

---

# HIPSSA Project

Support for Harmonization of the ICT Policies  
in Sub-Sahara Africa

ITU/HIPSSA CYBERSECURITY TECHNICAL ASSISTANCE FOR THE  
REPUBLIC OF RWANDA 2013

Capacity Building on  
Investigation

11-12 July 2013



# WHY LEA AND NOT ONLY CYBERCRIME INVESTIGATORS NEED TRAINING



# OPPORTUNITIES

- Case example 1: Within an investigation of a murder case law enforcement was unable to identify a murder based on search engine history. They were able to use search engine logs on the suspects computer to identify places he was interested in.



# SEARCHING FOR E-EVIDENCE

- Law enforcement is also in general prepared to identify computer systems and typical computer equipment
- Examples are desktop computer, screens, scanner



# SEIZING TRADITIONAL EVIDENCE

- Law enforcement is now prepared to deal with storage devices
- Typical storage devices are discs, CDs, DVDs



# CYBERCRIME

- Identifying storage devices can be difficult as the technology is developing so fast
- Storage devices are getting smaller and smaller and can be integrated in various tools



---

# HOW CYBERSECURITY ISSUES CHALLENGE EXISTING STRUCTURES



## COMPARING RW AND INTERNET

- When it comes to tangible goods such as books, guns and drugs they can only be brought into the country by physically moving them to the territory
- The same is relevant for anti-money laundering measures
- This does not only limit the ability of offenders to import/export such goods but also enables to implement control mechanism





# ENFORCEMENT

- To act in line with their mandates customs have means of control
- Example: X-Ray
- The x-ray allows customs to inspect check-in luggage without time consuming procedures of opening every bag
- The technology also allows customs to identify objects that that visitors bring into the country



# ENFORCEMENT

- Technology is constantly developing and enables customs to explore new ways of exercising their mandate
- One example is container security. X-ray allows to screen basically every container that comes into the country



# 3D PRINTER

- 3D printer allow the production of devices within a country that previously had to be imported
- New technology that will most likely become very popular in the coming years
- Princes already dropped below 5.000 USD



# 3D PRINTER - GUNS

- Recently there were several reports about plans/approaches to “print” a gun with a 3D printer
- Led to a controversial discussion about the technical possibility as well as legal considerations
- Some of the provider of templates for the “printing” of such guns removed them – however, there are concerns that even if the process of making available such templates they could widely be spread



# OPPORTUNITIES



# OPPORTUNITIES

- Availability of computer technology improved the ability of law enforcement to carry out investigations
- DNA sequence analysis and finger print databases are examples for an emerging use of information technology in traditional criminal investigation



# AUTOMATE

- Software tools are available to automate investigations
- Significant reduction of time for an investigation
- One example is the Software PERKEO that detects child pornography pictures on the basis of hash values



# AUTOMATE

- Automation techniques can also be used to identify copyright violations
- One example is file-sharing monitoring where software tools can automatically detect copies of copyright-protected art-work made available
- Another example is the automatic scanning of scientific work (like PhD)





# DEVICES PROCESSING DATA

- Devices do often store information that are valuable for traditional investigation
- The user do not necessary have knowledge about such operation
- One example is the iPhone that stored the geo-location of the user and thereby enabled the reconstruction of movements/travel



## DEVICES PROCESSING DATA

- In addition to “general” meta data the photos might include GPS data that shows where the photo was taken



## DEVICES PROCESSING DATA

- Criminals taking photos and placing them online might leave traces that can be used by law enforcement officers to identify them
- In addition to the “photo” graphic files might contain meta data
- Several camera models include the serial number of the camera in the meta data of each file



# TRACES

- “Nobody knows you are a dog” ?
- Internet users leave traces
- Access-Provider for example often for a certain period of time keep records to whom a dynamic IP-address was assigned



# AUTOMATE

- Example: If an offender is online and law enforcement is trying to identify him in real time anonymous communication systems might prevent the detection. However if law enforcement is able to get access to the cookies stored by the suspects browser they might be able to search for cookies stored during online banking. This could lead them to the suspect



## STORED DATA

- Even if the offender manages to delete evidence on his storage systems it might be possible to collect evidence at other sources
- One example: Archive.org maintains copies of websites



# CAPACITY BUILDING!!



# Understanding Cybercrime ITU

