



University of  
Western Sydney

Bringing knowledge to life

# **Current Issues in Computer Forensics**

**Ewa Huebner**

**University of Western Sydney**

**Australia**

**[e.huebner@scm.uws.edu.au](mailto:e.huebner@scm.uws.edu.au)**

# Computer Forensics at UWS

## → Started in 2004

### → Teaching

- new subject: Computer Forensics Workshop
- new specialisation in Computer Forensics for the Bachelor of Computer Science degree
- project work in Computer Forensics at various levels

### → Research

- Formed the Computer Forensics Research Group
- exploring the field to identify areas suitable for further research and unresolved issues

<http://www.scm.uws.edu.au/compsci/computerforensics/>

# My research interests

## → Operating systems

- This is the area I worked in as a professional and researcher for most of my career
- My PhD thesis dealt with persistence in operating systems

## → Also computer architecture

- Mostly modern superpipelined superscalar microprocessors

## → Currently – Computer Forensics

- Techniques and methodology to solve, document and enable prosecution of computer crime.
- Computer crime is broadly understood as criminal acts in which a computer is **the object** of the offence or **the tool** for its commission.

# Computer Crime

## → Computer centred crime

→ criminal activity targeting computer systems, networks, storage media, or other computer devices (new technology facilitating a new class of crime)

## → Computer assisted crime

→ use of computer systems as tools to assist in a criminal activity where using computers is not strictly necessary (new ways to commit conventional crimes)

## → Incidental computer crime

→ criminal activity where using a computer system is incidental to the activity itself (new tools to replace conventional tools)

# A Broad Definition of Computer Forensics

- **gathering of evidence (often as part of a criminal investigation) from computers, computer networks, and other digital devices.**
  - actual files or the traces of a user's activities left in the activity logs of operating systems, browsers, databases, web proxies, network firewalls, etc., etc.
- **requires detailed technical knowledge of the relationship between:**
  - a computer's operating system, the supporting hardware, system/application programs, the network.
- **knowledge of cryptographic and steganographic techniques is needed where data has been encrypted and/or hidden**
- **evidence gathering must proceed in a manner that ensures**
  - that the evidence is admissible in a court of law,
  - and can be documented and presented in an intelligible manner.

# Another Definition

→ **Computer forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.**

R. McKemmish, 'What is Forensic Computing?' (Australian Institute of Criminology, 1999)

→ **Four key elements**

→ Identification

→ Preservation

→ Analysis

→ Presentation

→ **All activities have to be meticulously documented**

# Identification

- **Based on the conventional crime handbook approach**  
(The definitions are broad and not uniquely matched to a computing environment)
  - Secure and isolate
  - Record the scene
  - Conduct a systematic search for evidence

# Preservation

## → The aim

- Minimal handling of the original.
- Account for any change.
- Comply with the rules of evidence.

## → Methodology

- Chain of custody has to be maintained
- Bit-by-bit copies (images) are obtained with write blockers installed which prevent writing to the original disk
- All analysis conducted using copies (repeatability)

## → Tools

- Utilities - dd, hashing tools (MDA-5, SHA1, etc), etc.
- Open source - SleuthKit/Autopsy, Helix etc.
- Commercial - EnCase, ProDiscover, DataAccess, X-Ways etc.

# Analysis

## → Methodology

→ For disk images the analysis includes

- Logical structure (explicit content of media)
- unallocated space to discover deleted files, hidden data etc
- Also hidden areas on disk

→ System event logs are also analysed to determine how the system was used in the past

→ Any other data captured by live system investigation

## → Tools

→ Utilities - hex editors, e-discovery tools etc.

→ Software packages same as for preservation

# Presentation

- **The findings of an investigation are to be presented in court**
  - a CF expert has to convince lay people (lawyers, judges etc.) that the evidence presented proves that criminal activities took place and what was the nature of these activities.
  - Technical terms should be avoided and if used appropriately explained
  - It has to match the requirements of the local jurisdiction.
- **May take a form of a report**
  - Based on the documentation produced in the course of investigation

# Is it (computer) science?

## → Daubert test

- Is the evidence based on a testable theory or technique?
- Has the theory or technique been peer reviewed?
- In the case of a particular technique, does it have a known error rate and standards controlling its operation?
- Is the underlying science generally accepted?

## → This applies more generally to all forensic science

# Conventional computer forensics

## → **Seize the computer hardware**

- Turn power off, disconnect
- Transport to a forensic lab for analysis

## → **Focus on acquiring evidence**

- by making a physical copy of computer storage,
- typically by performing a disk-to-disk bit-by-bit copy,
- Analysis performed using the copy (not the original)

## → **To be admissible in court**

- Standard rules apply (may differ for different legal systems)
- Off-the-shelf commercial and freeware software
- Well established procedures and methodology

# New technological challenges (1)

- **Large capacity drives (1TB and higher) create practical issues**
  - copying data is slow, and searching acquired data takes even more time.
- **Data file systems used in computers**
  - allow for data to be hidden from a normal user,
  - and made visible only if specialised tools are used.
- **Properties and mechanisms of computer operating systems (and file systems)**
  - are not documented or poorly documented by their developers,
  - and some properties can be used to hide data.

## New technological challenges (2)

- **On-line storage (aka Internet storage or virtual hard drive)**
  - became more popular and accessible.
  - data of interest to a forensic investigator may not necessarily reside in the physical box in front of them.
  - Some providers offer free on-line storage
- **Storage virtualisation technologies**
  - data kept on storage devices physically at other locations,
  - possibly in another legal jurisdiction and country,
  - and can be used and accessed as if they were local.
- **It became easy to establish and maintain a web site**
  - which is physically located beyond local legal jurisdiction,
  - and cooperation of other countries legal systems can be slow, costly, and difficult.

## New technological challenges (3)

### → Data encryption algorithms

- became so good that breaking a password using a brute force attack method to access protected data is practically impossible.
- Strong encryption tools, which not so long ago had only limited distribution, are now available freely to anyone.

### → Small, easy to hide (or destroy) storage devices

- became common and inexpensive.
- By the end of 2006 USB flash drives reached capacities of up to 64GB (price now ~ US\$5000)

### → And so it goes ...

# Our research projects

## → NTFS file systems

## → Live investigation of computer systems

→ Memory forensics

→ Virtualisation in computer forensics

# NTFS file systems

## → Data hiding in NTFS file system

- an exhaustive study of data hiding in the NTFS file system (commonly used in all versions of Windows)
- and the limitations of the forensic tools used to discover such data.

*(topic of next week's seminar)*

## → Investigation of standard backup utilities

- in their treatment of some hidden data in NTFS.

*The results published in Digital Investigation The International Journal of Digital Forensics & Incident Response*

# Live system investigations

- **Order of Volatility - The expected life span of data (\*)**

Registers, processor cache, RAM in peripheral devices	nanoseconds
Main memory	10's nanoseconds
Network state	milliseconds
Active processes	seconds
disks	minutes
Floppies, backup media	years
CD-ROM, paper	10's years

} Live system

(\*) D Farmer, W Venema "Forensic Discovery" Addison-Wesley 2005

# Data collecting methodologies

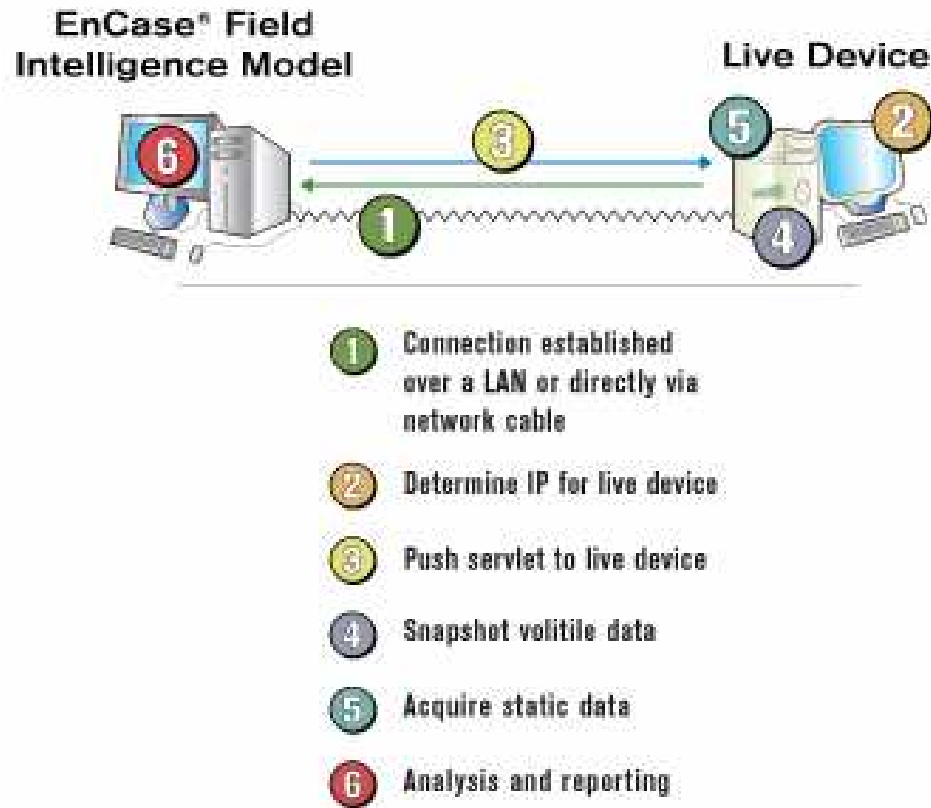
## → Forensic workstation connected to suspect system via TCP/IP network

- Use *netcat* or *cryptcat* to pipe output of commands run on suspect system to forensic workstation
  - Open source:
    - Mandiant First Response, see: <http://www.mandiant.com/>
    - The Forensic Server Project (TSP) by H. Carvey
  - Commercial tools provide module which installs an 'agent' on suspect system: ProDiscover, LiveWire Investigator, EnCase, (see the next slide)
- Requires network connection to the workstation collecting data, may not be forensically acceptable

## Data collection cont.

- **Run live agent-less data collection software on suspect system and output to external storage media like USB or FireWire disk**
- **Many commercial tools provide ‘live collection’ module,**
  - see for example X-Ways Capture (Win and Linux versions)
  - X-Ways warning: very small footprint, but if this is “not acceptable in the judiciary system you work in”, do not use it!

## Agent example: EnCase Field Intelligence Model



→ **Claims vs. reality:**

→ **“servlet” (or “agent”) needs to be installed on suspect system**

→ EnCase claim: *“non-intrusive, auto-updating, passive software agent”* is simply incorrect (but it sells!)

→ **BUT impact is unpredictable:**

→ A servlet itself is susceptible to attacks

→ A rootkit may be EnCase servlet aware (the most popular CF software!), and thus may trigger pre-programmed anti-forensics response

# Memory forensics

## → Potential of adding another dimension to the effectiveness of forensic investigation.

- Smaller volume than disk storage
- More difficult (if not impossible) to hide substantial volume of data
- More difficult to manipulate content
- Contains complete state of the system
- Some past events as well

## → Problem

- Analysis of physical memory not possible without disturbing its content
- Breaks (or stretches) the current rules of evidence

# Research in memory forensics

- **Measure the “forensic value” of memory**
  - What can be found in a memory dump
- **Find a way to obtain a complete and consistent memory dump**
  - without affecting its content
  - and to limit and control the disturbance to other evidence
- **Develop better software tools for forensic analysis of memory dumps**
  - Crash dump analysis tools cryptic and difficult to use
  - Analysis of memory content may give clues which can be confirmed by conventional analysis

# Persistence of data in memory

## → Content of memory

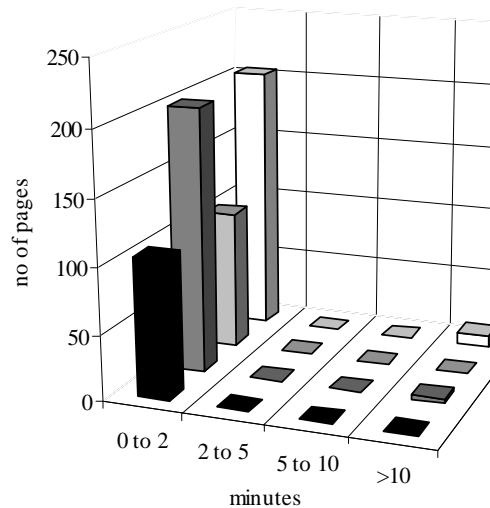
- Active processes address spaces (user and system)
- File block cache
- Unallocated page frames

## → Our study: longevity of user process data in physical memory

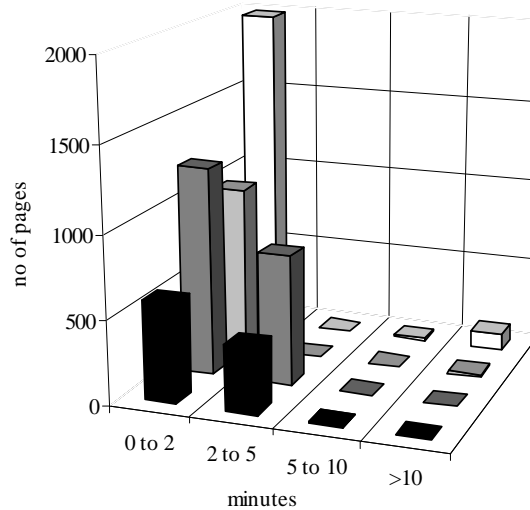
- experiments on Suse Linux and Windows XP systems
- to measure the age of pages we used an artificial load program which time-stamps data segment and block device cache pages.
- to compare the behaviour of both systems and to determine whether the rate of decay for user data depends on the demand for physical memory.

# Results

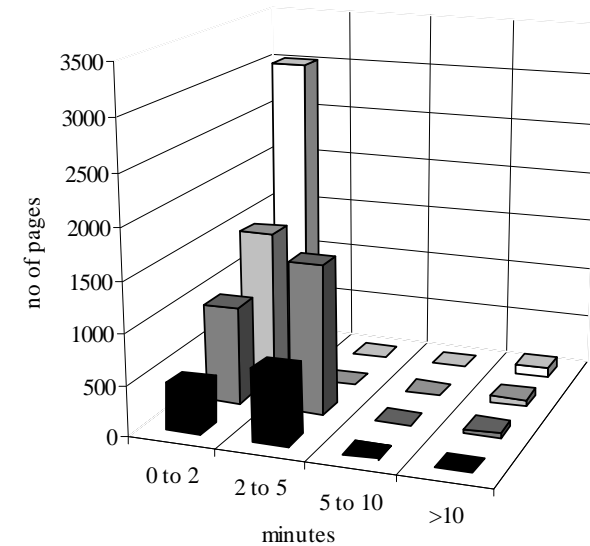
Light load



Heavy load



Very heavy load



■ Windows-Block Device Cache ■ Windows-Data Segment  
 □ Suse-Block Device Cache □ Suse-Data Segment

Windows and Linux systems preserve almost the same number of pages with user data, and the age distribution of these pages does not change significantly with the level of demand.

*The results published in Digital Investigation The International Journal of Digital Forensics & Incident Response*

# Future work in memory forensics (1)

## → Analysis of data longevity in memory and paging file of computer systems

- to determine the best practice in forensic investigations of volatile storage of computer systems
- with focus on encrypted data like files and passwords.
  - encrypted data resides in physical memory in clear text (unencrypted form) and afterwards it remains for some time in memory and paging file.
- Goal
  - measure how long such data persists under varied loads,
  - and how likely it is to be captured during investigation on mainstream platforms i.e. Windows and Unix.

## Future work in memory forensics (2)

### → Impact of operating system on forensic methodology

- with the focus on forensic acquisition and analysis of memory
- In theory OS could support such investigations both in terms of tools for analysis of data and by making the system data readily accessible for analysis.
- Conventional operating systems such as Windows and UNIX derivatives offer some memory-related tools
- Consider techniques developed for persistent operating systems, where lifetime of data is independent of the method of its creation and storage

*April 2008 special issue of ACM Operating Systems Review on  
Computer Forensics*

*(guest editors: Ewa Huebner & Frans Henskens)*

# ***ACM Operating Systems Review***

- Special Issue on Computer Forensics**
- Call for papers, deadline 1 December 2007**

Computer forensics practitioners and researchers are invited to contribute to this special issue of ACM OS Review by submitting papers presenting their original and unpublished work, which focuses on the relationship between operating systems and computer forensics.

<http://www.sigops.org/osr.html>

# Capturing memory

## → UNIX

- savecore command
- Available on most UNIX systems (not all flavours of Linux)
- Bypasses the file system
- Creates a vmcore file which can be analysed with crash utility
- UNIX memory device files
  - /dev/mem: mirror of the main memory
  - /dev/kmem: kernel virtual address space (contains main memory)

## → Windows

- 3rd party and Microsoft tools (not all in public domain)

## → Forensic flaws

- Dumping to a file system compromises original data
- Better use network as storage facility
- Whatever you do some parts of the system will be disturbed

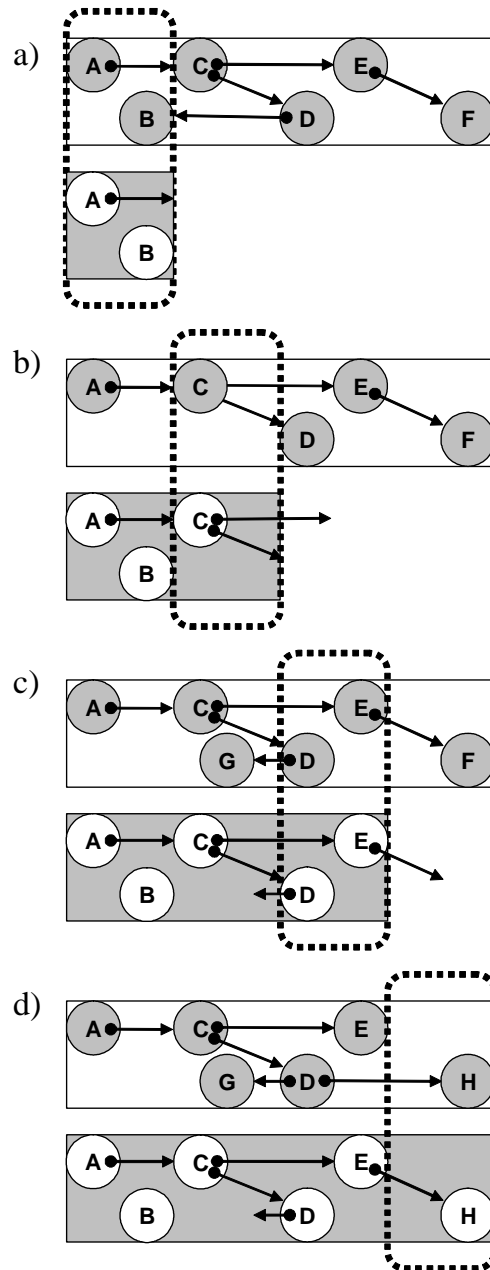
# Hardware assisted memory capture

- **Most trustworthy memory dump (in theory):**
  - If hardware assisted (using PCI card, FireWire interface, etc.).
- **PCI card “Tribble” (Carrier and Grand)**
  - See: B. Carrier and J. Grand, A Hardware-Based Memory Acquisition Procedure for Digital Investigations, Digital Investigations Journal, 1 (2004).
  - BUT: does it exist? Not a commercial tool - can not be purchased.
- **The Tribble card assumes that the system will be suspended while DMA (Direct Memory Access) transfer is in progress.**
  - BUT: not yet demonstrated that it is possible for the PCI controller to gain complete control over the CPU to stop it executing program code
  - DMA transfers are initiated by the CPU, and proceed in parallel with normal CPU activity, so such a 'stop the CPU' feature seems unlikely.

# Fundamental problem

**No known methodology  
which would guarantee that the acquired image of memory is a  
snapshot of memory content,  
rather it has been described as "memory smear".**

# Sequential nature of memory acquisition



→ A memory dump achieved in parallel with system execution is a technique that produces non-self-consistent data. Consider:

- a) Objects A and B are copied.
- b) Object B is deleted, object C is copied.
- c) Object G is created, objects D (with a pointer to object G) and object E (with a pointer to object F) are copied.
- d) Object F is deleted. Object H (pointed to by object D) is created. Object H is copied.

→ No mainstream OS provides a tool for capturing the complete and consistent state of the system.

# Virtual systems in CF methodology (1)

- **Computer systems are increasingly complex**
  - Analysis of their parts, like the disk or memory image, may not readily reveal all available information.
- **A new approach to computer forensics investigation**
  - Recreate the computer system and its immediate environment
  - by reproducing the collected images in a controlled way on similar or simulated hardware,
  - and observe the behaviour.
- **Again change the current mindset**
  - Investigation of a computer system to be viewed not as collecting evidence but as crime-scene investigation.

## Virtual systems in CF methodology (2)

### → potential to provide a valuable insight

- into the dynamic relationship of the investigated system with the outside computer networks and systems,
- as well as the specific setups and functions of the system itself
- Facilitate the discovery and interpretation of analogue data

### → We commenced a study

- to determine the methodology for virtual system investigation
- and to define its limitations.

# Our research in virtual systems (1)

## → Role of virtual environments in the analysis phase of computer forensics investigations.

- identified the limitations of virtual environments leading to the conclusion that virtual environments can not be considered as a replacement of conventional techniques of computer evidence collection.
- proposed a new approach where two environments, conventional and virtual, are used independently.
- demonstrated that this approach can considerably shorten time of the computer forensics investigations analysis phase and it also allows for better utilisation of less qualified personnel.

*The results accepted for publication in the International Journal of Digital Evidence*

## Our work in virtual systems (2)

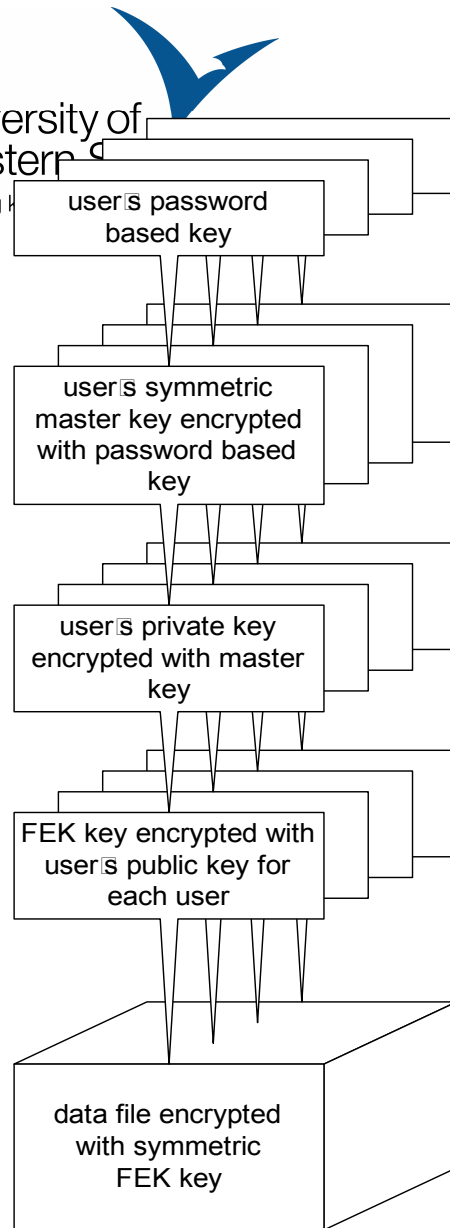
- **we continued research into applicability of two environments, conventional and virtual,**
  - this approach can be successfully used in the analysis phase of the computer forensics investigation of portable USB flash drives.
  - We also showed why virtualisation technique can complement but not completely replace conventional methods of computer evidence analysis.

*The results published in The Small Scale Digital Device Forensic Journal*

# Encrypted file systems

## → Using conventional methodology (bit-by-bit imaging)

- Encrypted files are practically impossible to decrypt without knowing the key and the method of encryption.
- The Windows operating system provides the option to encrypt files using an encryption driver bundled with the NTFS file system, the so called Encrypting File System (EFS).
- EFS files can be manipulated transparently by the owner and the system administrator as long as they reside in an NTFS file system.



## EFS encryption

1. File encrypted with a symmetric file encryption key (FEK) using one of the Data Encryption Standard algorithms depending on the version of the Windows system
2. FEK encrypted with a public key, using the asymmetric RSA algorithm for every user with permission to access the file; FEK keys cannot be decrypted without producing a private key for one of the legitimate users of the file.
3. Windows stores the private keys in the subfolder RSA of a users' profile directory. For each user this directory is further encrypted with a random symmetric master key, held in another subfolder named Protect.
4. Finally the Protect subfolder is encrypted using a key created from the user's password.

# Our research into dealing with encryption

- **we demonstrated the methodology of extracting EFS decrypted files from a live system.**
  - software utility: Robocopy (Robust File Copy Utility, a free utility available from Microsoft), which does not modify any metadata of the file system during extraction.
  - The proof is based on hash values calculated before and after the acquisition
  - The image is taken from NTFS source to a non-NTFS destination and automatically decrypted
  - with conventional methods (bit-by-bit copy) the files would remain encrypted
    - even when supplemented by the capture and analysis of physical memory.

*Accepted for publication in the Journal of Digital Forensic Practice.*

# Future work

## → **Memory forensics**

- Study longevity of memory and paging file content
- Supplement mainstream OS's to facilitate memory acquisition and analysis

## → **Virtual environments**

- Continued work on forensic application
- Investigation of protected USB U3 devices

## → **Dealing with protected data**

- by steganography and cryptography