




OECD International Academy for Tax Crime Investigation
Conducting Financial Investigations

 OECD

Computer Forensics: starting small

[the case of the Cyprus Tax Department]

Kyriacos IONAS
BSc, MSc, CFE, CFCE, EnCE, CAWFE
Republic of Cyprus
Tax Department
Tax Fraud Investigations Unit
Computer Forensics Lab






Disclaimer: Any opinions or views expressed in this presentation are my own and do not necessarily reflect the opinion(s) or view(s) of the Cyprus Tax Department.

Expected value gained?

- General knowledge
- Computers Forensics is “trendy”:
=> Opportunities? / Possibilities? / Ideas?
- Listen to a real example/case-study:
=> you could copy / avoid / customize.
- Ask questions

Credentials

CERTIFICATIONS AWARDED

Dec. 2018 – Dec. 2024	Certified Advanced Windows Forensic Examiner (CAWFE) International Association of Computer Investigative Specialists (IACIS) – Certificate ID: 15732	
Nov. 2017 – Nov. 2023	EnCase Certified Examiner (EnCE) – ID: 15-1117-7861 openText (formerly Guidance Software)	
April 2015 – Dec. 2024	Certified Forensic Computer Examiner (CFCE) International Association of Computer Investigative Specialists (IACIS) – Certificate ID: 15732	
July 2014 – July 2020	AccessData Certified Examiner (ACE) AccessData	
April 2014 – (no expiration)	Certified Fraud Examiner (CFE) Association of Certified Fraud Examiners (ACFE) – member no.: 654110	

“... a **confession** has for centuries been considered the “**queen of proofs**,” the most probative evidence one can have”.

<https://www.nytimes.com/2002/09/01/opinion/the-truth-about-confessions.html>

The New York Times



copyright (c) 1999 Daniel F. Simons. All rights reserved.

Count how many times, the players wearing white, pass the ball.

► <https://youtu.be/vJG698U2Mvo>

Outline

- 1. Computer Forensics
- 2. Cyprus Tax Department case study: *Starting small*

Footnote 1: DFL = Computer Forensics Lab
Footnote 2: CTD = Cyprus Tax Department

Poll:

Where is your organization regarding computer forensics?

1. Do nothing with digital information.
2. Collect digital evidence, no forensic experts
3. New DFL and dedicated forensic expert(s)
4. Seasoned DFL, experts, long experience
5. Cooperation with external DFL
(e.g. police DFL)

Overview

1. Computer Forensics
 - **What is Computer Forensics?**
 - First Responders
 - Digital Evidence Handling
2. Cyprus Tax Department case-study

Footnote 1: DFL = Computer Forensics Lab
Footnote 2: CTD = Cyprus Tax Department

"The word forensic comes
from the Latin **forēnsis**,
meaning
"of or before the forum"."

Etymology of the word "Forensics"

What is 'Digital Evidence'?

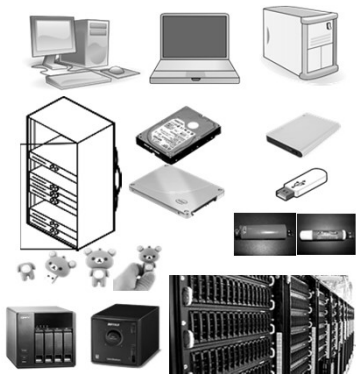
“Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.

This evidence is acquired when data or electronic devices are seized and secured for examination.”

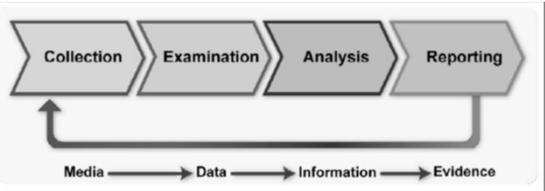
- National Institute of Justice (2008) *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*

Electronic Devices
Examples

- Personal Computer
- Laptop Computer
- Server Computer
- Rack server
- Hard Disk
- Solid State Drive (SSD)
- External Hard Disk
- USB Thumb Drive
- Network Access Storage (NAS)
- etc.



Four Phases Forensic Process



Source: Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-86.

Characteristics of Computer Forensics

▶ Completeness (of data):

◦ “With an IT Forensic tool we are sure to get all available information stored on any electronic media in the company.”

▶ Safety (during collection):

◦ “... using an IT Forensic tool is also a very safe way to collect information, for both the company and the tax administration.”

▶ Forensic value (of evidence):

◦ “... using an IT Forensic tools and methods gives the tax administration the proof that the information used in an audit did actually come from the company’s media and that we did not change anything when finding and examining the information.”

• S., J. and J. C. 2010. Use of IT Forensics in the Fight against Fraud. Tax Tribune:36-38

Characteristics of Computer Forensics

▶ Completeness (of data):

◦ “With an IT Forensic tool we are sure to get all available information stored on any electronic media in the company.”

▶ Safety (during collection):

◦ “... using an IT Forensic tool is also a very safe way to collect information, for both the company and the tax administration.”

▶ Forensic value (of evidence):

◦ “... using an IT Forensic tools and methods gives the tax administration the proof that the information used in an audit did actually come from the company’s media and that we did not change anything when finding and examining the information.”

• S., J. and J. C. 2010. Use of IT Forensics in the Fight against Fraud. Tax Tribune:36-38

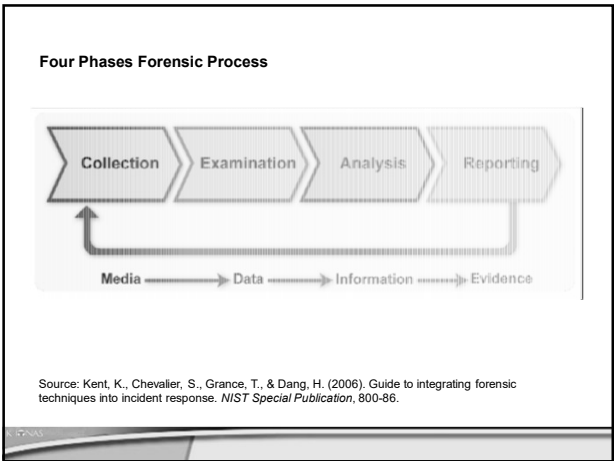
“Characteristics” good enough?

»» Let’s talk about

‘Collection’

of Digital Evidence

• S., J. and J. C. 2010. Use of IT Forensics in the Fight against Fraud. Tax Tribune:36-38



Collection procedures matters!!

»Evidence needs to be collected properly, because:

- The lawyers may attack the *evidence-collection-process*.
- Problems during collection means the e-evidence may not admissible.

Poll:
Who should be responsible for Collecting digital evidence?

1. Digital Forensic Unit personnel?
2. Specialised Investigators?
3. All Control Officers?
4. Specialised (National) Agency?


Overview

1. Computer Forensics
 - What is Computer Forensics?
 - **First Responders**
 - Digital Evidence Handling
2. Cyprus Tax Department case-study

Footnote 1: DFL = Computer Forensics Lab
Footnote 2: CTD = Cyprus Tax Department

Computer Forensics Principles\Rules

First Responder Guide:
The investigators 1st responder guide for the initial response to computer related incidents
by e-Crime Wales



First Responder Guide
The Investigators 1st responder guide for the initial response to computer related incidents

Source: PCeU (2010) First Responder guide: The investigators 1st responder guide for the initial response to computer related incidents

The principles of computer-based electronic evidence

“Don't change a bit, use your wit.”

► **Principle 1**

“No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.”

1	0	0	0
0	1	0	0
0	0	0	1
0	0	1	0


Source: PCeU (2010) First Responder guide: The investigators 1st responder guide for the initial response to computer related incidents

The principles of computer-based electronic evidence

“Know the works? Open the box.”

► **Principle 2**

“In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person **must be competent to do so** and be able to give evidence explaining the relevance and the implications of their actions.”




Source: PCeU (2010) First Responder guide: The investigator's 1st responder guide for the initial response to computer related incidents

The principles of computer-based electronic evidence

“Keep audit trail, or else you'll fail!”

► **Principle 3**

“An audit trail or other record of all **processes applied** to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.”



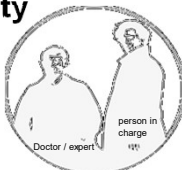
Source: PCeU (2010) First Responder guide: The investigator's 1st responder guide for the initial response to computer related incidents

The principles of computer-based electronic evidence

“Know the laws, YOU are the boss!”

► **Principle 4**

“The person in charge of the investigation [*the case officer*] **has overall responsibility** for ensuring that the law and these principles are adhered to.”







Source: PCeU (2010) First Responder guide: The investigator's 1st responder guide for the initial response to computer related incidents

Mnemonic method (R.E.S.P.E.C.T.)

- **R**econnaissance
- **E**ngage Digital Forensic Lab
- **S**ecure & Isolate
- **P**hotograph & Document
- **E**xamination / Interview Suspect
- **C**ollect & Identify evidence
- **T**ransport & Safeguard evidence

The principles of computer-based electronic evidence

   	<ul style="list-style-type: none"> ‣ Principle 1 – <i>Don't change a bit, use your wit.</i> ‣ Principle 2 – <i>¿Know the works? Open the box.</i> ‣ Principle 3 – <i>Keep audit trail... or else you'll fail!</i> ‣ Principle 4 – <i>Know the laws! YOU, are the boss!</i>
--	--

Source: PCeU (2010) First Responder guide: The investigator's 1st responder guide for the initial response to computer related incidents.



Evidence Collection & Preservation | Digital Evidence –
UCO Forensic Science Institute
published: June 8, 2015
by University of Central Oklahoma
Last viewed: 24/12/2021

‣ <https://youtu.be/rZ63OH2TAOo>

REPUBLIC OF CYPRUS

Better computer forensics for your countries:

How can you help each other?
Who can you bring together?
What resources can be shared?

»»» ▶ Break out rooms

(Relax and just talk)

استرخ وتحدث فقط

On the crime scene

»»» ▶ Digital Evidence
Collection & Handling

Words of caution.

Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition

“First responders without the proper training and skills should not attempt to explore the contents of or to recover information from a computer or other electronic device, other than to record what is visible on the display screen. **Do not press any keys or click the mouse.**”

† Mukasey et al. (2008) Electronic Crime Scene Investigation: A Guide for First Responders

Securing and Evaluating the Scene

Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition

Safety comes first!

▶“... primary consideration should be officer safety...”

▶“... compliance with departmental policy...”

McKasey et al. (2008) Electronic Crime Scene Investigation: A Guide for First Responders

Mnemonic method (R.E.S.S.P.E.C.T.)

▶Reconnaissance

▶Engage Digital Forensic Lab

▶Safety

▶Secure & Isolate

▶Examination / Interview Suspect

▶Collect & Identify evidence

▶Transport & Safeguard evidence

[Part 4] When We Left Earth - The Explorers

Published 9 months ago • 6 views • (O) PUBLIC DOMAIN

SPACE Cats

By stux

Privacy

Public

Category

Science & Technology

Licence

CC0 1.0

Language

English

Tags

documentary, NASA, space, When We Left Earth

Duration


49min 18sec

▶https://peertube.tv/w/1Qt5HPrrGaxhe5Gd9e1YLq

Mnemonic method (R.E.S.P.E.C.T.)

- **R**econnaisance
- **E**ngage Digital Forensic Lab
- **S**ecure & Isolate
- **P**hotograph & Document
- **E**xamination / Interview Suspect
- **C**ollect & Identify evidence
- **T**ransport & Safeguard evidence

**Unplug power to
router or
modem.**



Networked Home/Small Business Personal Computer(s)

First Responder Guide
The investigation of computer crime and the initial response to computer-related incidents

Securing the Scene

REPUBLIC OF CYPRUS

Source: PCeet (2016) First Responder guide- The investigation of computer crime and the initial response to computer-related incidents

“To Pull the Plug or Not to Pull the Plug, that Is the Question”

“I can picture a stressed out, overworked computer forensic technician on the phone with an on-scene responder, attempting to guide them through a proper shutdown and then a controlled boot process—prompting the following exchange:

-Responder: *It says to hit any key.*

-Forensic Tech: *Uh-huh.*

-Responder: *Hang on.... Um... where is the ‘any key’?*

-Forensic Tech: *You’ve got to be kidding me.... Just pull the @\$@#% plug, wrap it in tape, and bring it to me!”*

Source: Jack Wiles, Anthony Reyes (2007) The Best Damn Cybercrime and Digital Forensics Book Period. Your Guide to Digital Information Security, Incident Response, and Computer Forensics

Other useful instructions:

First Responder Guide

The investigator is expected to follow the initial response to computer related incidents

➤Consider the presence of legally privileged (LPP), special procedure or excluded material, when data is to be seized. If this is likely seek prosecutor advice.

➤As with any crime scene, isolate any suspect/equipment to prevent interference with potential evidence. This will include all parties present at the crime scene until their status is established.

➤If you reasonably believe that a particular device is involved in the crime you are investigating, take immediate steps to preserve the evidence, usually by having the person in control of it stop using it.

Source: IACB (2010) First Responder guide: The investigator's first response guide for the initial response to computer related incidents

Documenting the scene*

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

▶“The initial documentation of the scene should include a detailed record using video, **photography**, and **notes and sketches** to help recreate or convey the details of the scene later.”

Source: Mukasey et al. (2008) Electronic Crime Scene Investigation: A Guide for First Responders

Draft Blueprint

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

▶“... include the entire location, including the type, **location**, and **position of computers**”

▶“... persons of interest at the crime scene and **record their location**”

Manager
A
*1

Conference Room
*2

Server room
*3
*4

Reception
*5

*B *F

Legend:

A = Mr. David Cowle

1 = K101-00122-LC-20220121

Draft sketch / Not to scale

Source: Mukasey et al. (2008) Electronic Crime Scene Investigation: A Guide for First Responders



Evidence Collection & Preservation | Crime Scene Management Overview -
UCO Forensic Science Institute
Published: June 8, 2015
by University of Central Oklahoma
Last viewed: 24/12/2021


»<https://youtu.be/sFtM9s0UrIA>

REPUBLIC OF CYPRUS



First thing you do:
»Ask for the password!

REPUBLIC OF CYPRUS

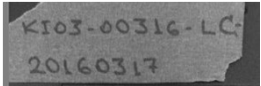


◦ Evidence stickers, labels, or tags.

REPUBLIC OF CYPRUS

↑ Mukasey et al. (2008) Electronic Crime Scene Investigation: A Guide for First Responders

Labeling seized evidence

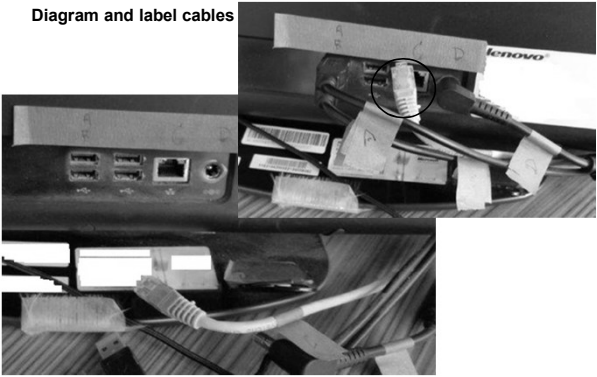


Case No.	KI##-CCYY-##-PN##-YYYYMMDDHHMM	Item Name	
Case No.		Item Name	

- ▶KI## → Kyriacos Ionas ##evidence seized.
- ▶CCYY→ CCC= case number, YY=year.
- ▶IN→ Item Name ie DC=desktop computer, LC=laptop computer, ..., UD=unknown device
- ▶PN →Part & No: ie HD=hard drive, TD=thumb drive, SD-SD card, UI=unknown item: **HD01, HD02**

Source: PCeU (2010) First Responder guide: The investigator's 1st responder guide for the initial response to computer related incidents.

Diagram and label cables



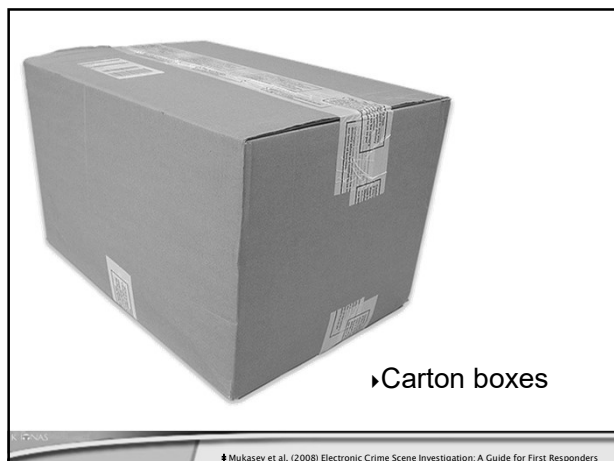
Source: PCeU (2010) First Responder guide: The investigator's 1st responder guide for the initial response to computer related incidents.



Antistatic Bag

◦ Antistatic bags

↑ Mukasey et al. (2008) Electronic Crime Scene Investigation: A Guide for First Responders



Transportation Procedures

When transporting e-evidence, ensure that-

- it's kept away from **magnetic fields**.
- it's not kept in a vehicle for **prolonged periods**.

© Mukasey et al. (2008) Electronic Crime Scene Investigation: A Guide for First Responders

*"All seized items will be correctly handled / packaged / exhibited / labelled and preserved with **continuity recorded during the movement and storage**, to maintain the integrity of the evidence."*

Chain of custody

Source:
PCeU (2010) First Responder guide: The investigators 1st responder guide for the initial response to computer related incidents

Source: PCeU (2010) First Responder guide: The investigators 1st responder guide for the initial response to computer related incidents

Sealed and signed packaging

•Signed by officer

•Signed by suspect

TEKMHPIO

VAT SE

U.K.
C&E 685A

HM Revenue & Customs – Digital Forensic Group

Property / Exhibit Label

Case

Seal Number

Label Reference

Description



containing the image(s) of
an exhibit identified as
received by the Digital Forensics Group under seal
reference and supporting
documentation

Signature

Date

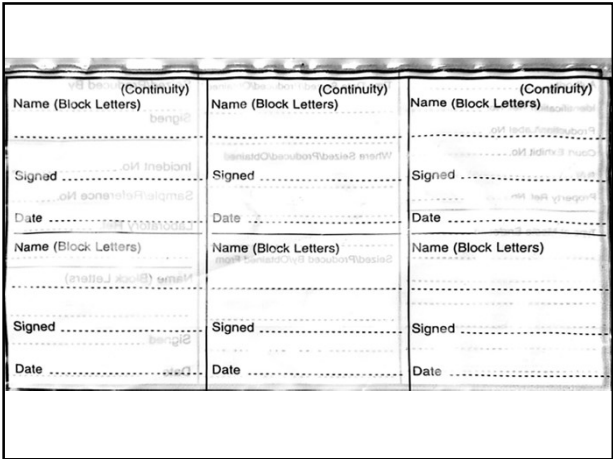
Time

Date	Officer/Witness	Old seal	New seal	Remarks
FOR COURT USE ONLY				
Court		Case		
Signature of Magistrate/Judge of the Peace/ Clerk of the Court		Exhibit No.		
Date				

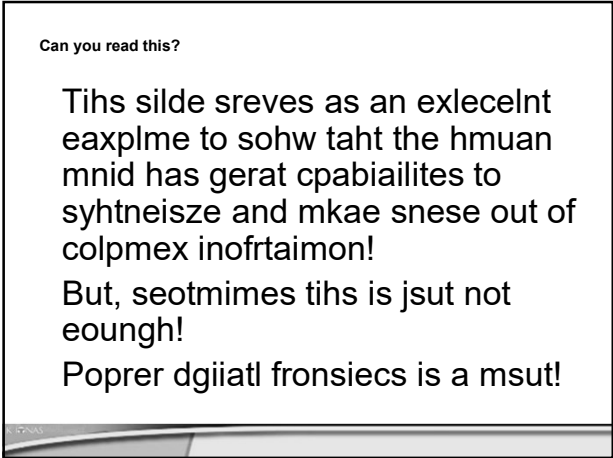
		CA04	
Exhibit Ref / Item Ref No:	Officer:	Search URN:	 HM Revenue & Customs
PF Ref/Book No:		Lab Ref No:	
Description of exhibit/item:			
I IDENTIFY THIS EXHIBIT AS THAT REFERRED TO IN MY STATEMENT Signature(s) of Person(s) Identifying Item:			
From Place/Person:		Signature of further Witness(es):	
Taken by:		Sealed by:	
Date:	Time:	Date:	Time:
Draft sketch / Not to scale Draft sketch / Not to scale			

Office:	Date:			FOR USE IN CENTRAL STORE
Name:				
Officers in case:	Name:	No:	Unit/Team:	
Office Ref:	Name: -----			
Central Store:	Location: -----			
DCIS Ref:	Store: -----			
Event URN/Item No.	-----			

Authority.....	Time/Date Seized/Produced/Obtained.....	Seized/Produced By.....
Identification Ref. No.....		Signed.....
Production/Label No.....	Where Seized/Produced/Obtained.....	Incident No.....
Court Exhibit No.....		Sample/Reference No.....
R. V.....		Laboratory Ref.....
Property Ref. No.....		Name (Block Letters).....
Type of Media Enclosed.....	Seized/Produced By/Obtained From.....	Signed.....
		Date.....







What percentage of financial fraud cases have a digital forensics element?

Does the COST of establishing/running a lab worth the BENEFIT?

»»» »Break out rooms

(Relax and just talk)

استرخ وتحدث فقط

A roadmap to the creation of a new Digital Forensic Lab

»»» »The case of
Cyprus Tax Department

«Training establishments have identified that the **ideal candidate** for a forensic analyst post, is that of a **keen and knowledgeable** amateur in computers with a thirst for the field and **previous investigative experience.**»

Personnel - Skill Profiles

» The Association of Chief Police Officer of England, Wales and Northern Ireland (2009)
ACPO Managers Guide: Good Practice and Advice Guide for Managers of e-Crime Investigations, p.8

CTD roadmap to a Digital Forensic Lab

- ▶2010:
 - Fiscalis "IT Forensic" in Copenhagen, Denmark
 - Suggestion to Management
- ▶2011:
 - Visit to DFL¹ of Cyprus Police
 - Visit to DFL¹ of Hellenic Police
 - Public announcement for our new DFL¹
- ▶2012:
 - Re-arranged an office, to use (part of it) as a Lab
- ▶2013:
 - Received Digital Forensic Tools for Lab

Footnote 1: DFL = Computer Forensics Lab

Crime scene photo (reliability)!



Year 2013

- ▶ 9th March 2013:
 - Received Server (IBM System x3500 M3)
- ▶ 13th March 2013:
 - Received Digital Forensic Software Tools and TD2
- ▶ 26-28 March 2013:
 - FISCALIS WV¹ "Cyprus' IT Forensic Unit"
- ▶ 1-4 July 2013:
 - Quick training by Police Academy
- ▶ 24th July 2013:
 - First case (in cooperation with the Police)

Footnote 1: WV = Working Visit

Main goals

- Collect data / information
- Collect e-evidence
(Forensically - look the part?)
- Minimise risk

© ITCNAT
Certain commercial entities, equipment, or materials may be identified in this document. Such identification is not intended to imply recommendation or endorsement by the presenter.

**Collect data / information
(examples)**

- emails with incriminating communication
- bank accounts numbers (undeclared funds)
- excel files (true sales / income)
- deleted Z-reports (temp files)
- Excel / Word invoices

© ITCNAT

**Collect data / information
(examples)**

- Business contacts / Suppliers / Clients
- Deciphering of documents
- Password recovery
- Virtualise suspect machine

© ITCNAT

Local Collaborations / Network

- Department of Information Technology Services (DITS)
 - Started the same project with us
- Cyprus Police
 - Electronic Data Forensic Lab

Education (for a Digital Forensic Analyst)

- Cyprus Police Academy
 - Electronic Data Forensic Lab
- FISCALIS
 - Computer Forensics Workshops & Working visits
- IOTA
 - Computer Forensics Seminar
- OLAF
 - Computer Forensics & Analysis Trainings
- Guidance & AccessData *(paid trainings)*
 - On-line trainings

International affiliations / memberships / co-operations / resources

<https://www.iota-tax.org/>

‣ **Intra-European Organisation of Tax Administrations**




International affiliations / memberships / co-operations / resources

https://ec.europa.eu/anti-fraud/contacts/general-enquiries_en

►OLAF Computer Forensics
& Analysis Trainings



European Commission
EUROPEAN ANTI-FRAUD OFFICE

European Commission > OLAF > Media corner > Press releases > OLAF organises digital forensics training

HOME INVESTIGATIONS POLICY OLAF AND YOU MEDIA CORNER ABOUT US


OLAF organises digital forensics training for
national anti-fraud investigators

21/09/2015

International affiliations / memberships / co-operations / resources

<https://www.nw3c.org/>

►National White Collar Crime Center




Agency Search Results

Agency Name	Address	Join Date
Republic of Cyprus Tax Department/Operations/Fraud & Investigations Unit	Paphos District Tax Office Paphos, 8011	10/21/2016

International affiliations / memberships / co-operations / resources

<https://www.swgde.org/home>

►Scientific Working Group on Digital
Evidence (SWGDE)



International affiliations / memberships / co-operations / resources

<https://www.nist.gov/programs-projects/digital-forensics>

► **U.S. National
Institute of
Standards and
Technology (NIST)**

International affiliations / memberships / co-operations / resources

<https://nij.ojp.gov/library/publications/electronic-crime-scene-investigation-guide-for-first-responders-second-edition>

► **U.S. Department
of Justice /
National Institute
of Justice (NIJ)**

Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition

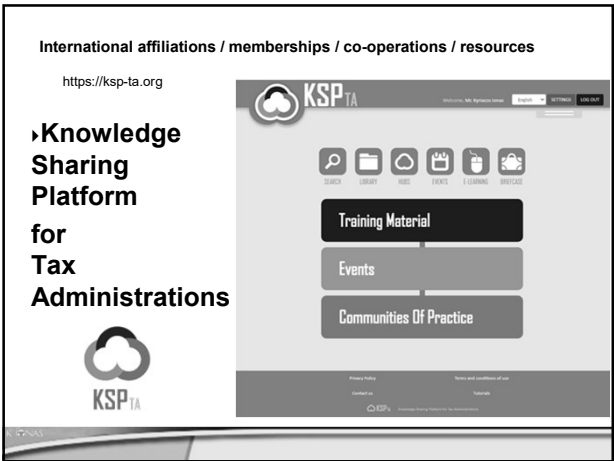
International affiliations / memberships / co-operations / resources

<https://www.ecrimewales.com>

**First Responder Guide:
The investigators 1st
responder guide for the
initial response to computer
related incidents**
by e-Crime Wales

First Responder Guide
The Investigators 1st responder guide for the initial response
to computer related incidents

Source: PCeU (2010) First Responder guide: The investigators 1st responder guide for the
initial response to computer related incidents







International affiliations / memberships / co-operations / resources

<https://sherloc.unodc.org/>

United Nations Office on Drugs and Crime

UNODC
SHERLQOC
SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME

The SHERLQOC portal is an initiative to facilitate the dissemination of information regarding the implementation of the United Nations Convention against Transnational Organized Crime, the Rome Protocol thereto and the International Legal Framework against Terrorism.

Hot Topics

- Electronic Evidence: This section on Electronic Evidence provides an overview of different types of resources (laws, jurisprudence, bibliographic materials, articles) as relevant to national and regional level to regulate the use and admissibility of electronic evidence in legal proceedings.
- Revised: This section to access the revised module used for the revision of the Convention for the Treatment of the Detention of the United Nations Convention against Transnational Organized Crime and the Protocol thereto.

Databases

- Case Law Database: A comprehensive case law database that allows you to see how Member States are handling cases related to organized crime and terrorism in their courts.
- Database of Legislation: An extensive repository of laws adopted by the governments of the United Nations Convention, the Protocol thereto and the International Legal Framework against Terrorism. Most of the legislation included in the database has been created specifically to counter the relevant crime type.
- CNA Directory: Directory of national authorities that have been designated to receive, respond and provide requests pertaining to mutual legal assistance, extradition and transfer of sentenced persons, cooperation of law enforcement.
- Bibliographic Database: An annotated bibliography providing synopses of key articles on organized crime and terrorism, searchable by countries, research methods and keywords.


UNODC
United Nations Office on Drugs and Crime

SHERLQOC
SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME

International affiliations / memberships / co-operations / resources

<https://www.youtube.com/c/SANSDigitalForensics>

SANS Digital Forensics and Incident Response YouTube Channel





SANS Digital Forensics and Incident Response
29.2K subscribers

SUBSCRIBED

International affiliations / memberships / co-operations / resources

League of Arab States

The power of networking.



Overview

1. Computer Forensics
2. Cyprus Tax Department case-study
 - Establishing a DFL¹ for CTD²
 - Main goals
 - Networking and Trainings
 - To start (small) or not to start?

Footnote 1: DFL = Computer Forensics Lab
Footnote 2: CTD = Cyprus Tax Department

Roles within a Laboratory

- **The Laboratory Manager**
 - Day to day running of the laboratory (i.e. job scheduling, HR management, quality management & review process, safety management etc)
- **Computer Forensics Examiner/Analyst**
 - User of the digital forensic tools and processes.
- **Case Investigator/Liaison**
 - Person who interfaces to the outside world.
- **Laboratory Technician**
 - Perform a set of basic laboratory tasks with regard to defined standards, procedures and metrics (i.e. imaging, duplicate)

Source: Andrew Jones, Craig Vaili (2011) Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility (pp 80-81)

Issues of a one-person Computer Forensics Lab

"one swallow doesn't make a summer" ☺

- **Difficulties in acquiring/achieving:**
 - diversified knowledge,
 - error-checking mechanisms,
 - standardisation (ISO status).
- **Risk of loosing a key player.**

Positives of starting a Computer Forensics Lab (even a small one)

"quality over quantity?"

► In-house know-how:

- Share knowledge internally
- New type of information/evidence, available to investigators regularly
- New 'forensic experts' can be identified
- Stay in touch with technological advances

Positives of starting a Computer Forensics Lab (even a small one)

"quality over quantity?" ☺

► **Allow business continuity:**

- Seizing electronic media can be avoided
- Focus on data / information (rather than storage media)

Positives of starting a Computer Forensics Lab (even a small one)

"quality over quantity?" ☺

► **Deterrent effect:**

- 'Surprise' suspects
- Give an impression of having advanced abilities

Positives of starting a Computer Forensics Lab (even a small one)


"quality over quantity?" ☺

► **Liaison with police:**

- Police help necessary for complex cases
- FEFs¹ no longer a 'black box'

Footnote 1: FEF = Forensic Evidence Files

Security Awareness (2021)
"2021 Security Awareness Report: Managing Human Cyber Risk"



»» **►Insight on best practice**

Having the Right People

►Strategic, long-term investment in self-motivated people

►You need 2.5 FTEs*
(relatively early on)

►Target number: a minimum of 3.5 FTEs*

* FTEs = Full-time Equivalents

Intuition:
SANS Security Awareness (2021) 2021 Security Awareness Report: Managing Human Cyber Risk

Demonstrate organisational commitment to the DFL


- ▶ Have at least one dedicated full-time person
- ▶ Provide the right title for that person
 - *Head Investigator in Digital Forensics Unit*
- ▶ Prepare a Mission Statement for your DFL
 - DFL's Mission statement
 - DFL's Targets

* DFL = Digital Forensics Lab

Intuition:
SANS Security Awareness (2021) 2021 Security Awareness Report: Managing Human Cyber Risk

It's not only about the personnel!

»» **You are not the Boss!**



Ensure leadership support


- ▶ Forensic capabilities is the norm?
 - *What are the others doing?*
- ▶ Create 'pressure' not to be last.
- ▶ Communicate benefits
 - Benefits to Tax Authority & suspect businesses

**A Digital Forensics project,
much like a pandemic,
is (sometimes) not managed easily at the beginning!**

»» A *cautionary* tale

Computer Forensics Principles\Rules

First Responder Guide:
*The investigators 1st
responder guide for the
initial response to computer
related incidents*
by e-Crime Wales

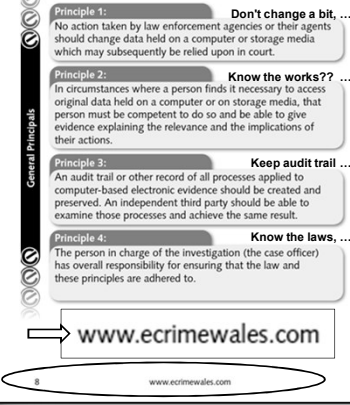


First Responder Guide
The Investigators 1st responder guide for the initial response to computer related incidents

Source: PCeU (2010) First Responder guide: The investigators 1st responder guide for the initial response to computer related incidents.

www.ecrimewales.com

e-Crime Wales is a partnership of organisations and agencies committed to equipping Welsh businesses with the knowledge and tools to be aware, vigilant, informed and ultimately safe from the destructive effects of e-Crime in all its forms.



General Principles

Principle 1: Don't change a bit, ...
No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

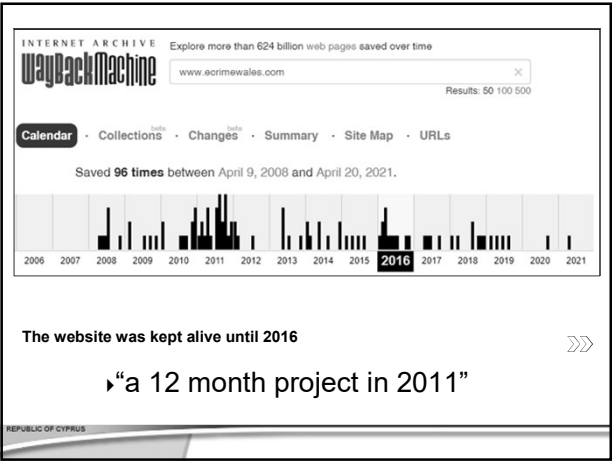
Principle 2: Know the works?? ...
In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

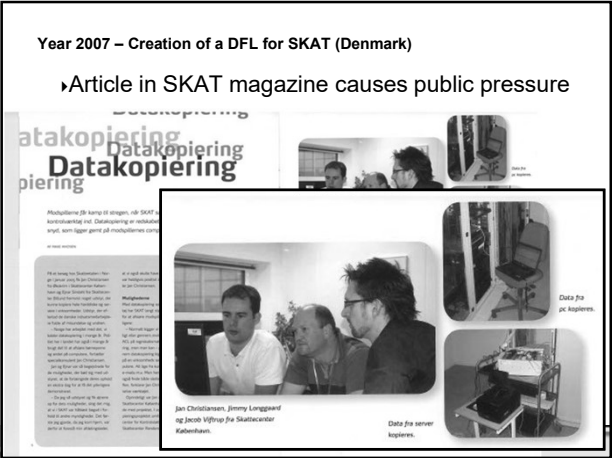
Principle 3: Keep audit trail ...
An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

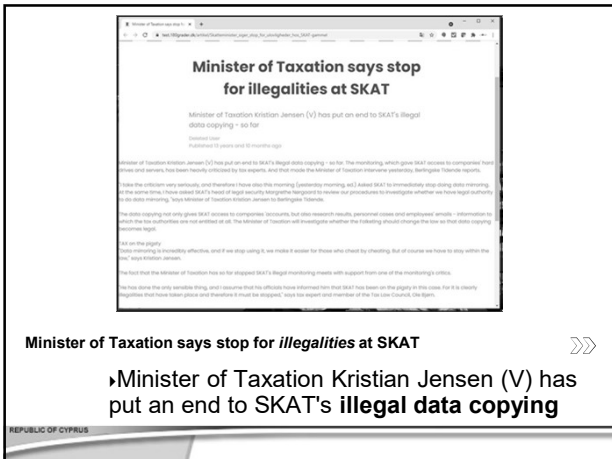
Principle 4: Know the laws, ...
The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

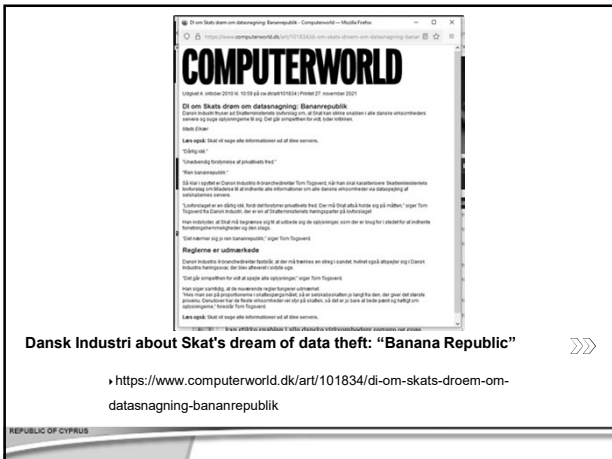
www.ecrimewales.com

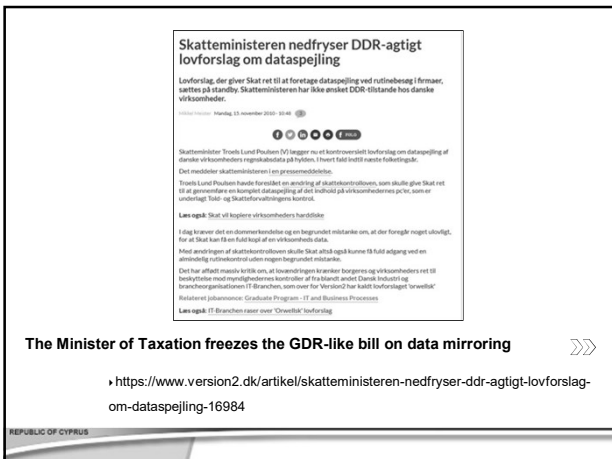


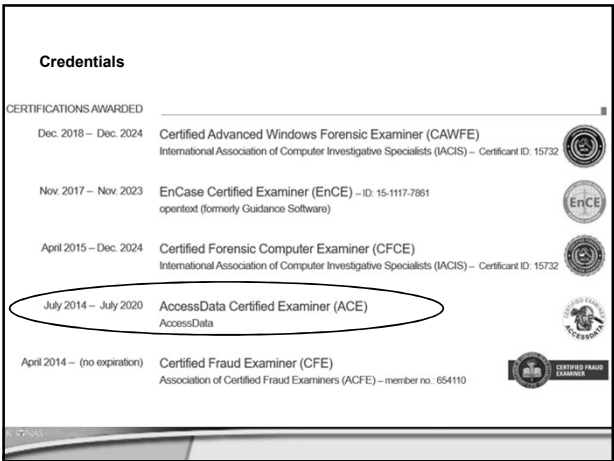


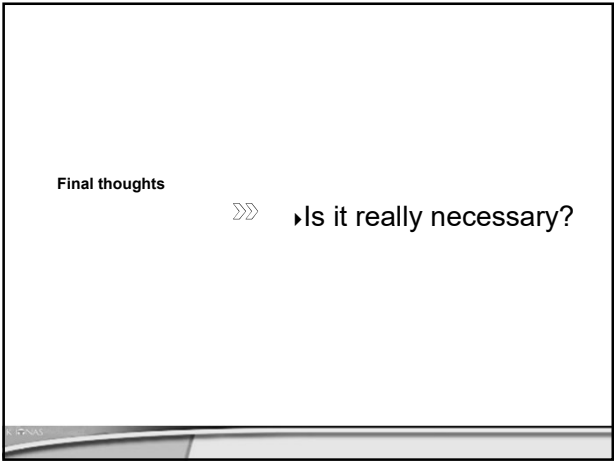


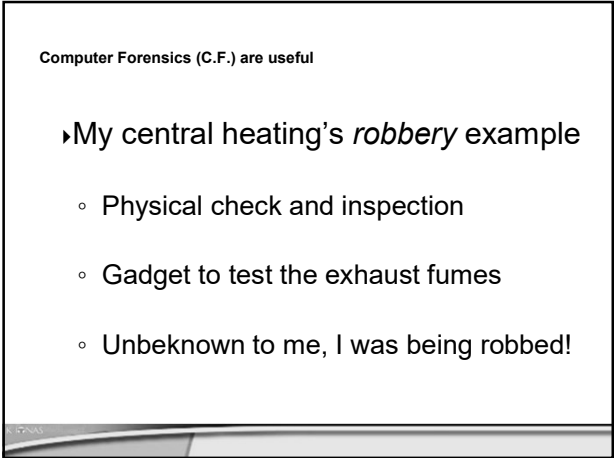













Computer Forensics (C.F.) are useful

- ▶Nevertheless:
- ▶C.F.: It's not panacea.
- ▶C.F.: It's only part of the equation
- ▶It's the whole 'equation' that brings home results



Count how many times, the players wearing white, pass the ball.

▶https://youtu.be/IGQmdoK_ZfY

Disclaimer: Any opinions or views expressed in this presentation is my own and does not necessarily reflect the opinion(s) or view(s) of the Cyprus Tax Department.

The handouts for this presentation will be available in

<https://preview.inwink.com/2022-january-italy-mena-academy/content/documents-and-articles>

Contact info:

Kyriacos Ionas
Computer Forensics Lab
Tax Fraud Investigations Unit
Cyprus Tax Department
Tel.: 00357 26 8043 26 – Fax: 00357 26 9493 91
E-mail: kionas@tax.mof.gov.cy
<http://www.mof.gov.cy/tax>

Personal / Social media:

cy.linkedin.com/in/kyriacosionas
