Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Defeating the Secrets of OTP Apps

M.A., M.Sc. Philip Polleit, Friedrich-Alexander-Universität, Erlangen
Dr.-Ing., Michael Spreitzenbarth, Friedrich-Alexander-Universität, Erlangen

philip@polleit.de

// Agenda

- Introduction
- Forensic Use
- Background
- Research
- Results
- Conclusion

// Introduction

- **Information age** requires secure authentication

// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)

// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected

// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
- April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)

// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
- April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)
- July 2017: BKA reports database with 500 million „stolen“ e-mail addresses (incl. passwords)

// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
- April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)
- July 2017: BKA reports database with 500 million „stolen“ e-mail addresses (incl. passwords)
- May 2018: **Twitter** prompts users to change their passwords (as they saved these **unencrypted**).

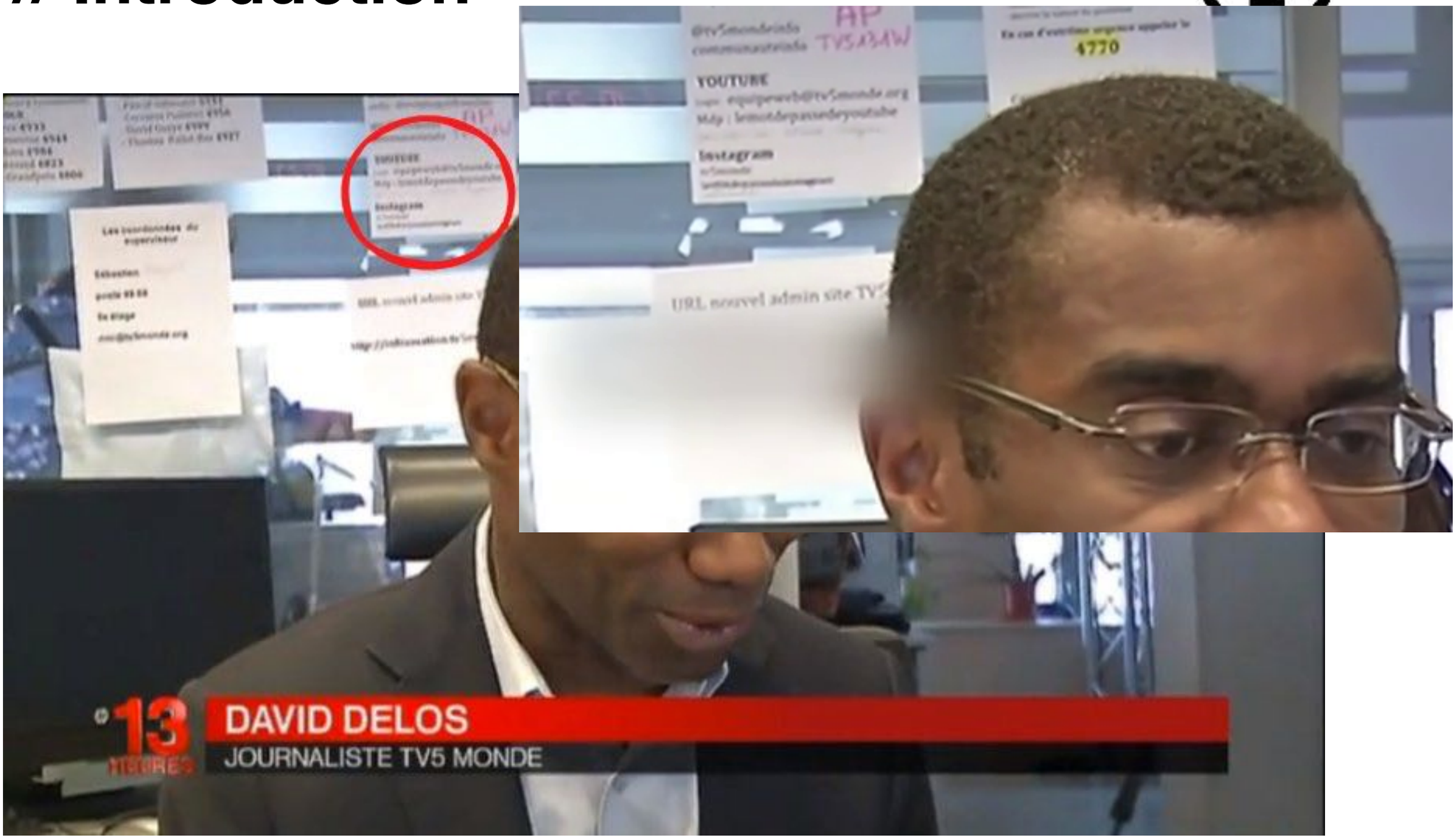
// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
- April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)
- July 2017: BKA reports database with 500 million „stolen“ e-mail addresses (incl. passwords)
- May 2018: **Twitter** prompts users to change their passwords (as they saved these **unencrypted**).
- —> Weak PW (user) / **unsalted** Hashes (provider)

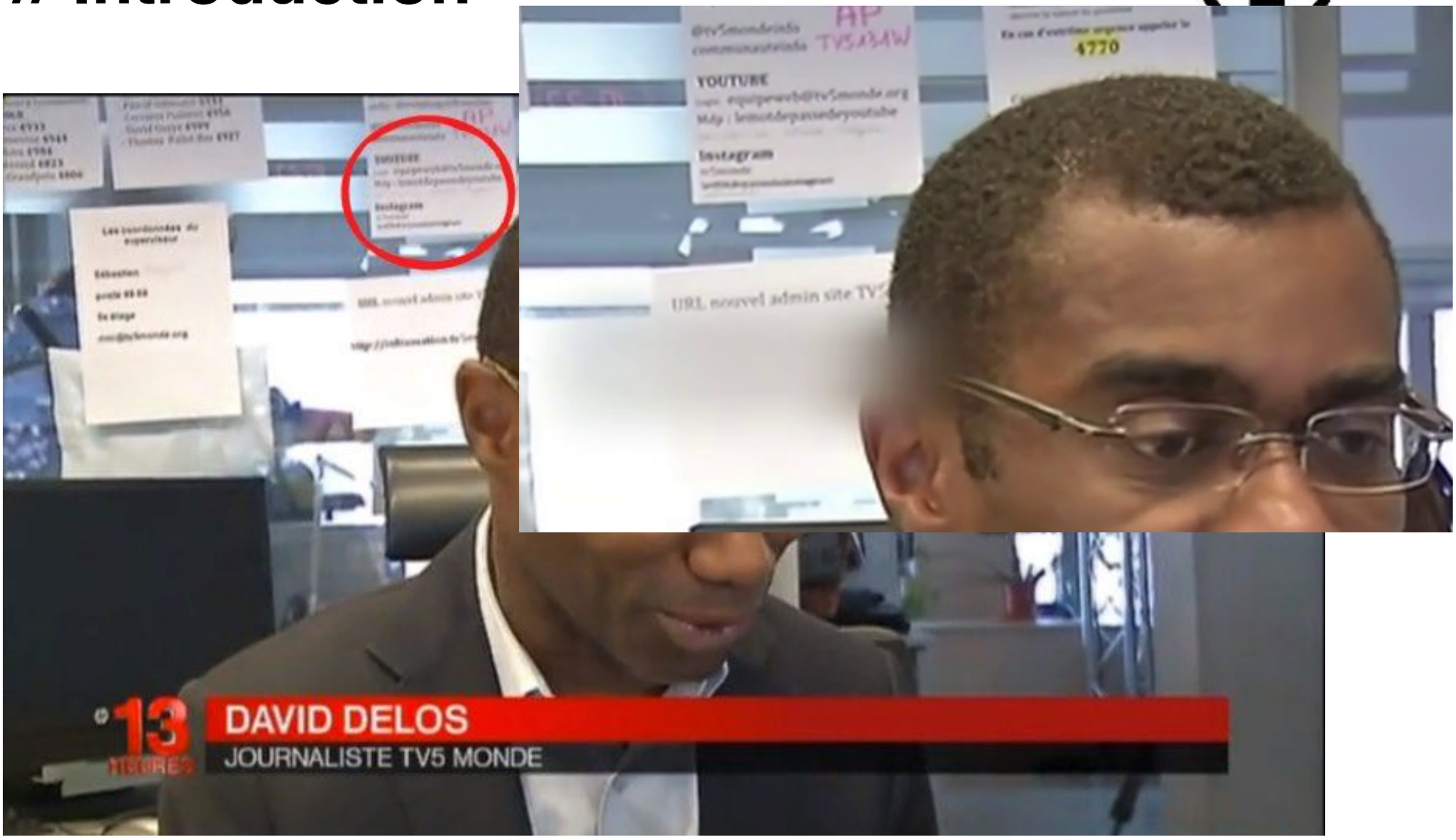
// Introduction

// Introduction

// Introduction



// Introduction



„lemotdepassedeyoutube“

// Introduction

// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented

// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories

// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories
    - **"Knowledge"** (passwords, user names, PINs)
    - **"Being"** (e.g. fingerprint, biometric features)
    - **"Possession"** (hardware token, credit card, key)

// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories
    - **"Knowledge"** (passwords, user names, PINs)
    - **"Being"** (e.g. fingerprint, biometric features)
    - **"Possession"** (hardware token, credit card, key)
- Classic implementation is **SecurID** token from „RSA“

// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories
    - **"Knowledge"** (passwords, user names, PINs)
    - **"Being"** (e.g. fingerprint, biometric features)
    - **"Possession"** (hardware token, credit card, key)
- Classic implementation is **SecurID** token from „RSA“
- **"Tokenless"** MFA is implemented by software

// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories
    - **"Knowledge"** (passwords, user names, PINs)
    - **"Being"** (e.g. fingerprint, biometric features)
    - **"Possession"** (hardware token, credit card, key)
- Classic implementation is **SecurID** token from „RSA“
- **"Tokenless"** MFA is implemented by software
- Popular forms are so-called **2FA** apps für smartphones that generate **OTPs** ("one-time password“)

// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories

vords, user names, PINs)
rint, biometric features)
vare token, credit card, key)

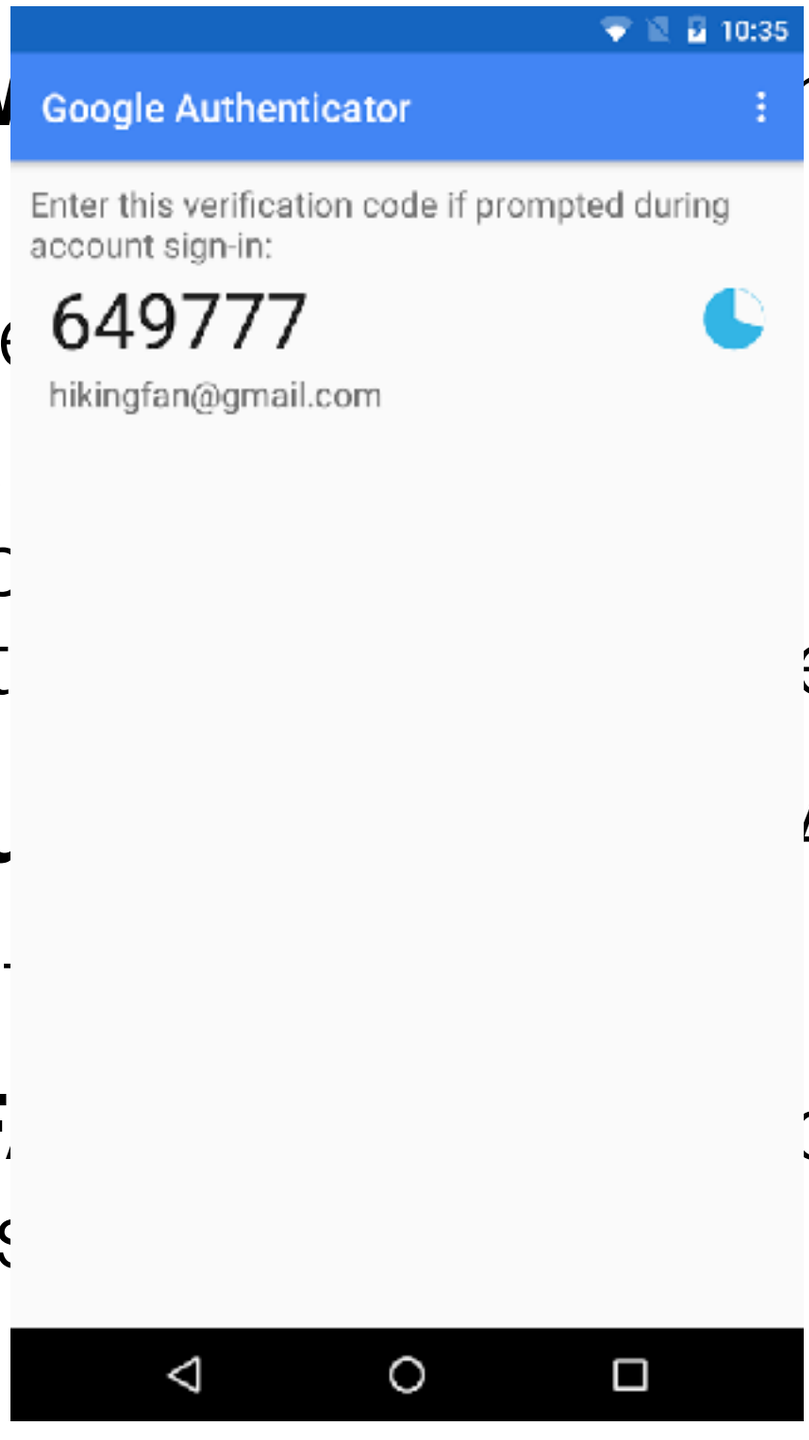
- Cl **SecurID** token from „RSA“
- **"Tokenless"** MFA is implemented by software
- Popular forms are so-called **2FA** apps für smartphones that generate **OTPs** ("one-time password“)

// Introduction

- **Multi-factor Authentication (M** ns to overcome the risks presented
- Factors can be divided into thre

vords
rint, b
ware t
ey)

- Cl **Secu** A“
- **"Tokenless"** MFA is implemen
- Popular forms are so-called **2F** ones that generate **OTPs** ("one-time pass



// Forensic Use

// Forensic Use

- Central question of any criminal procedure is „**Causality**“

// Forensic Use

- Central question of any criminal procedure is „**Causality**“
- Computer forensic consideration proofs whether the

// Forensic Use

- Central question of any criminal procedure is „**Causality**“
- Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an **instrument of crime**

// Forensic Use

- Central question of any criminal procedure is „**Causality**“
- Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an **instrument of crime**
- Consideration literally **stops** at the „**keyboard**“

// Forensic Use

- Central question of any criminal procedure is „**Causality**“
- Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an **instrument of crime**
- Consideration literally **stops** at the „**keyboard**“
- 2FA app examination puts the **user** (perpetrator) into **focus**

// Forensic Use

- Central question of any criminal procedure is „**Causality**“
- Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an **instrument of crime**
- Consideration literally **stops** at the „**keyboard**“
- 2FA app examination puts the **user** (perpetrator) into **focus**
- Otherwise defense strategy could be: „**it wasn’t me**“

// Forensic Use

- Central question of any criminal procedure is „**Causality**“
- Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an **instrument of crime**
- Consideration literally **stops** at the „**keyboard**“
- 2FA app examination puts the **user** (perpetrator) into **focus**
- Otherwise defense strategy could be: „**it wasn’t me**“
- However analyzing authentication process closes the **gap**

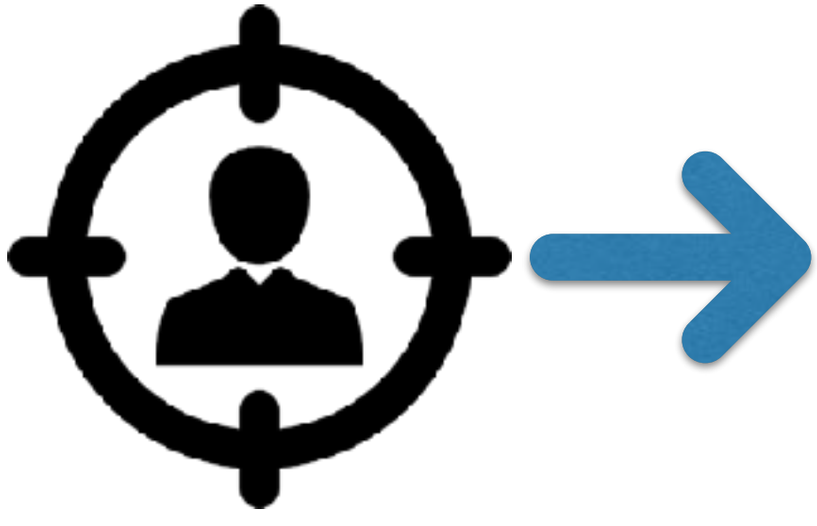
// Forensic Use

- Central question of any criminal procedure is „**Causality**“
- Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an **instrument of crime**
- Consideration literally **stops** at the „**keyboard**“
- 2FA app examination puts the **user** (perpetrator) into **focus**
- Otherwise defense strategy could be: „**it wasn’t me**“
- However analyzing authentication process closes the **gap**
- **Chain of evidence** could be closed

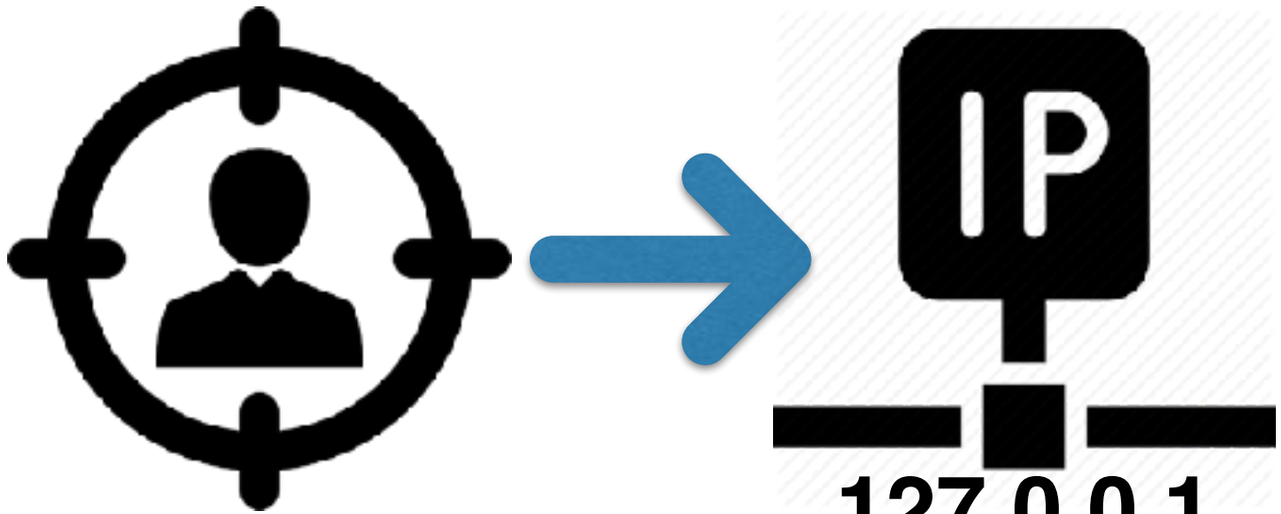
// Forensic Use

// Forensic Use

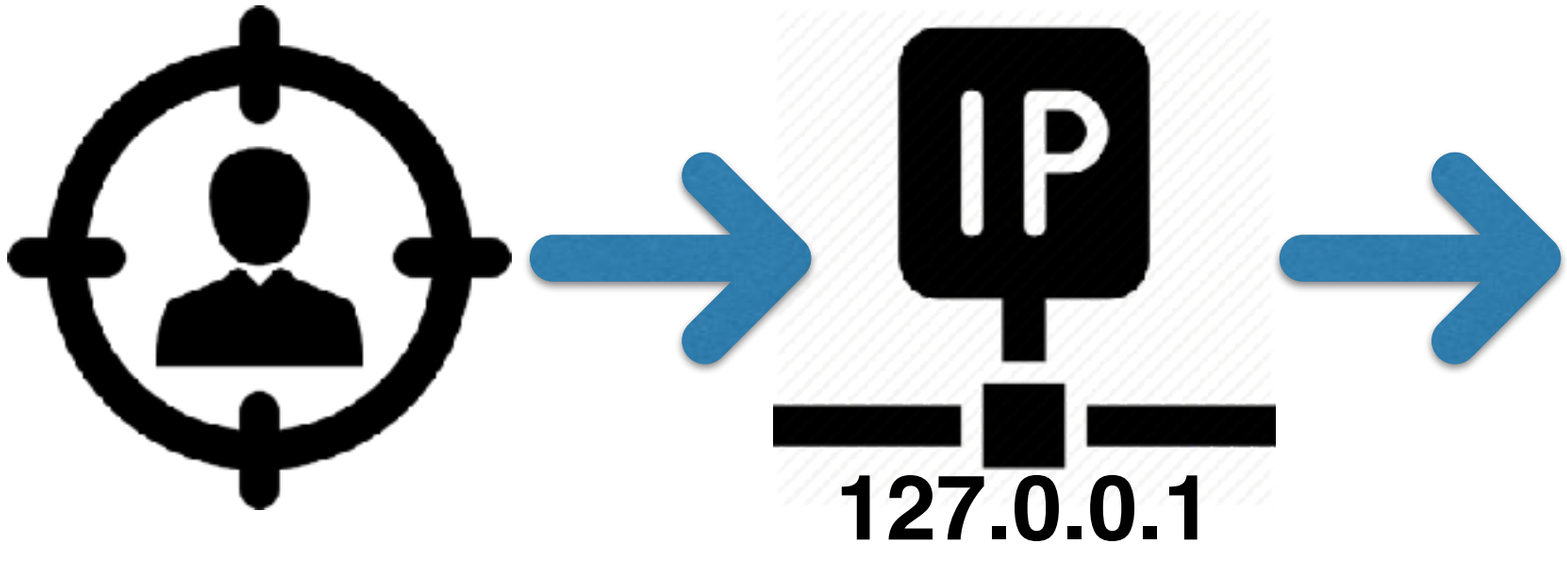
// Forensic Use



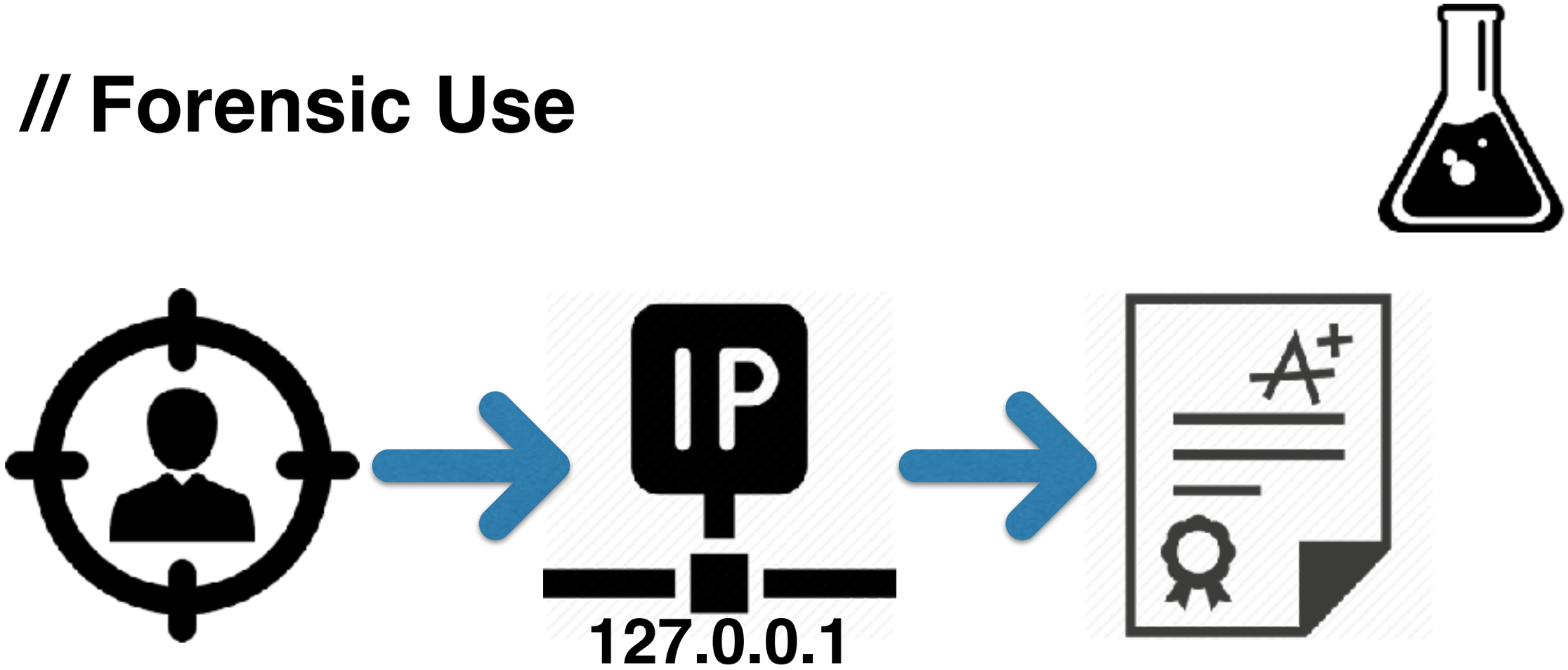
// Forensic Use



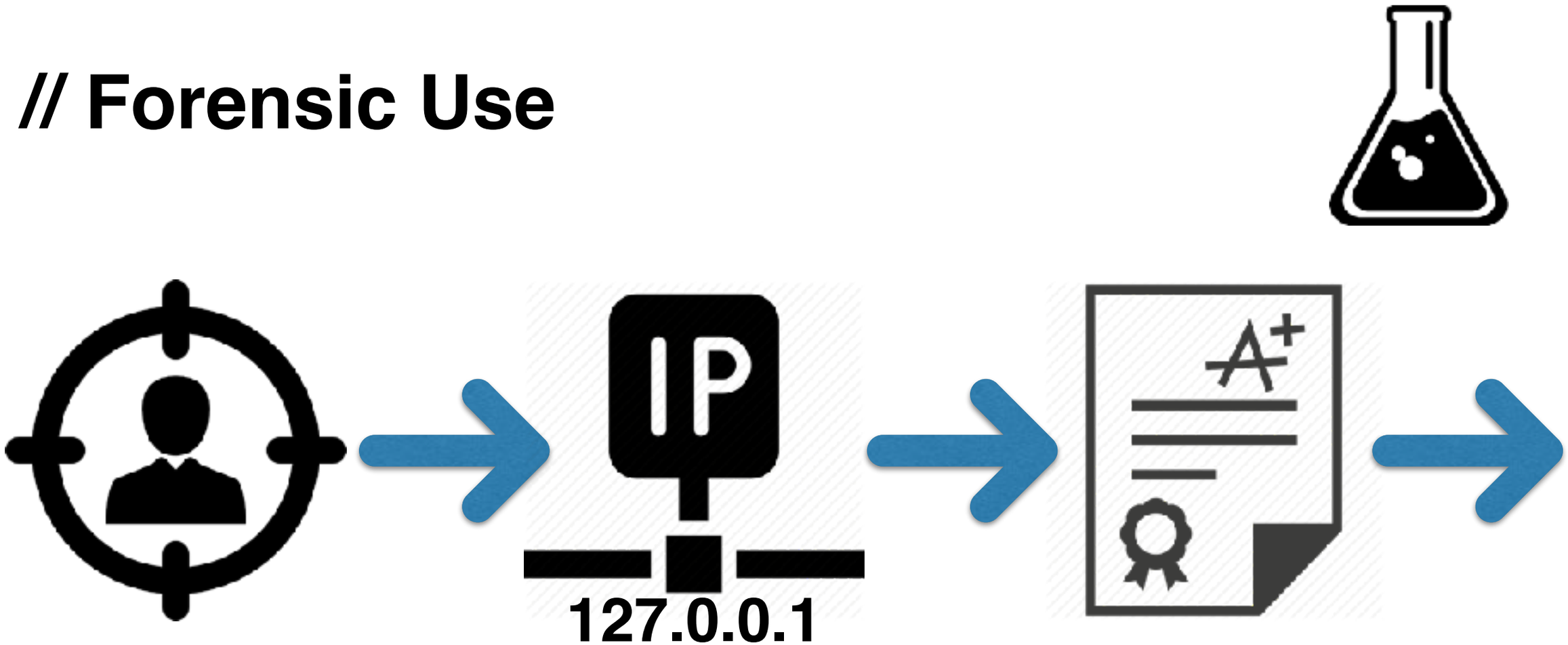
// Forensic Use



// Forensic Use

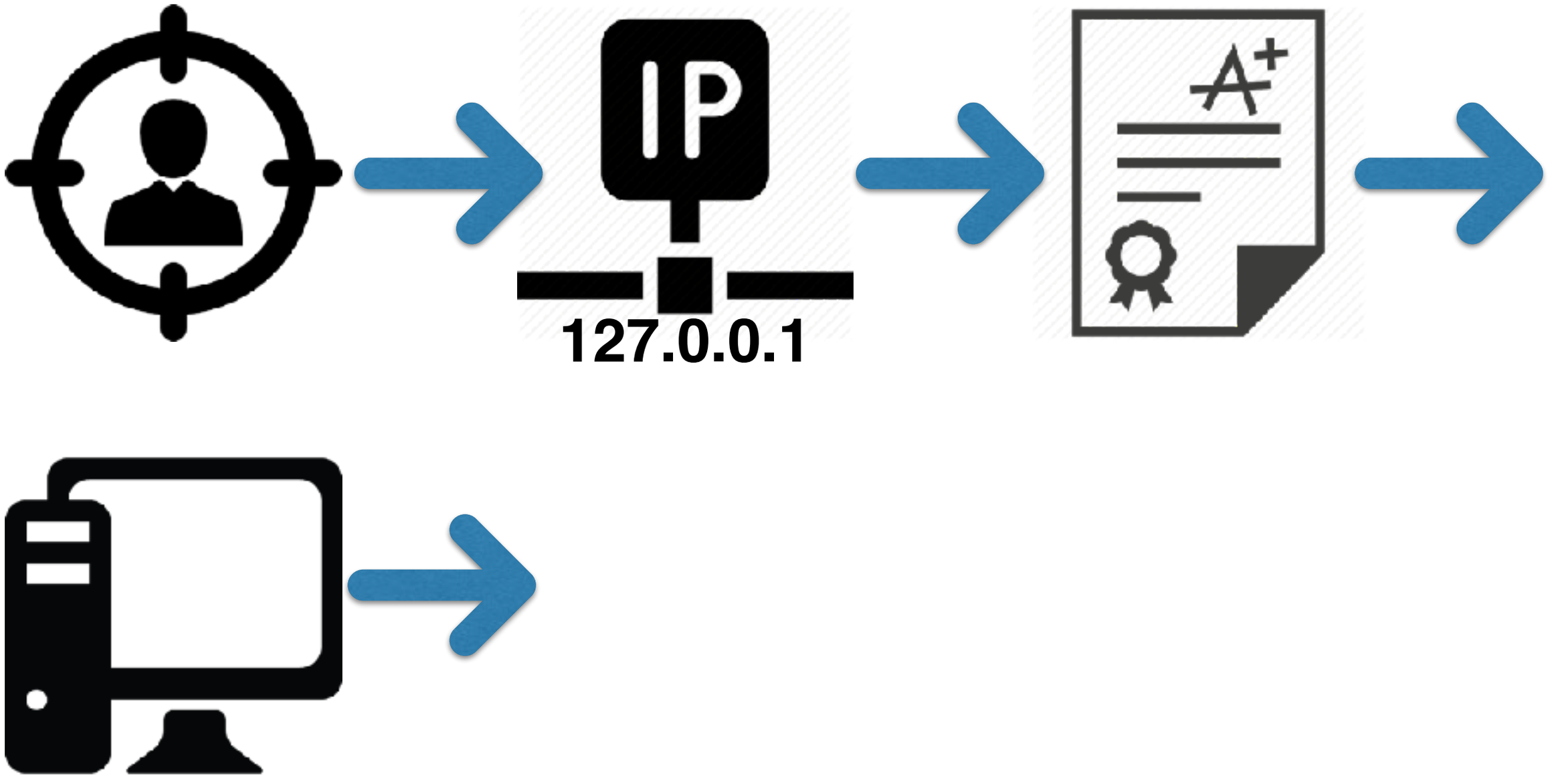


// Forensic Use

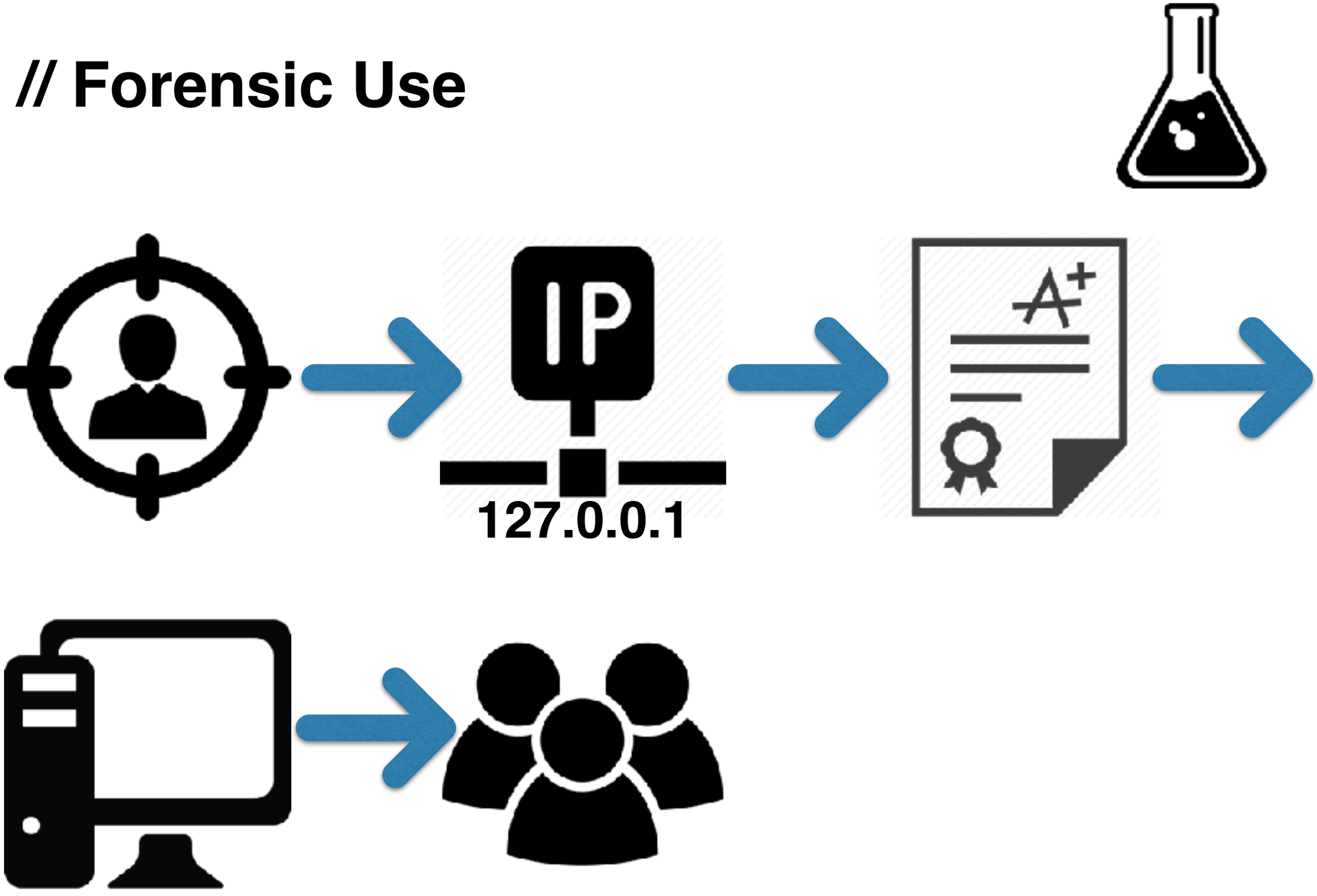


// Forensic Use

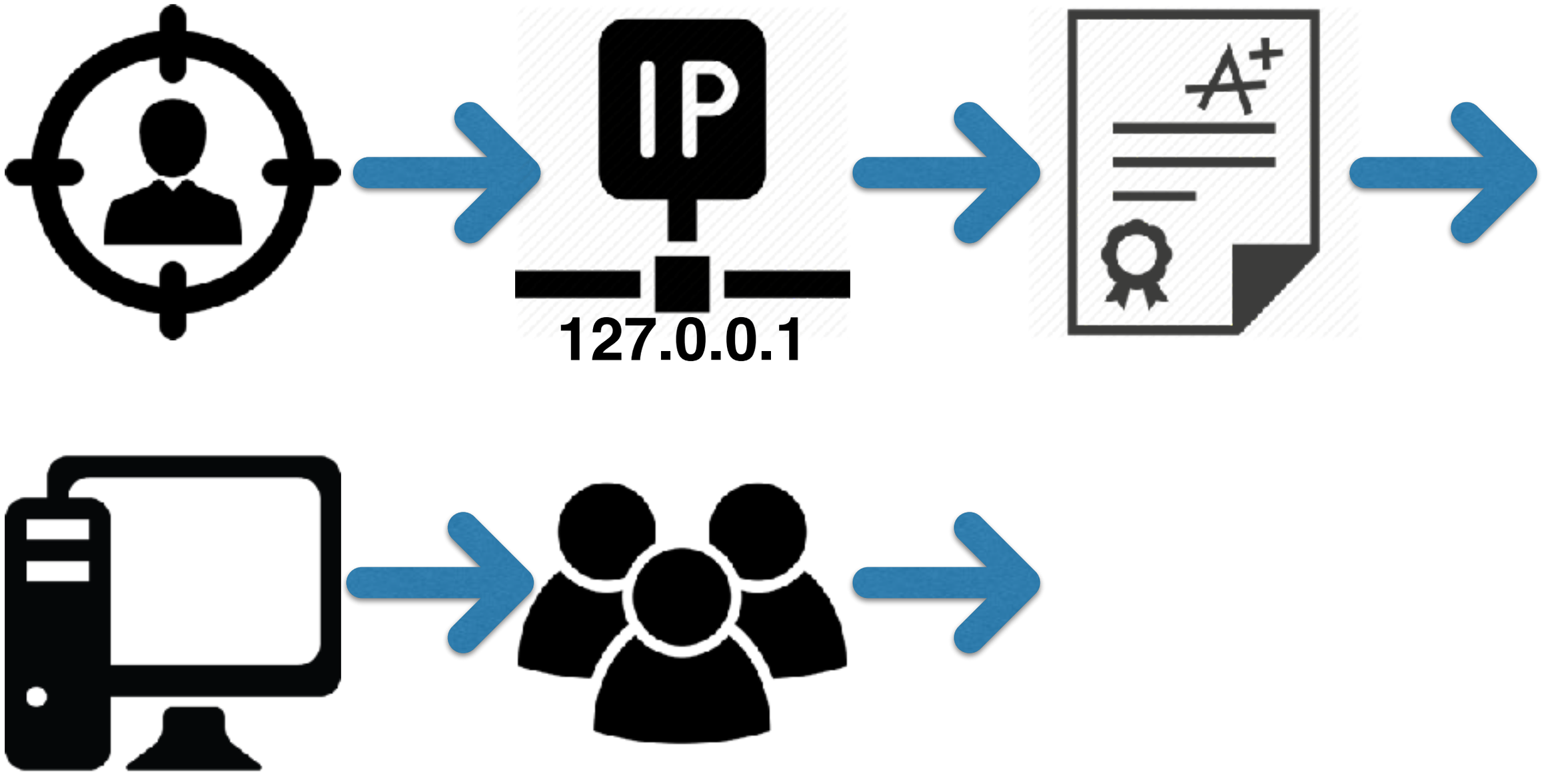
// Forensic Use



// Forensic Use



// Forensic Use

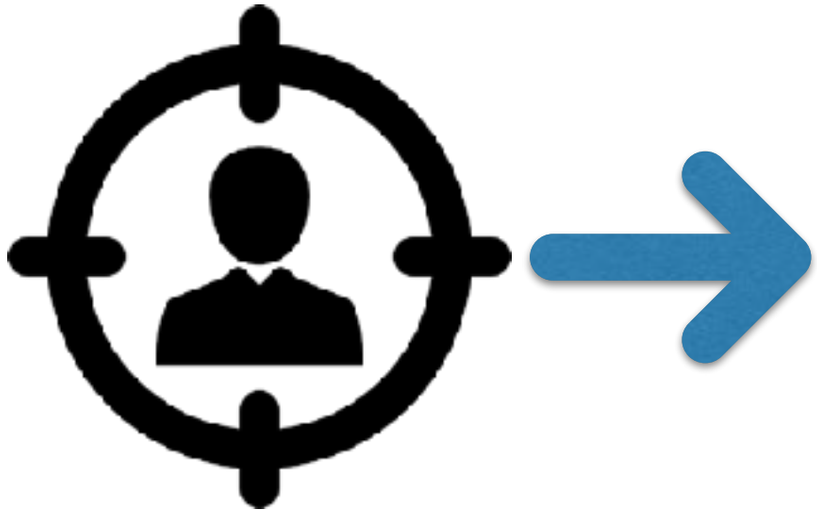


// Forensic Use

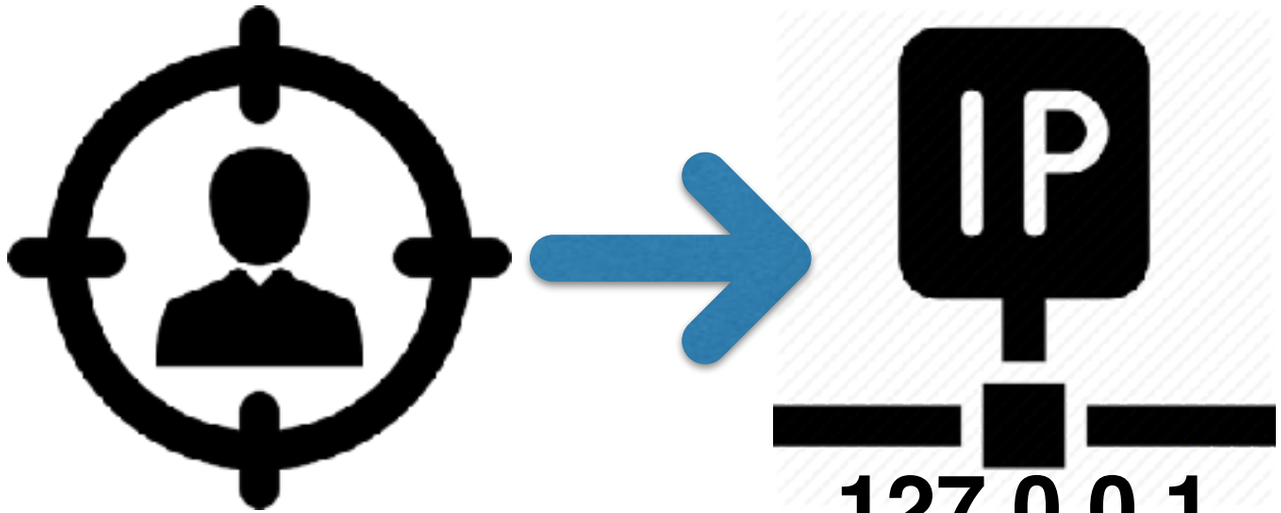
// Forensic Use

// Forensic Use

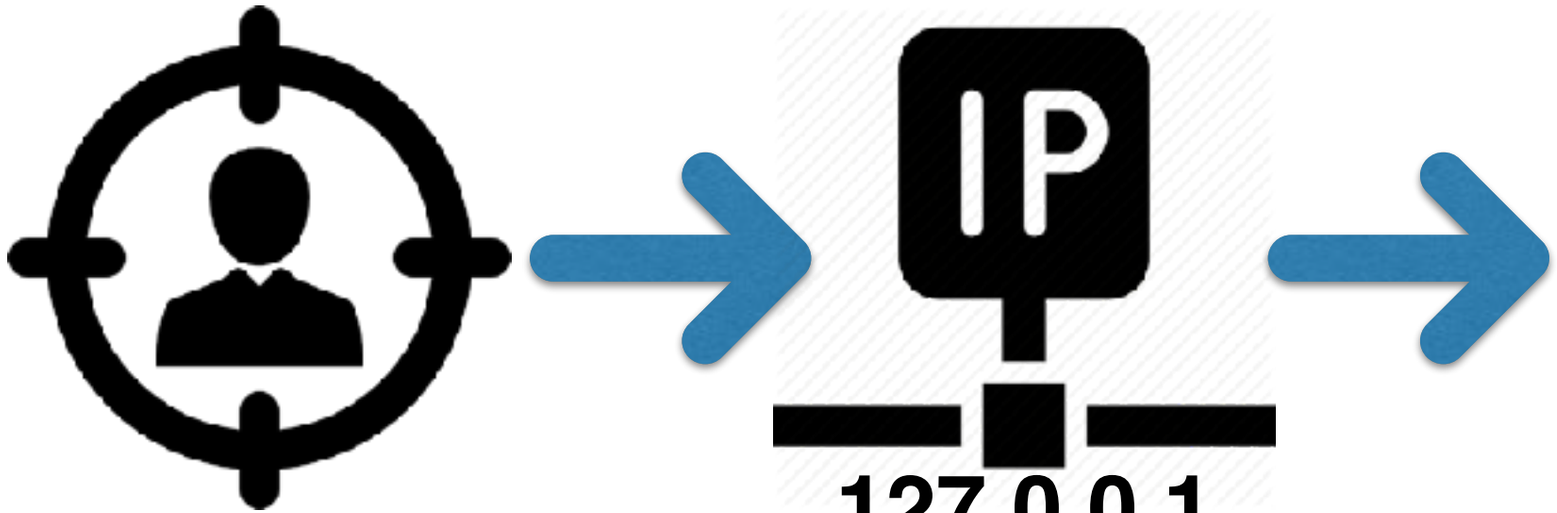
// Forensic Use



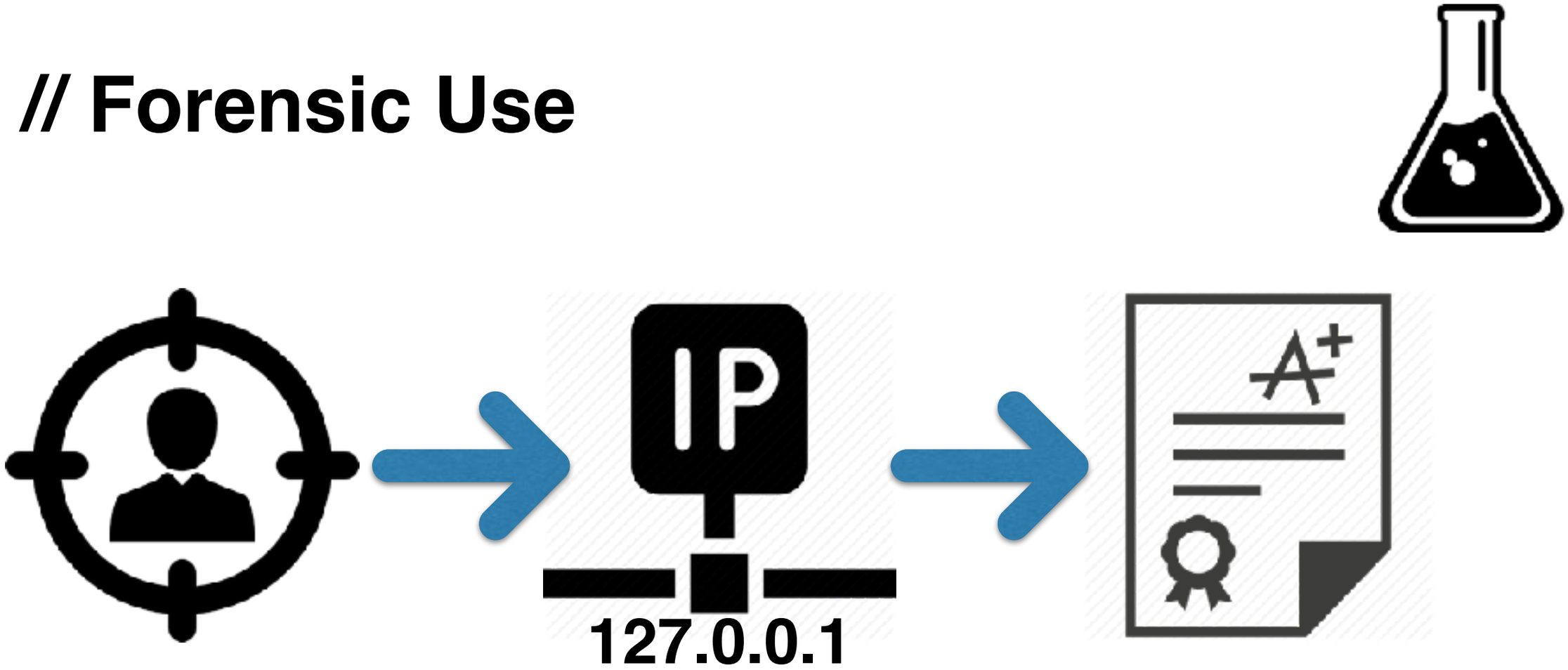
// Forensic Use



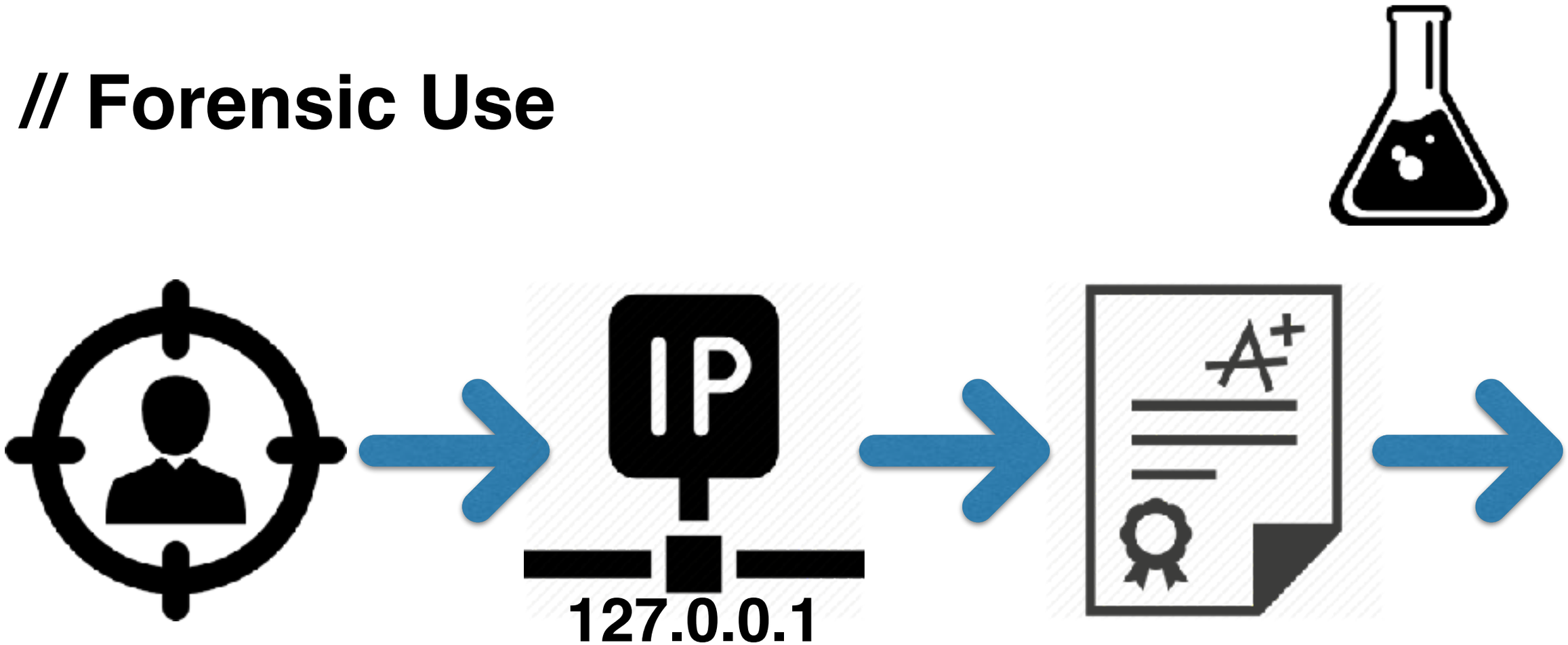
// Forensic Use



// Forensic Use

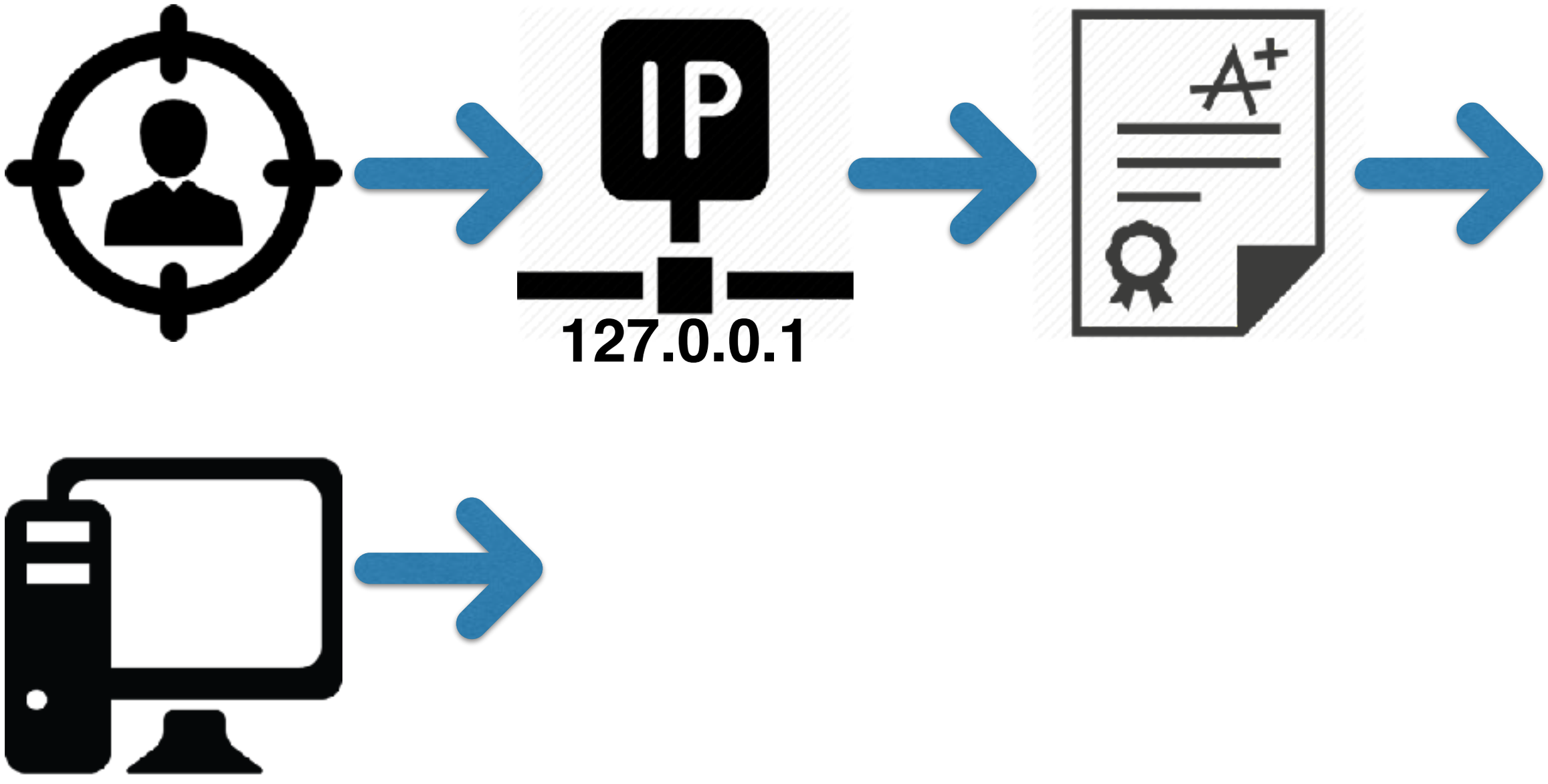


// Forensic Use

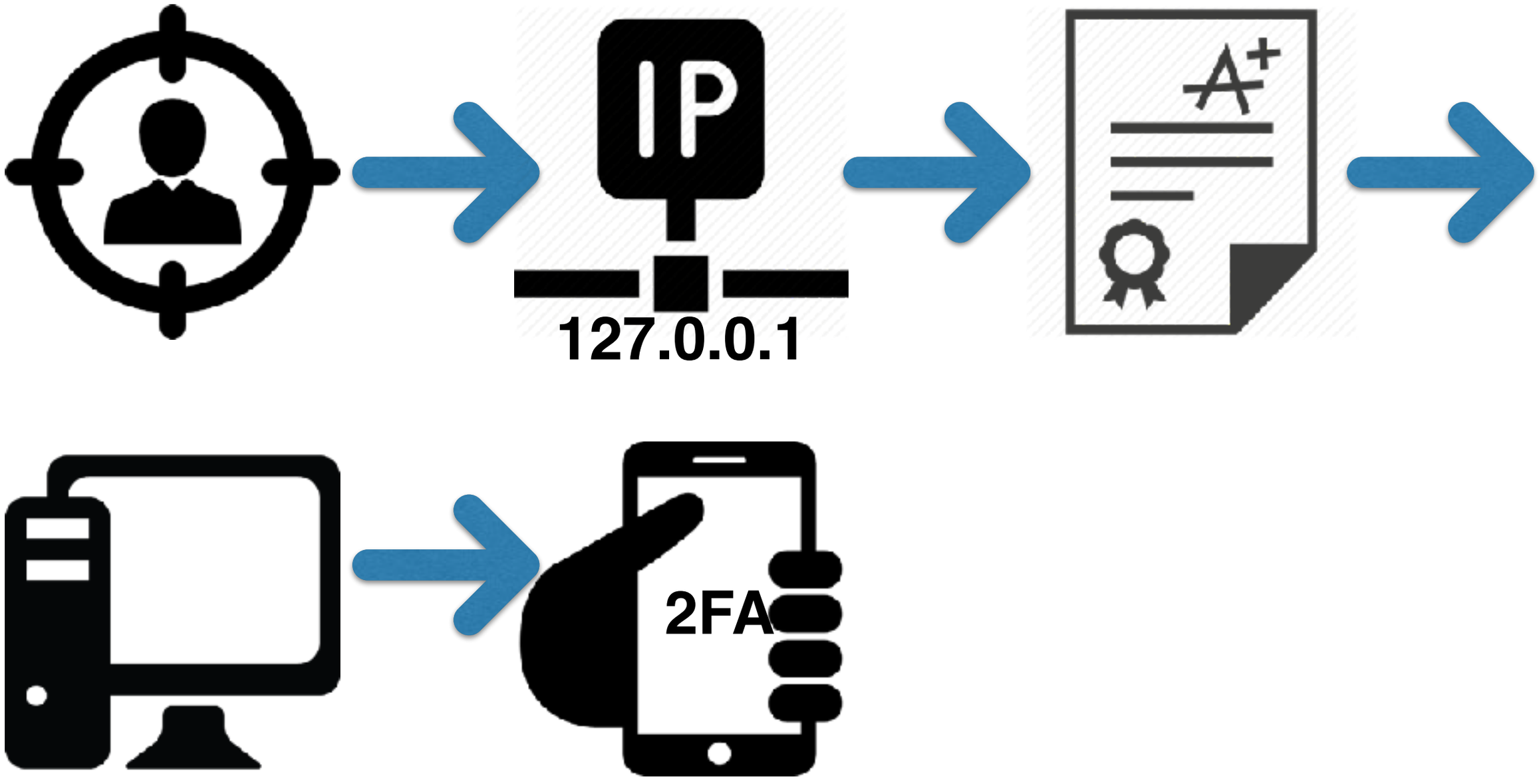


// Forensic Use

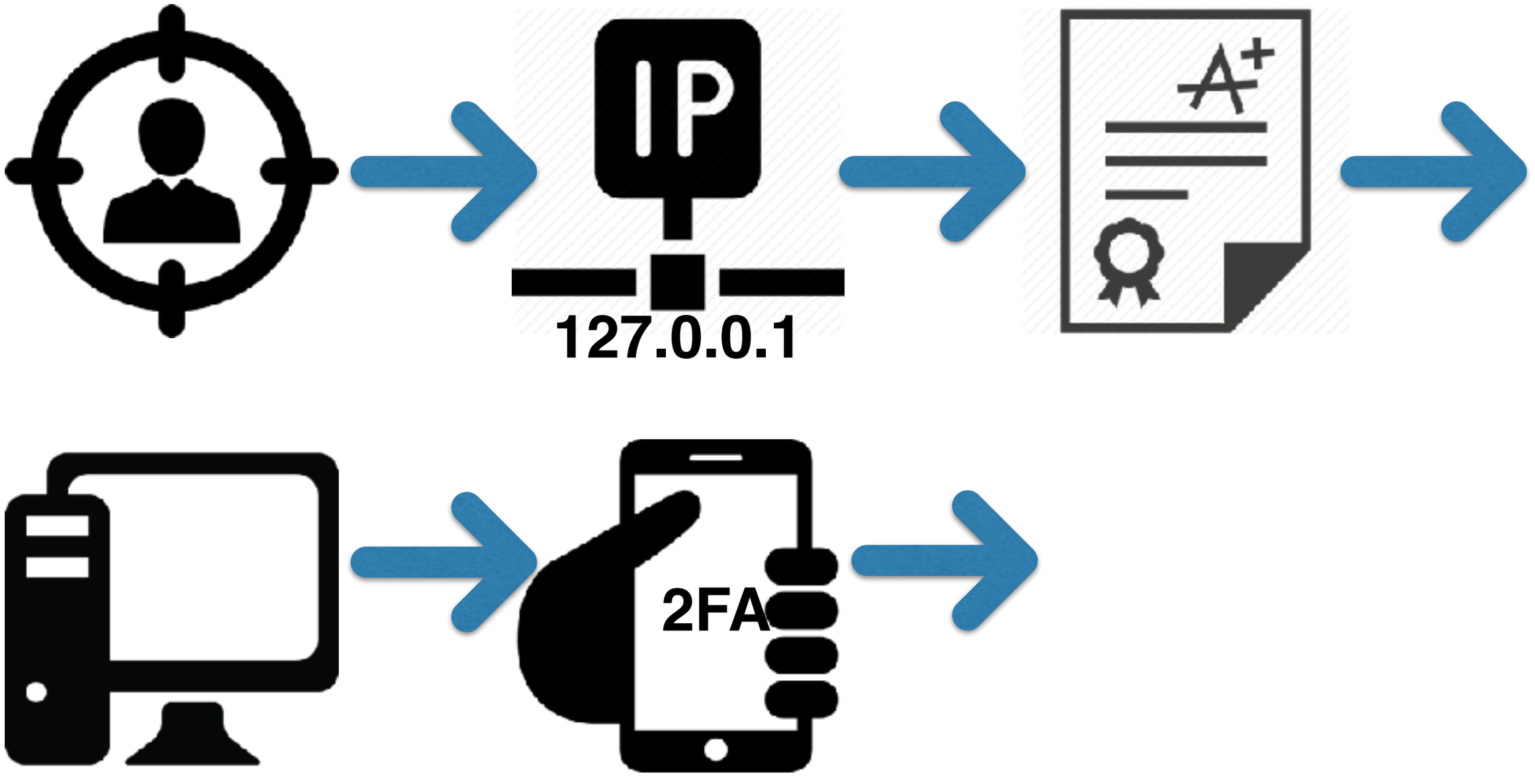
// Forensic Use



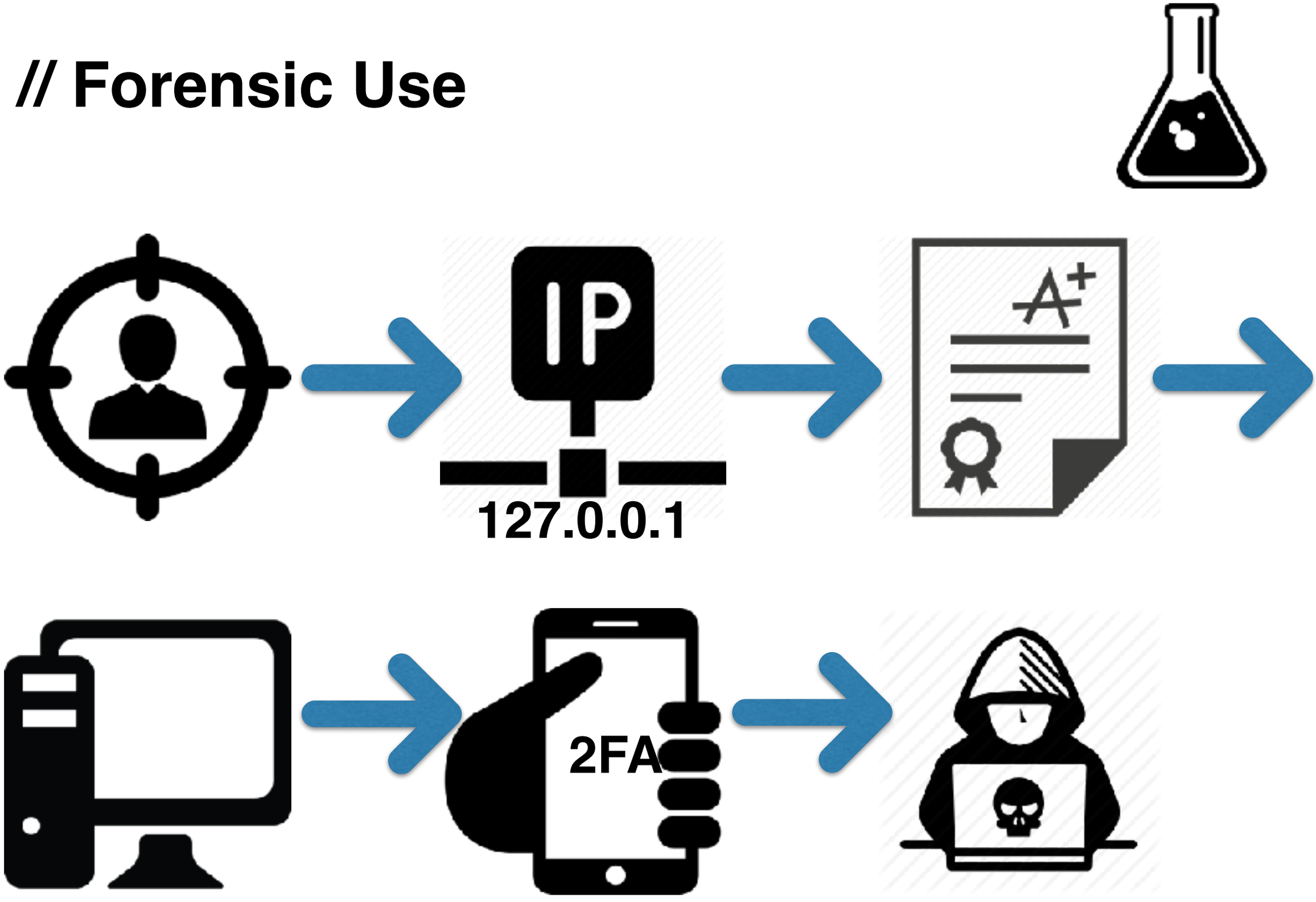
// Forensic Use



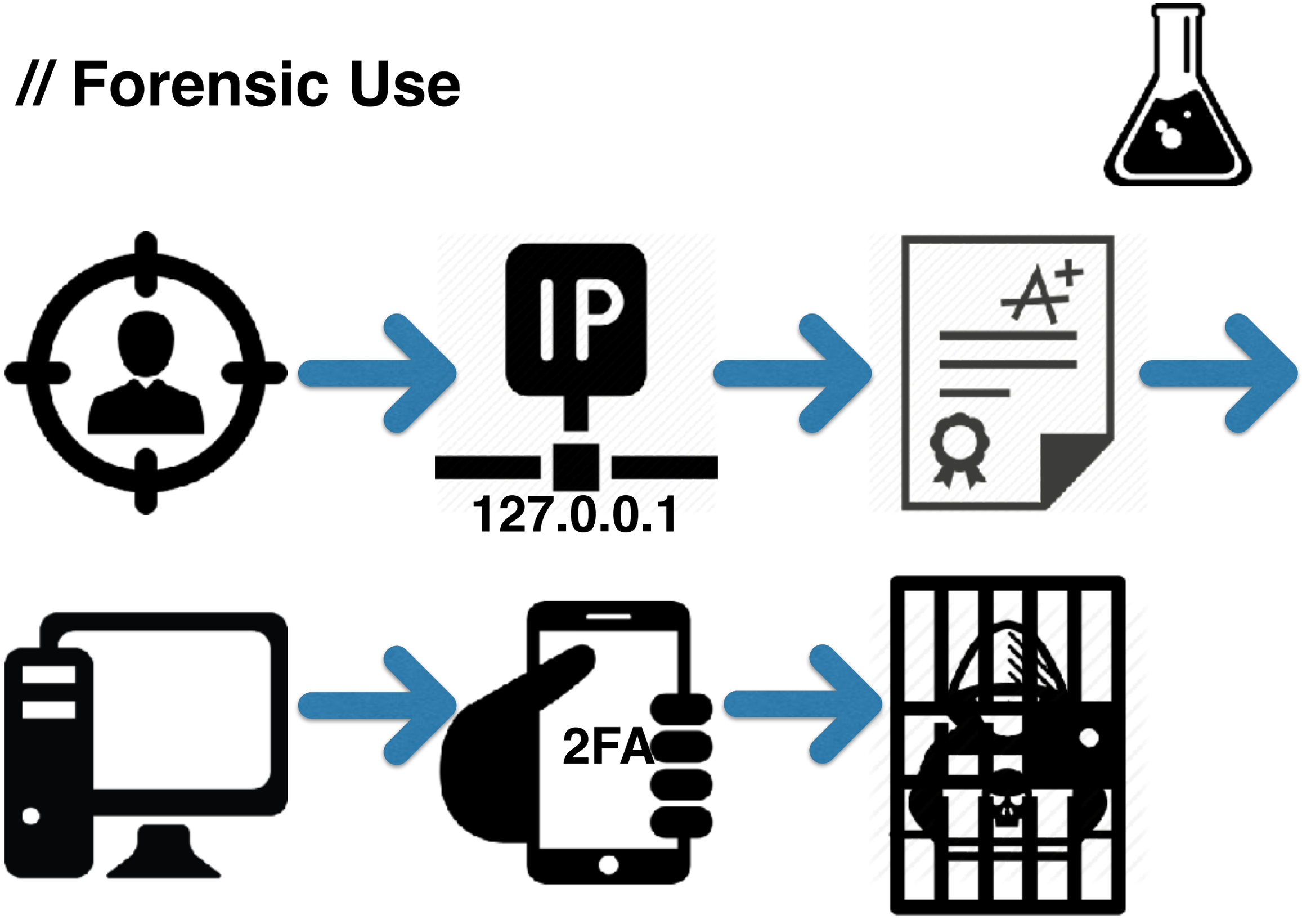
// Forensic Use



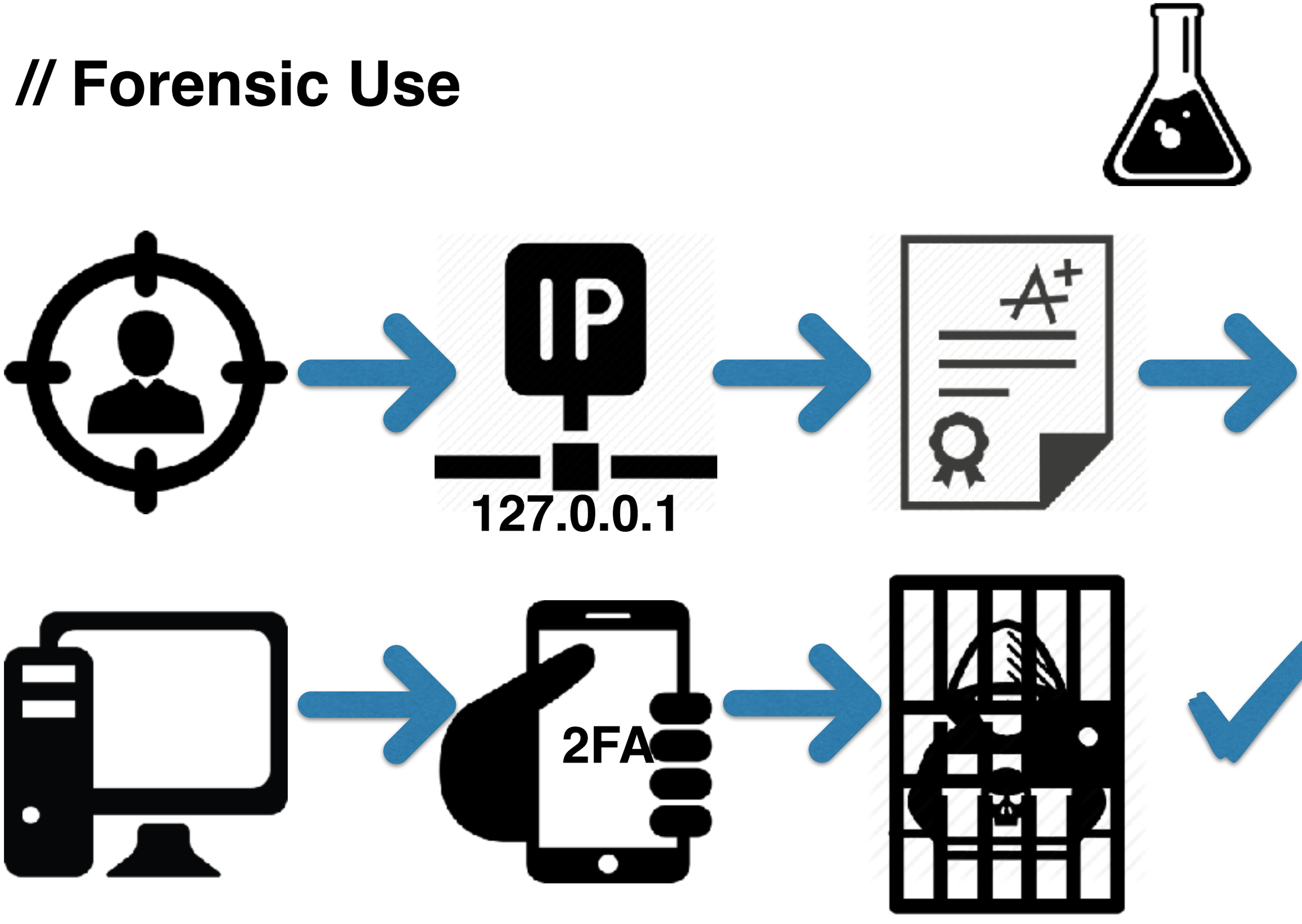
// Forensic Use



// Forensic Use

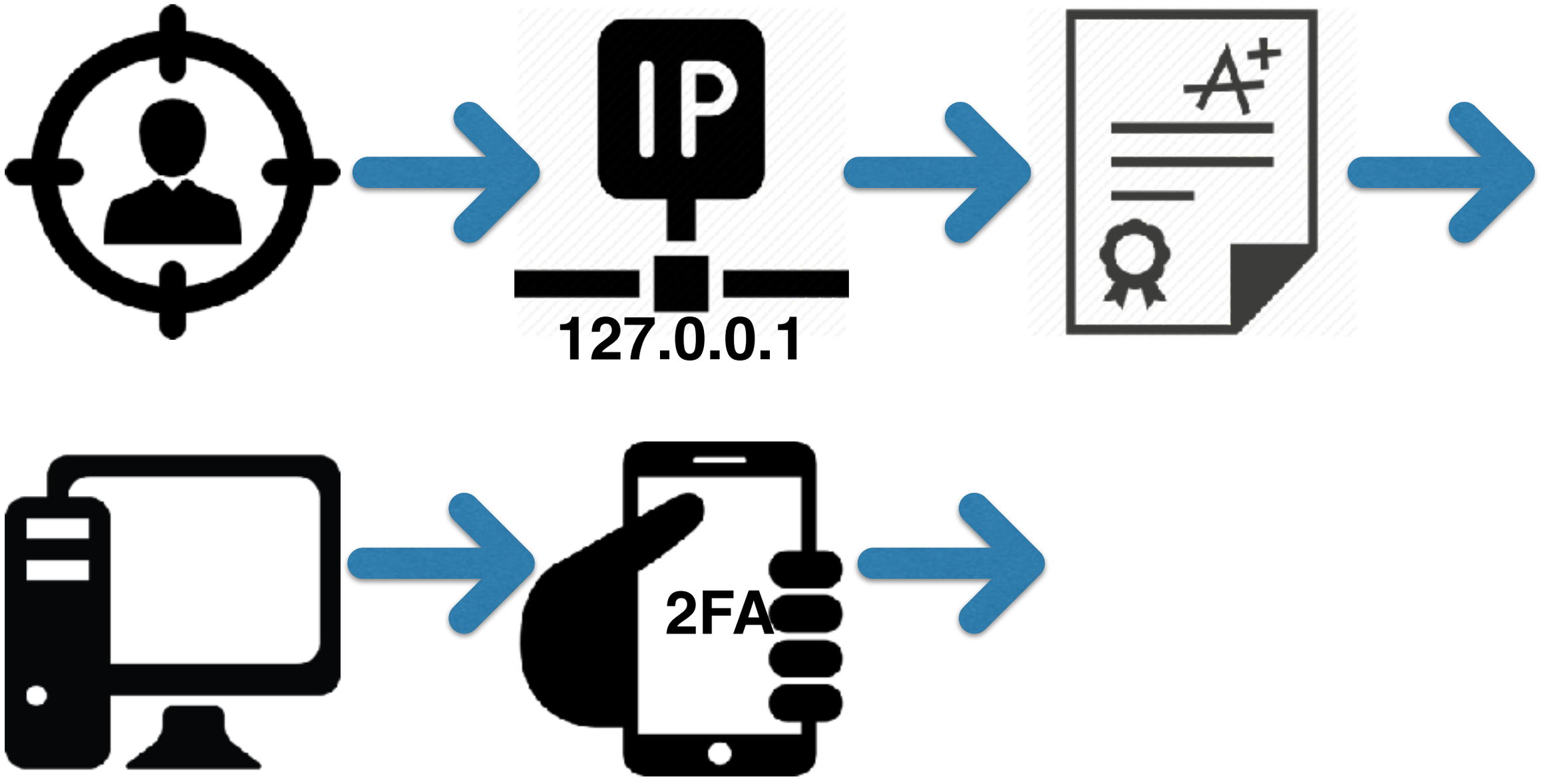


// Forensic Use

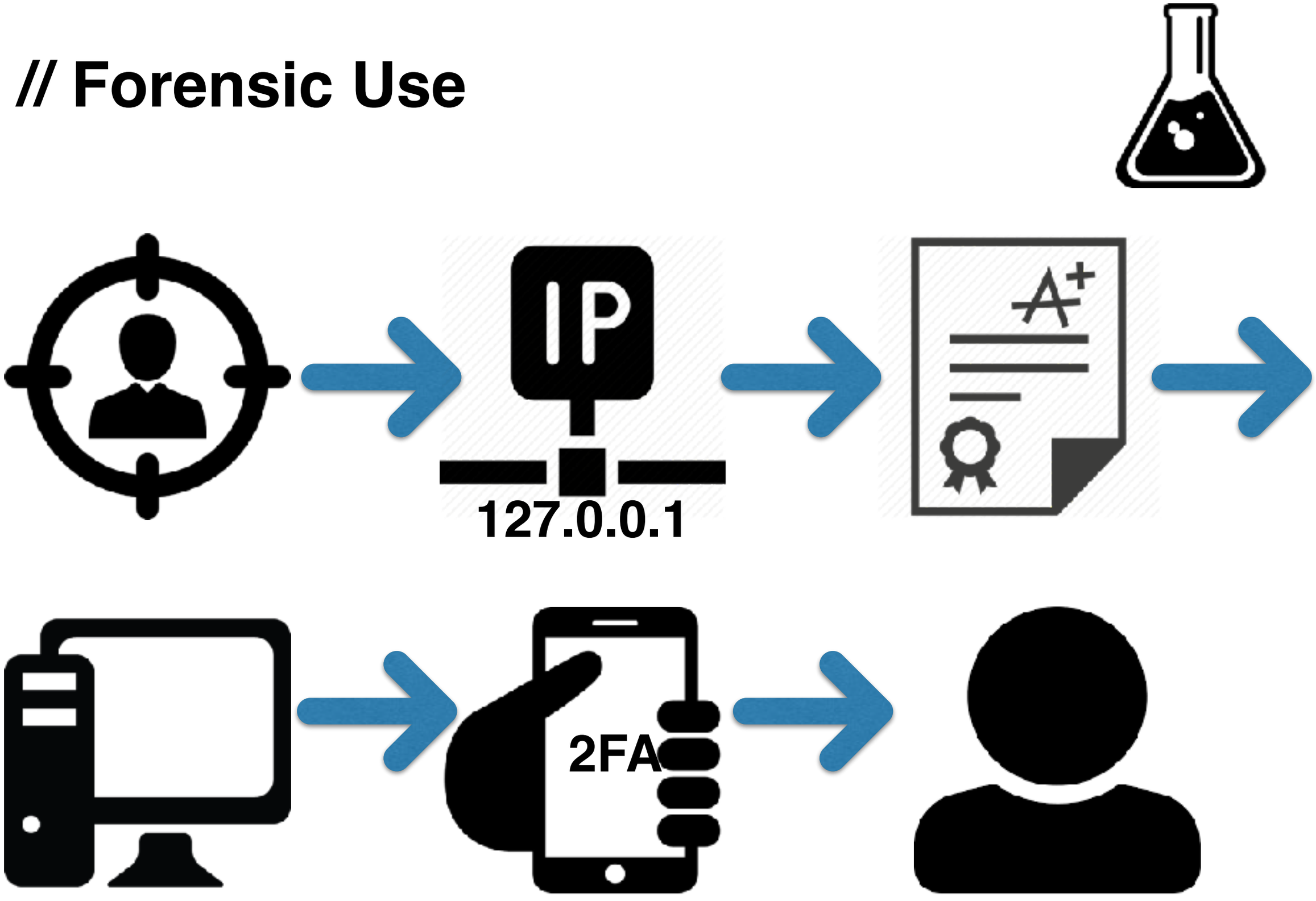


// Forensic Use

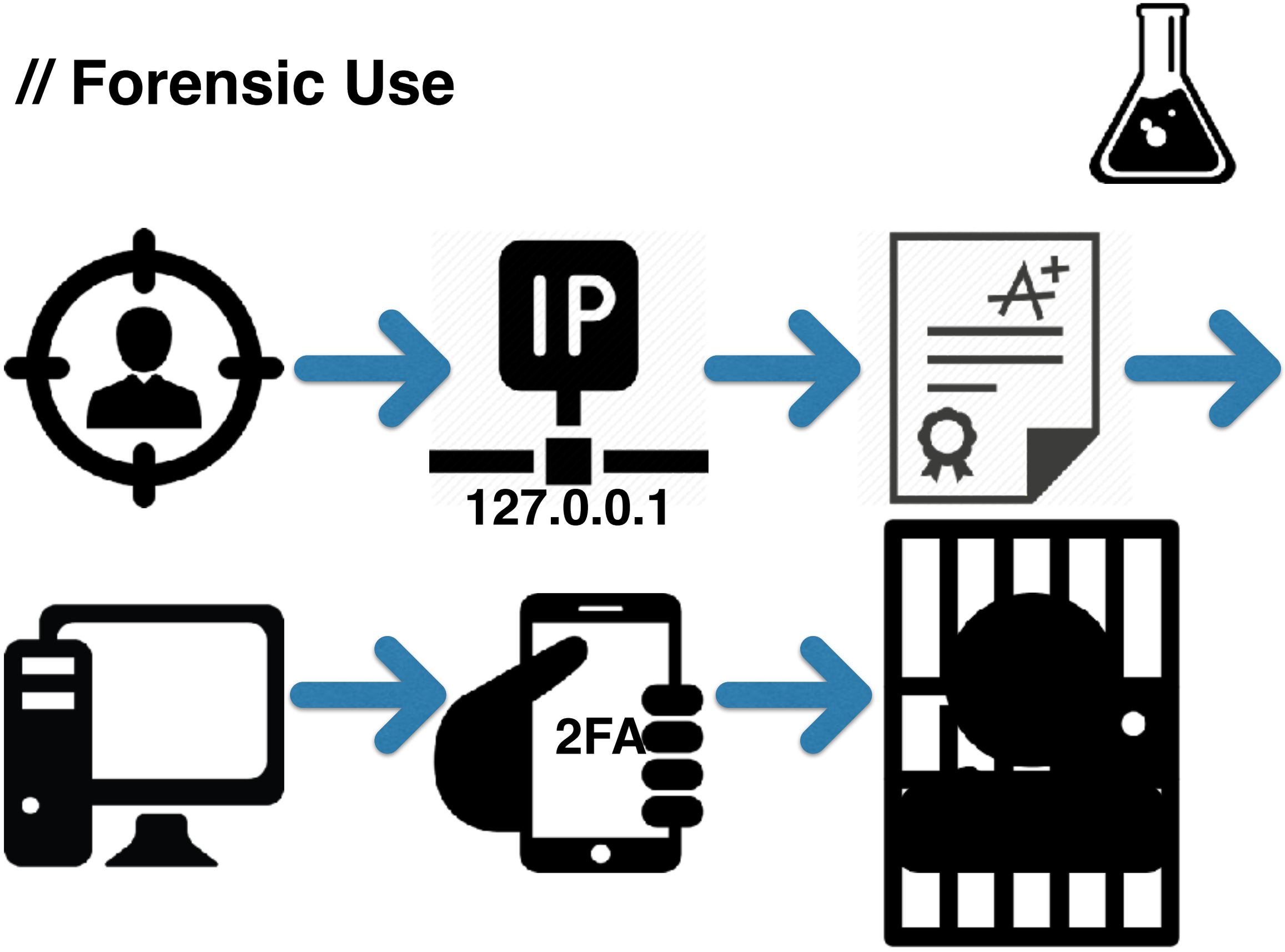
// Forensic Use



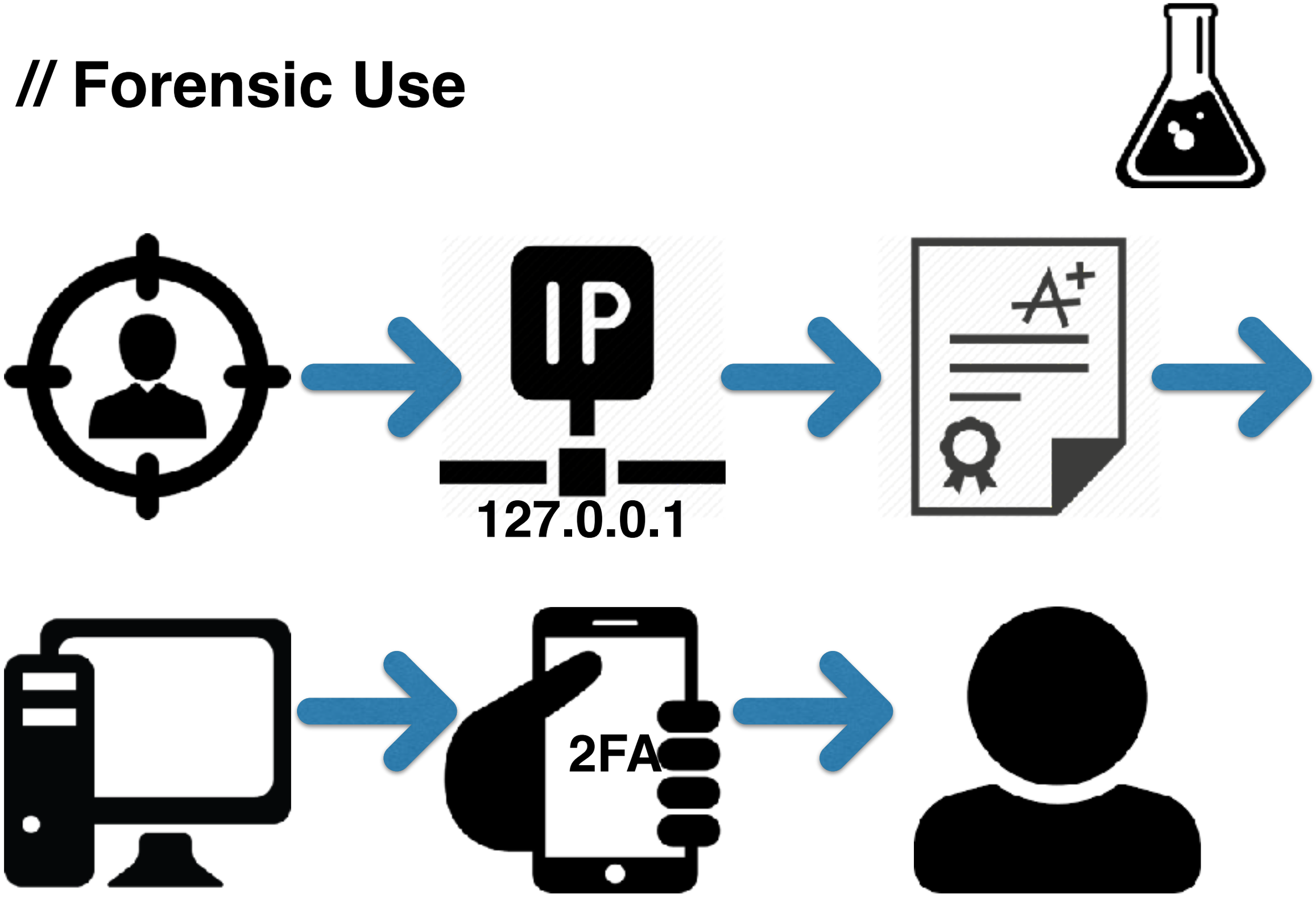
// Forensic Use



// Forensic Use



// Forensic Use



// Background

// Background

- Leslie **Lamport** formulated idea of using **OTP** in November 1981

// Background

- Leslie **Lamport** formulated idea of using **OTP** in November 1981
- $\boldsymbol{S = H(r_a \| ggKW)}$, see RFC 2289

// Background

- Leslie **Lamport** formulated idea of using **OTP** in November 1981
- $\boldsymbol{S} = \boldsymbol{H}(\boldsymbol{r}_a \| \boldsymbol{ggKW})$, see RFC 2289
- Of central importance is the **"shared secret"** (ggKW), as an essential basis for calculating the OTP

// Background

- Leslie **Lamport** formulated idea of using **OTP** in November 1981
- $\boldsymbol{S} = \boldsymbol{H}(\boldsymbol{r}_a \| \boldsymbol{ggKW})$, see RFC 2289
- Of central importance is the **"shared secret"** (ggKW), as an essential basis for calculating the OTP
- Three different types can be distinguished:
  - time-controlled method
  - challenge-response controlled method
  - event-driven method

// Background

- Leslie **Lamport** formulated idea of using **OTP** in November 1981
- $\boldsymbol{S = H(r_a \| ggKW)}$, see RFC 2289
- Of central importance is the **"shared secret"** (ggKW), as an essential basis for calculating the OTP
- Three different types can be distinguished:
  - time-controlled method
  - challenge-response controlled method
  - event-driven method
- Security of the **2FA app** strongly depends on **integrity** of the **operating system**

// Research

// Research

- The samples (2FA apps) were examined whether they

// Research

- The samples (2FA apps) were examined whether they

// Research

- The samples (2FA apps) were examined whether they
  - analyse the **environmental-integrity** during setup

// Research

- The samples (2FA apps) were examined whether they
  - analyse the **environmental-integrity** during setup
  - **encrypt** the „shared secret“ (and how)

// Research

- The samples (2FA apps) were examined whether they
  - analyse the **environmental-integrity** during setup
  - **encrypt** the „shared secret“ (and how)
  - allow **cloning** of the database (with stored secrets)

// Research

- The samples (2FA apps) were examined whether they
  - analyse the **environmental-integrity** during setup
  - **encrypt** the „shared secret“ (and how)
  - allow **cloning** of the database (with stored secrets)
  - disclose secrets due to **network-traffic** caused

// Research

- The samples (2FA apps) were examined whether they
  - analyse the **environmental-integrity** during setup
  - **encrypt** the „shared secret“ (and how)
  - allow **cloning** of the database (with stored secrets)
  - disclose secrets due to **network-traffic** caused
  - enable **stealing** of „shared secret“

// Research

// Research

- Examination procedure

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (before execution)

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (before execution)
  - Record **network-traffic** during execution

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (before execution)
  - Record **network-traffic** during execution
  - **Re-backup** after execution and configuration

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (before execution)
  - Record **network-traffic** during execution
  - **Re-backup** after execution and configuration
  - Calculate the **differences** of both snapshots

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (before execution)
  - Record **network-traffic** during execution
  - **Re-backup** after execution and configuration
  - Calculate the **differences** of both snapshots
  - **Analysis** of the collected data

// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (before execution)
  - Record **network-traffic** during execution
  - **Re-backup** after execution and configuration
  - Calculate the **differences** of both snapshots
  - **Analysis** of the collected data
  - **Verification** of the results using tests in AVD

// Results

Sample: „Google Authenticator“

Icon	Anwendung	Version	Hash (MD5)	Größe
	Google Authenticator	4.74	2658652deea2a274c90e111135634e1f	6,9 MB
Programmpfad:	/data/data/com.google.android.apps.authenticator2			
UID:	u0_a128			
Ablage Shared Secret:	{app_verz}/databases/databases (SQLite)			
Format des TOTP:	Dezimal (6-stellig)			
Shared Secret:	rffl4xngz3bzhe5g7fhji4rzra			

// Results

Sample: „Google Authenticator“

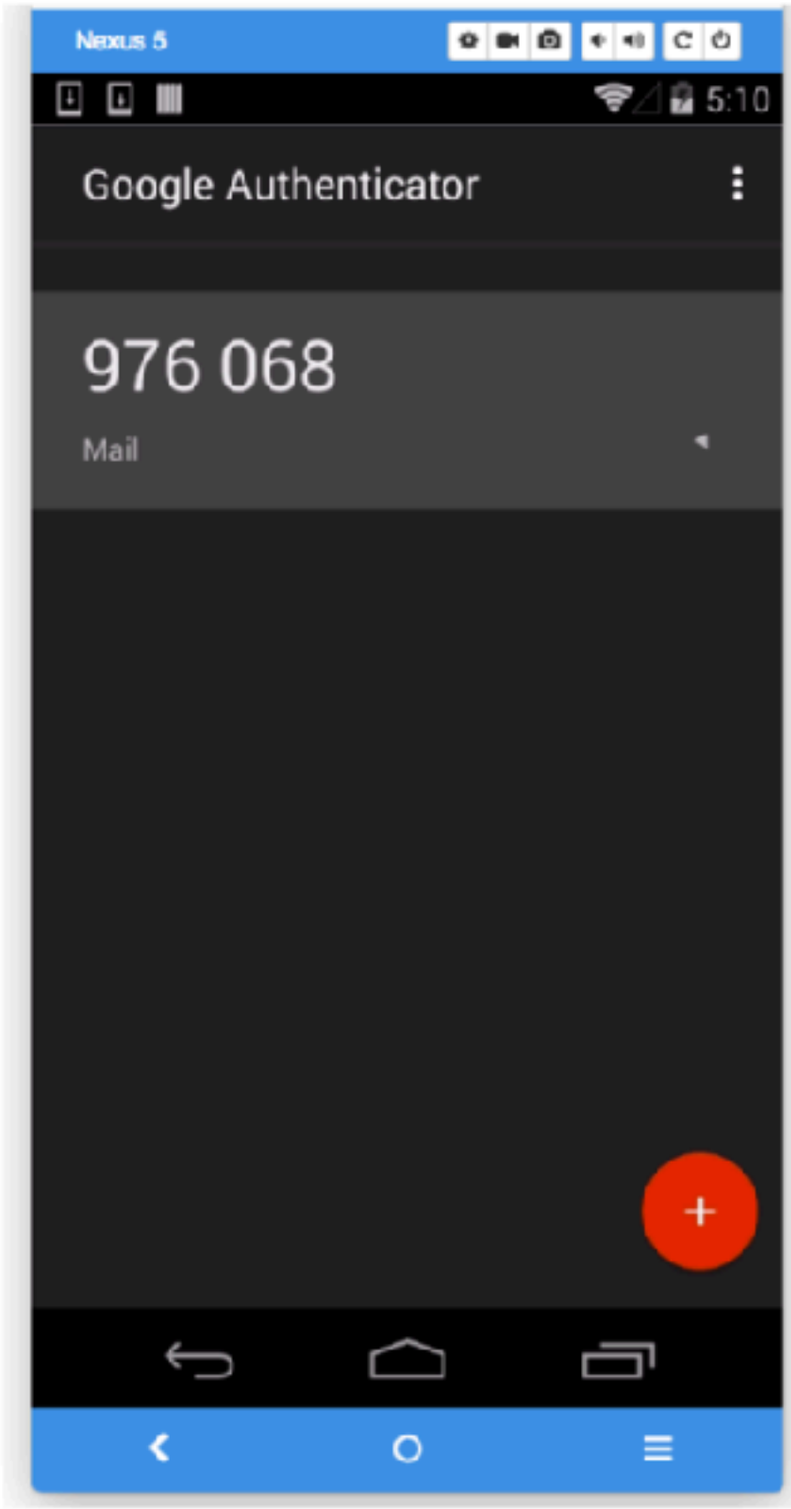
Icon	Anwendung	Version	Hash (MD5)	Größe
	Google Authenticator	4.74	2658652deea2a274c90e111135634e1f	6,9 MB
Programmpfad:	/data/data/com.google.android.apps.authenticator2			
UID:	u0_a128			
Ablage Shared Secret:	{app_verz}/databases/databases (SQLite)			
Format des TOTP:	Dezimal (6-stellig)			
Shared Secret:	rffl4xngz3bzhe5g7fhji4rzra			

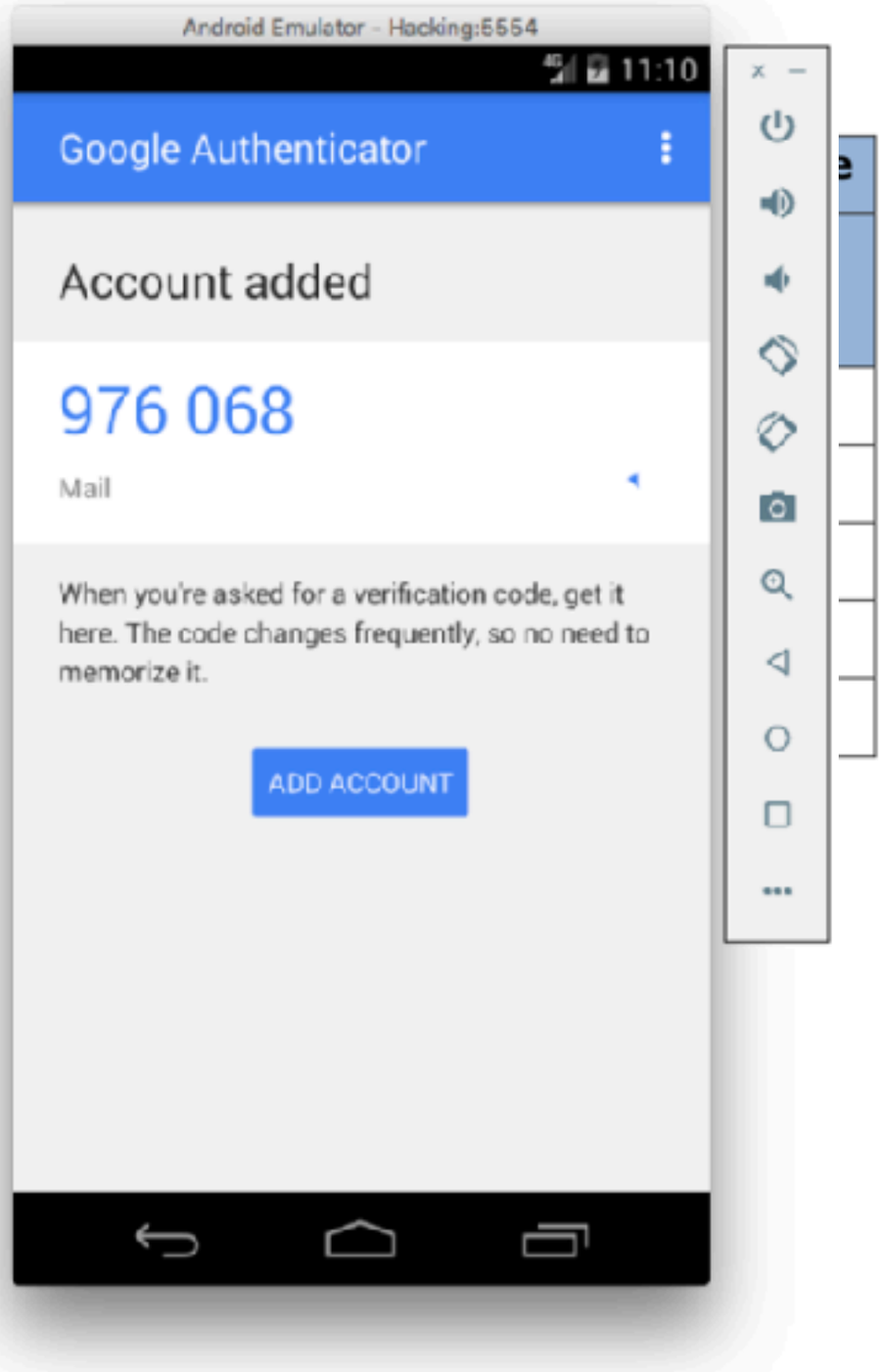
```
42:GA philip$ adb pull /data/data/
com.google.android.apps.authenticator2/databases/databases/

42:GA philip$ sqlite3 ./databases "select * from accounts" >
google_authenticator_secret.txt


42:GA philip$ cat google_authenticator_secret.txt 1|Dropbox|
rffl4xngz3bzhe5g7fhji4rzra|0|0|0||Dropbox


42:GA philip$
```

// Results

```
>> POST https://91.215.103.66/appcfg.php
        ← 304 [no content] 601ms
   POST https://172.217.23.174/fdfe/apps/contentSync
        ← 200 application/protobuf 61b 816ms
   POST https://172.217.23.174/auth
        ← 200 text/plain 266b 327ms
   POST https://172.217.17.42/plusi/v3/ozInternal/gmsgnotsfetchbyidentifier?alt=proto
        ← 200 application/x-protobuf 610b 426ms
   GET
https://172.217.23.161/proxy/RmHevzGfWbmd87_FmcOWySSx1f5WGNu7rNiv7_Zq5OYs8UvbUmv9aQfdAqp
vdBUiOiGxWTs1OMcquRF9RLhRAOzJbJUdOKyV_uEg=w360
       ← 200 image/png 18.5k 186ms
   POST https://172.217.17.42/plusi/v3/ozInternal/gmsgnotssetreadstates?alt=proto
        ← 200 application/x-protobuf 48b 151ms
   POST https://216.58.214.74/play/log?format=raw&proto_v2=true
        ← 200 text/plain 38b 268ms
   POST https://172.217.23.174/auth
        ← 200 text/plain 265b 238ms
   GET https://66.102.1.102/history/api/lookup?client=web_app
       ← 200 application/javascript 55b 235ms
   GET https://66.102.1.102/history/api/lookup?client=device
       ← 200 application/javascript 55b 220ms


⇩  [1/10]
                                                              ?:help
[*:8080]
```

// Results





42:G
com.

42:G
goog

42:G
rffl4x

42:G

// Results

Sample: „Duo Mobile“

Icon	Anwendung	Version	Hash (MD5)	Größe
	Duo Mobile	3.16.1	afe74d12a8f4f9cb8e107727d0010727	12,3 MB
Programmpfad:	/data/data/com.duosecurity.duomobile			
UID:	u0_a156			
Ablage Shared Secret:	{app_verz}/files/duokit/accounts.json			
Format des TOTP:	Dezimal (6-stellig)			
Shared Secret:	hvwb64jexhst5xg2rg5j5nfwci			

// Results

Sample: „Duo Mobile“

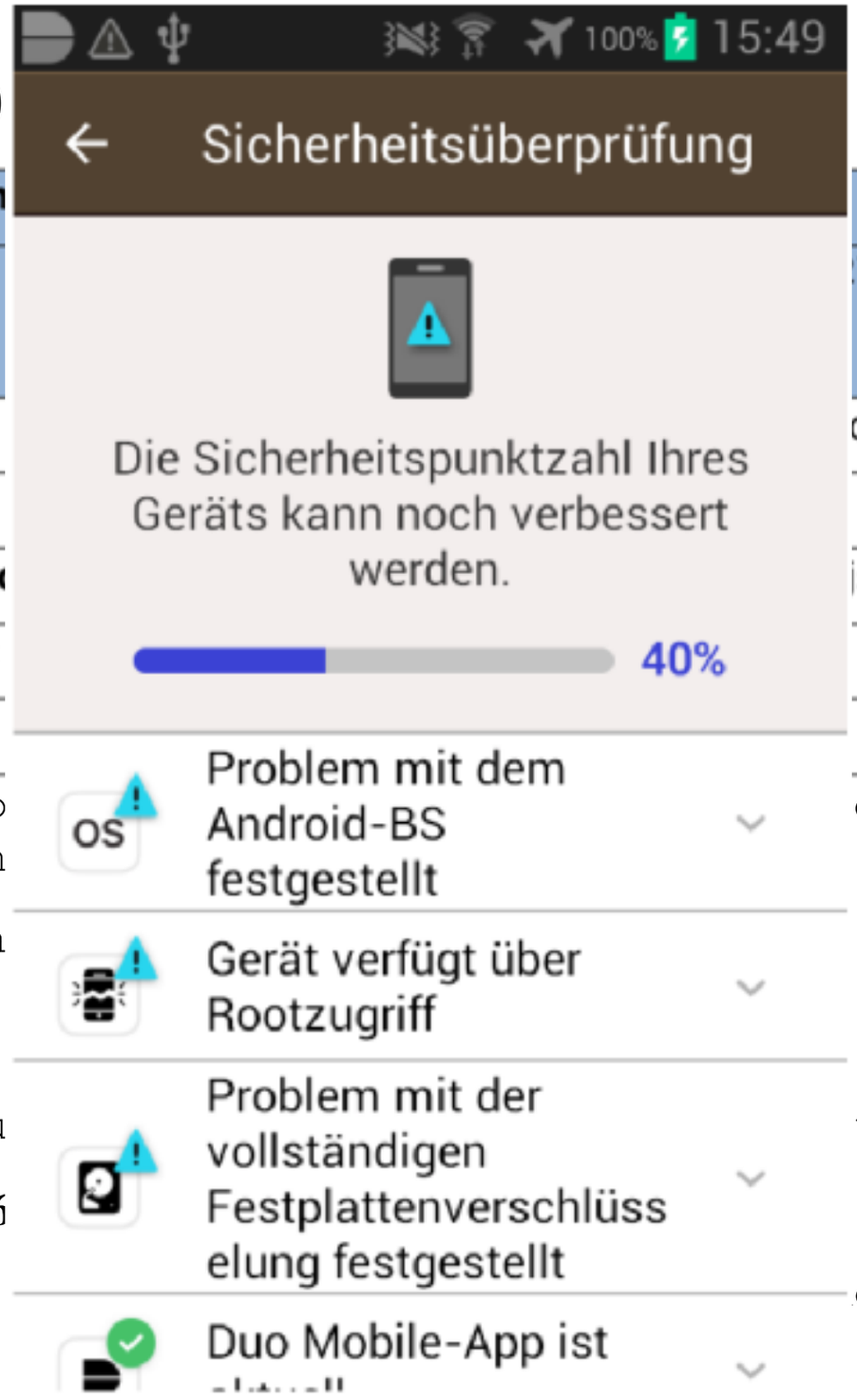
Icon	Anwendung	Version	Hash (MD5)	Größe
	Duo Mobile	3.16.1	afe74d12a8f4f9cb8e107727d0010727	12,3 MB
Programmpfad:	/data/data/com.duosecurity.duomobile			
UID:	u0_a156			
Ablage Shared Secret:	{app_verz}/files/duokit/accounts.json			
Format des TOTP:	Dezimal (6-stellig)			
Shared Secret:	hvwb64jexhst5xg2rg5j5nfwci			

```
42:Duo philip$ adb pull /data/data/com.duosecurity.duomobile/files/
duokit/accounts.json

42:Duo philip$ cat accounts.json
[

{
"name": "philipevalu@wegwerfemail.info", "otpGenerator": {

"otpSecret": "HVWB64JEXHST5XG2RG5J5NFWCI" },

"logoUri": "android.resource://com.duosecurity.duomobile/drawable/
ic_dropbox"

} ]
```

// Results

Sample: „D

Icon	Anwendun		Größe
DUO	Duo Mobile	7d0010727	12,3 MB
Programmpfad:		obile	
UID:			
Ablage Shared Se		ison	
Format des TOTP:			
Shared Secret:			




```
42:Duo philip$ adb p                                    duomobile/files/
duokit/accounts.json

42:Duo philip$ cat a
[

{
"name": "philipevalu                                    tor": {

"otpSecret": "HVWB6

"logoUri": "android.                                    obile/drawable/
ic_dropbox"

} ]
```

// Results

X = Yes; O = No; - = unwanted behavior; + = wanted behavior

2FA App Name	Cloning Possible	Encrypted Secret	Device Integrity Check	PIN Protection	Secure SSL-Connection	Secure OTP-Push
Google Authenticator	X-	O-	O-	O-	N/A	N/A
Microsoft Authenticator	X-	O-	O-	O-	X+	O-
Authy 2-Factor Authentification	O+	O-	O-	X+	X+	N/A
DUO Mobile	X-	O-	X+	O-	X+	X+
FreeOTP	X-	O-	O-	O-	N/A	N/A
Sophos Authenticator	X-	O-	O-	O-	N/A	N/A
Push Authenticator	X-	O-	O-	O-	N/A	N/A
OTP Authenticator	O+	O-	O-	O-	N/A	N/A
Yandex.Key	O+	X+	O-	X+	N/A	N/A
Symantec VIP Access	O+	X+	O-	O-	X+	X+
2FA Token	X-	O-	O-	O-	N/A	N/A
Launchkey	X-	N/A	O-	X+	X+	N/A
CyAuth Cylocklite	X-	X+	O-	O-	X+	N/A
Topicus KeyHub	X-	O-	O-	O-	X+	N/A
Latch	O+	X+	O-	O-	O-	N/A
Okta Verify	O+	X+	O-	O-	X+	N/A

// Results

// Results

- Security implementations vary greatly

// Results

- Security implementations vary greatly
- 50 % of apps do not **encrypt** „shared secret“

// Results

- Security implementations vary greatly
- 50 % of apps do not **encrypt** „shared secret“
- 12.5 % of the apps only use other **notation**

// Results

- Security implementations vary greatly
- 50 % of apps do not **encrypt** „shared secret“
- 12.5 % of the apps only use other **notation**
- Security strongly dependent on OS

// Results

- Security implementations vary greatly
- 50 % of apps do not **encrypt** „shared secret“
- 12.5 % of the apps only use other **notation**
- Security strongly dependent on OS
- 56 % of the apps allow **copying the DB**

// Results

- Security implementations vary greatly
- 50 % of apps do not **encrypt** „shared secret“
- 12.5 % of the apps only use other **notation**
- Security strongly dependent on OS
- 56 % of the apps allow **copying the DB**
- Only about 1/5 of the apps offer PIN protection

// Results

- Security implementations vary greatly
- 50 % of apps do not **encrypt** „shared secret“
- 12.5 % of the apps only use other **notation**
- Security strongly dependent on OS
- 56 % of the apps allow **copying the DB**
- Only about 1/5 of the apps offer PIN protection
- Only 44 % do not generate **network traffic**

// Conclusion

// Conclusion

- Pro 2FA-App

// Conclusion

- Pro 2FA-App

  - Comprehensive use of 2FA is recommended
  - 2FA app reduces number of devices to carry
  - SM have more (transparent) data/sensors

// Conclusion

- Pro 2FA-App
  - Comprehensive use of 2FA is recommended
  - 2FA app reduces number of devices to carry
  - SM have more (transparent) data/sensors
- Pro HW-Token

// Conclusion

- Pro 2FA-App

  - Comprehensive use of 2FA is recommended
  - 2FA app reduces number of devices to carry
  - SM have more (transparent) data/sensors

- Pro HW-Token

  - HW token self-sufficient -> no area of attack via remote
  - "Stealing" the "shared secret" undermines factor **property**
  - 2FA apps persuade to use a single device only
  - Spread of specific malware threatens 2FA apps
  - FIDO-Alliance combines secure hardware and PKI

Thank you for your attention
Questions? 42!