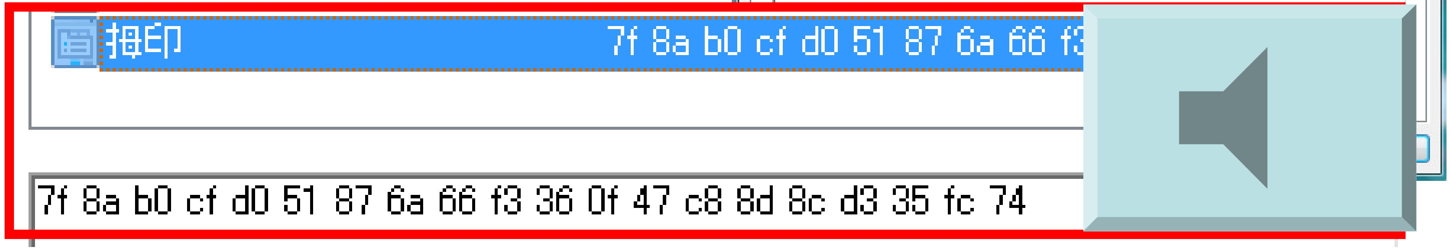


証明書

表示(S): <すべて>

フィールド	値
サブジェクト キー識別子	54 5a cb 26 3f 71 cc 94 46 0d 96 53 ea ...
サブジェクトの別名	Directory Address:OU=アプリケーションCA,...
キー使用法	Certificate Signing, Off-line CRL Signin...
基本制限	Subject Type=CA, Path Length Constrai...
拇印アルゴリズム	sha1
拇印	7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c...

7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c8 8d 8c d3 35 fc 74



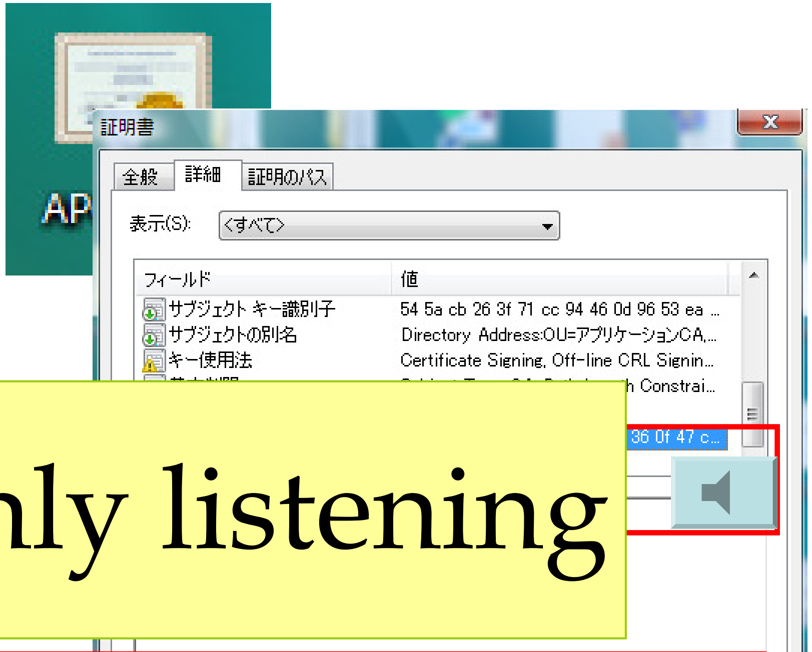
拇印 7f 8a b0 cf d0 51 87 6a 66 f3

7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c8 8d 8c d3 35 fc 74

Example: Music scores

- **Check these fingerprints.**

=?

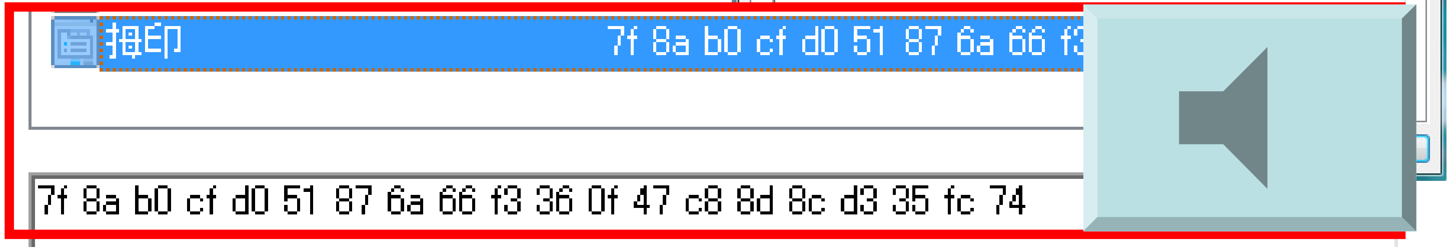


証明書

表示(S): <すべて>

フィールド	値
サブジェクト キー識別子	54 5a cb 26 3f 71 cc 94 46 0d 96 53 ea ...
サブジェクトの別名	Directory Address:OU=アプリケーションCA,...
キー使用法	Certificate Signing, Off-line CRL Signin...

Passive mode: Only listening

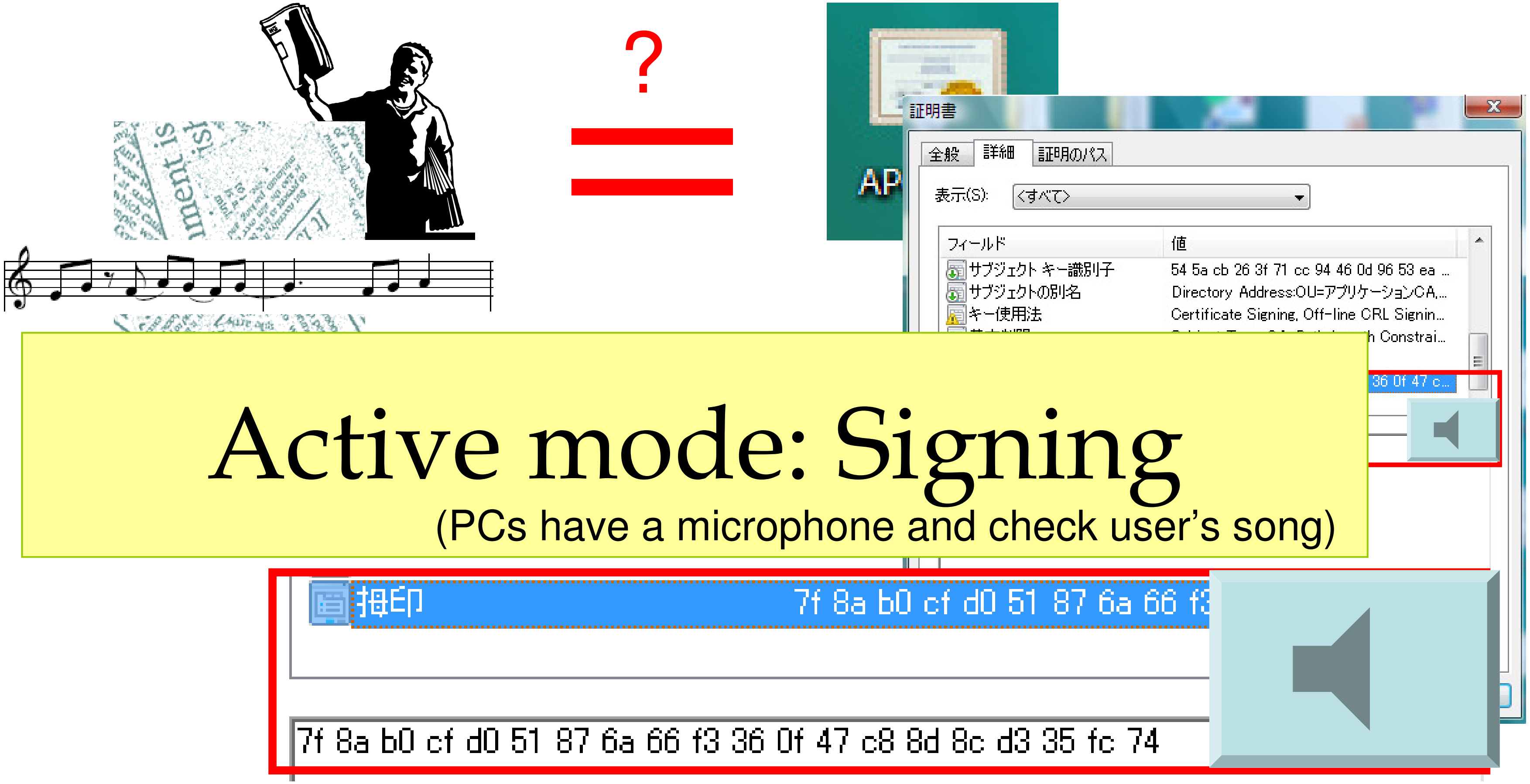


拇印 7f 8a b0 cf d0 51 87 6a 66 f3

7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c8 8d 8c d3 35 fc 74

Example: Music scores

- **Check these fingerprints.**



証明書

全般 詳細 証明のパス

表示(S): <すべて>

フィールド	値
サブジェクト キー識別子	54 5a cb 26 3f 71 cc 94 46 0d 96 53 ea ...
サブジェクトの別名	Directory Address:OU=アプリケーションCA,...
キー使用法	Certificate Signing, Off-line CRL Signin...
	...h Constrai...
拇印	7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c...

```
7f 8a b0 cf d0 51 87 6a 66 f3 36 0f 47 c8 8d 8c d3 35 fc 74
```

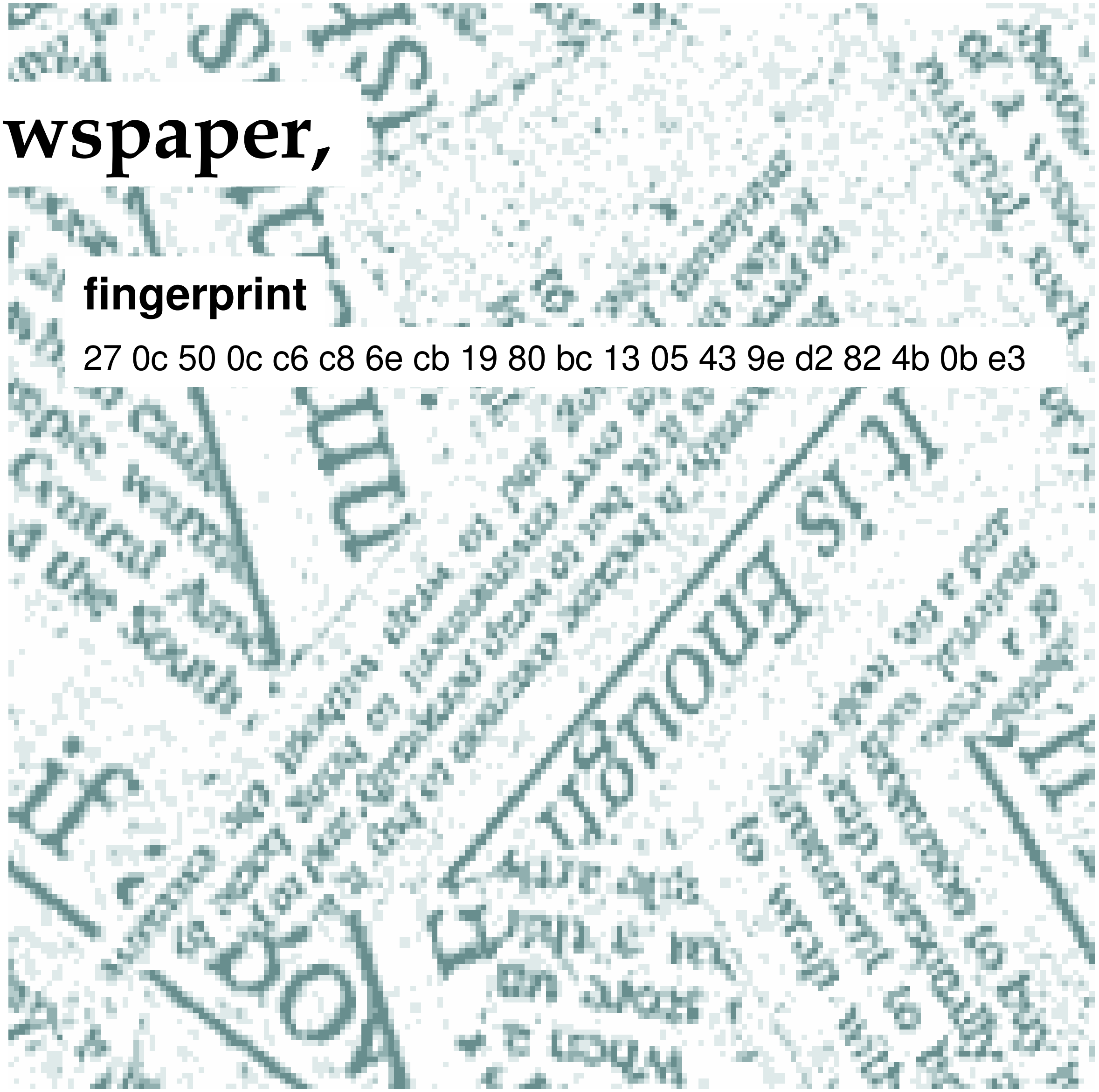
Active mode: Signing

(PCs have a microphone and check user's song)

Is it more complicated ?

Simple example: Input fingerprint

- **In a newspaper,**

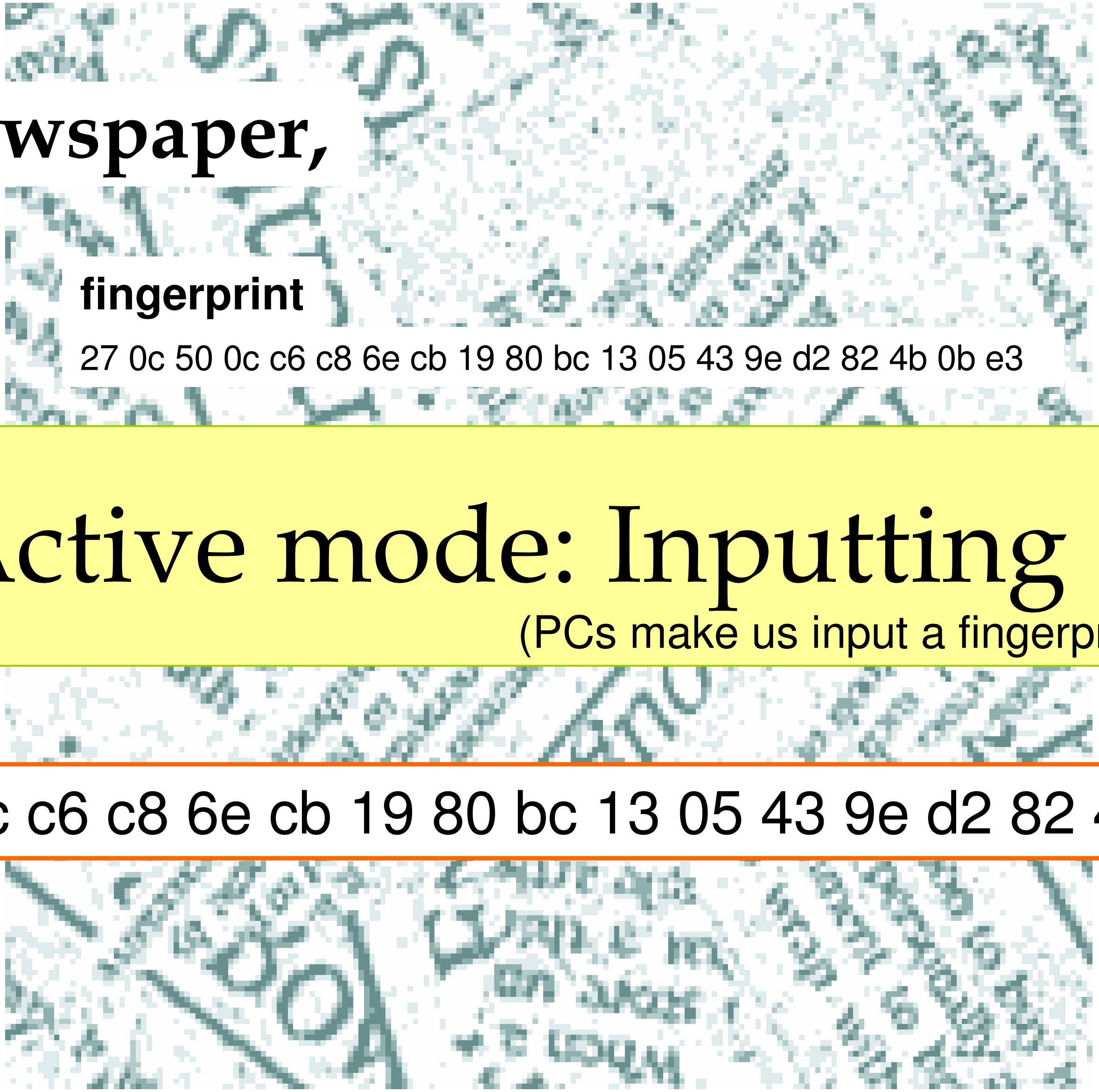


fingerprint

27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3

Simple example: Input fingerprint

- In a newspaper,



fingerprint

27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3

Active mode: Inputting

(PCs make us input a fingerprint)

27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3

APCAroot

Is it a boring task ?

We need something incentive

Active mode: Inputting

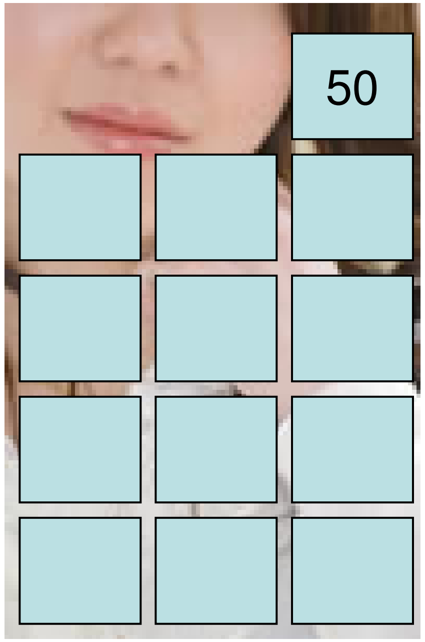
(PCs make us input a fingerprint)

27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3

We need something incentive

Active mode: Inputting

(PCs make us input a fingerprint)



27 0c 50 0c c6 c8 6e cb 19 80 bc 13 05 43 9e d2 82 4b 0b e3