Your Connection to ICT Research

Digital Investigations & Forensics Analysis

Practices and Technologies

Syed Naqvi, PhD

Syed.Naqvi@cetic.be

The Sixth International Conference on Digital Society (ICDS 2012)
Valencia, Spain – 30 January 2012

Introduction

Stages of IT Security

- **Attack prevention**

  Pre-incidence measures

  Access control, security policy, intrusion detection, …

- **Attack tolerance**

  During-incidence measures

  Honeypots, intrusion tolerance, sabotage tolerance, …

- **Attack aftermath**

  Post-incidence measures

  CERT, forensics analysis, …

Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- E-mail Updates
- News Feeds

Be Crime Smart
- Wanted by the FBI
- More Protections

Use Our Resources
- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Headline Archives

CYBER BANKING FRAUD
Global Partnerships Lead to Major Arrests

10/01/10

Members of the theft ring managed to steal $70 million. **View: Wanted poster of suspects**.

The cyber thieves were smart. Instead of targeting corporations and large banks that had state-of-the-art online security, they went after the accounts of medium-sized companies, towns, and even churches. Before they were caught, members of the theft ring managed to steal $70 million.


CRIME SCENE-DO NOT ENTER

FORENSICS - Ground situation

Over 85% of cases prosecuted involve digital evidence

Meadaris, K., "Grants to help develop ways to improve digital evidence collection", Purdue University, October 2006.

50% of all cases handled by the FBI to involve at least one computer forensic examination

Scott L. Ksander, "Issues of Privacy and Information Security", Ackerman Colloquium on Technology & Citizenship Education, July 2007

Global digital-forensics market is estimated to be $1.8 billion by 2011 (~ 1/3 of this market share will come from US)

PC Pro Magazine - 21 Jan 2010

http://www.pcpro.co.uk/news/260227/dell-delves-into-digital-detective-work

cetic
Your Connection to ICT Research

Digital Forensics in Businesses

Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program

By Douglas Barbin, CISSP, CPA, CFE, and John Patzakis

Imagine restricting an internal company audit or investigation to allow the review of only 10 percent of all documents relevant to that investigation. As recent university studies reveal,1 more than 90 percent of all information is now created in digital form. Therefore, when company auditors ignore computer evidence, they essentially limit themselves to 10 percent of the available information. For this reason, the burgeoning practice of computer forensics has become synonymous with computer investigations and audits.

Computer forensics is the collection, preservation, analysis and court presentation of computer-related evidence. In addition to civil and criminal jury trials, computer evidence often is presented in arbitration, administrative and mediation proceedings, congressional/government hearings and presentations to corporate management. Accordingly, the proper collection and analysis of computer evidence through accepted computer forensic protocols is a critical component to any internal investigation or audit where the results have at least the potential to be presented in legal proceedings.

Computer forensics ensures the preservation and authentication of computer data, which are fragile by nature and easily can be altered, erased or subject to claims of tampering without proper

Digital Forensics

Definition – Digital Forensics Science

- Forensic science is the application of natural science to matters of law
- Forensic science seeks to find the root cause of an event
- "To be considered a discipline, Digital Forensic Science must be characterized by the following associated entities:
  - Theory: *a body of statements and principles that attempts to explain how things work*
  - Abstractions and models: *considerations beyond the obvious, factual, or observed*
  - Elements of practice: *related technologies, tools, and methods*
  - Corpus of literature and professional practice
  - Confidence and trust in results: *usefulness and purpose*
- The current state of Digital Forensic Science exhibits only some of these characteristics and they are not tied to specific disciplinary practices considered by any group as scientifically rigorous."*

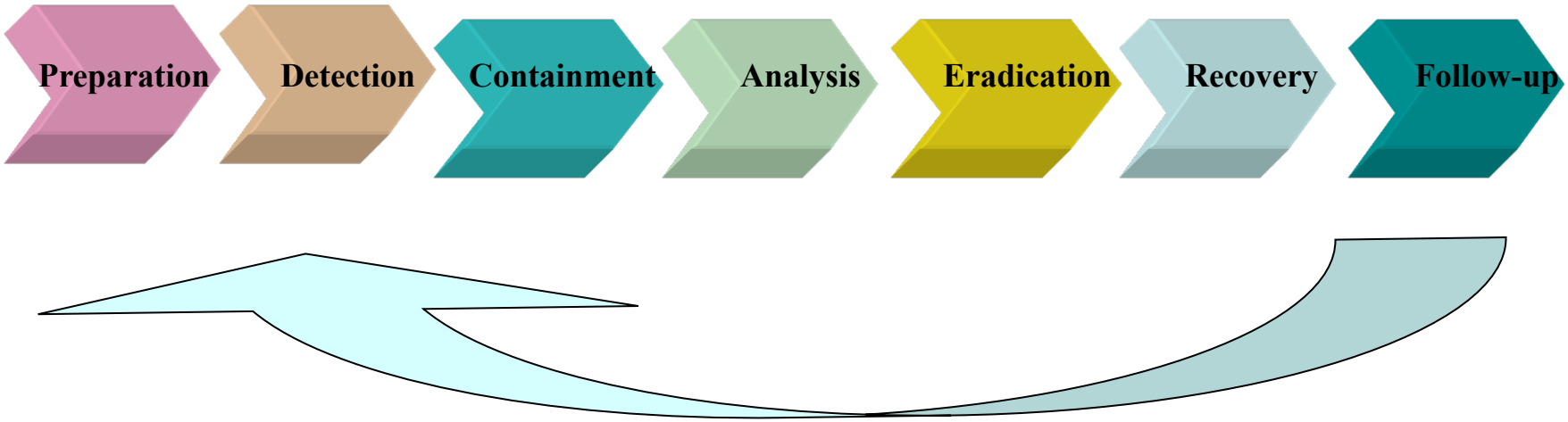
* Source: "A Road Map for Digital Forensic Research" 6th November 2001, The Digital Forensic Research Work Shop

Definition - Digital Forensics Practice

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

Source: "A Road Map for Digital Forensic Research" 6th November 2001, The Digital Forensic Research Work Shop

Digital Forensics Events Management



cetic
Your Connection to ICT Research

An Example of Forensic Investigation

- **Identification**
  - Call received
- **Preservation**
  - Case file opened
  - Server imaged
    - Image in chain of custody
  - Server logs preserved
  - Entry in case file
- **Collection**
  - SafeBack used
  - Policies reviewed for authority to proceed
- Began interviews
- Event described
  - Unavailable mortgage database
  - Server checked: db gone
  - Observed action by admin including remote login
  - Restore from backup unsuccessful – data bad
- Entry in case file

Source: "A New Approach to Complex Digital Investigations" by Peter Stephenson, 2003

An Example of Forensic Investigation

- **Examination**
  - Data recovered from server drive
    - Database deleted and partially overwritten
    - Placed in chain of custody
    - Entry in case file
  - Data recovered from server logs
    - Login by admin from a network connection
      - Gateway address
      - Attack PC address and name
    - Placed in chain of custody
    - Entry in case file
  - Data recovered from gateway logs
    - Time & date of access to gateway by attack PC
    - IP address of attack PC
    - Entry in case file
    - Placed in chain of custody

Source: "A New Approach to Complex Digital Investigations" by Peter Stephenson, 2003

An Example of Forensic Investigation

- **Examination cont.**
  - Data recovered from attack PC
    - SafeBack used
    - Placed in chain of custody
    - Policies reviewed for authority to proceed
    - Login info re: victim recovered
    - Authentication data for victim recovered
    - Attack PC username recovered: suspect identified
    - Suspect logged in at time of event
    - Entry in case file

Source: “A New Approach to Complex Digital Investigations” by Peter Stephenson, 2003

An Example of Forensic Investigation

- **Examination cont.**
  - Data recovered from floor swipe card access log
  - Placed in chain of custody
  - Entry in case file
  - Witness interviews
    - Co-workers in physical proximity place suspect at desk within 1 hour of event
    - Supervisors places suspect at desk within 3 minutes of event
  - Entry in case file
- **Analysis**
  - Timeline of events created
  - Evidence linked and traceability established
  - Entry in case file

Source: "A New Approach to Complex Digital Investigations" by Peter Stephenson, 2003

An Example of Forensic Investigation

Presentation

- Timeline and chain of evidence documented in final report
- Suspect interviewed and presented with conclusions and evidence
- Entry in case file

- **Decision**
  - Suspect confesses
- **END**

Source: “A New Approach to Complex Digital Investigations” by Peter Stephenson, 2003

Formal Expression

Digital Investigation Process Language

- Started with the Common Intrusion Specification Language (CISL)
  - Derived from LISP
    - Formal language proven using the Lambda Calculus
  - A “language that can be used to disseminate event records, analysis results, and countermeasure directives amongst intrusion detection and response components.”
    - Found by Doyle at MIT to be inadequate for that task - however, offers a very rich language for forensic digital analysis
      - Still requires some extensions

Source: “A Common Intrusion Specification Language (CISL)” Feiertag, et al, last revised 11 June 1999

Developing the Process Language

- CISL structure
  - S-expressions
    - Data structure developed by Rivest in 1997 that is "…suitable for representing arbitrary complex data structures." (Rivest, S-Expressions, 4 May 1997)
    - May be byte strings or lists of simpler S-expressions
  - Semantic Identifiers (SIDs)
    - Tags added at the beginning of an S-expression that give a semantic clue to the interpretation of the rest of the S-expression
      - Verb SIDs
      - Role SIDS
      - Atom SIDS
      - Conjunction SIDs
      - Referent SIDs

Source: "A Common Intrusion Specification Language (CISL)" Feiertag, et al, last revised 11 June 1999

Typical CISL S-Expression

```
(OpenApplicationSession
  (When
    (Time 14:57:36  24 Feb 1998)
  )
  (Initiator
    (HostName 'big.evil.com')
  )
  (Account
    (UserName 'joe')
    (RealName 'Joe Cool')
    (HostName 'ten.ada.net')
  )
  (Receiver
    (standardTCPPort 23)
  )
)
```

Interpretation

At 14:57:36 on 24 Feb 1998, someone at big.evil.com opened a telnet session on ten.ada.net logging in as username: joe, real name: Joe Cool.

Source: "A Common Intrusion Specification Language (CISL)" Feiertag, et al, last revised 11 June 1999

Fragment of Earlier Example Expressed in DIPL

Identification

Call received

```
(And
  (Report
    (Initiator
      (RealName 'Joe Operator')
    )
    (Observer
      (RealName 'Peter Stephenson')
    )
    (AttackNickName 'access denied to a file or object')
    (FileName 'Mortages.db')
    (Target
      (HostName 'Server1')
    )
  )
```

Source: "A New Approach to Complex Digital Investigations" by Peter Stephenson, 2003

Fragment of Earlier Example Expressed in DIPL

Preservation

- Case file opened
- Server imaged
  - Image in chain of custody
- Server logs preserved
- Entries in case file

```
(ManageCase
  (Initiator
    (RealName 'Peter Stephenson')
  )
  (CaseName 'Case123')
  (BeginTime 16:35 1 Jan 1998)
)
(Image
  (Initiator
    (RealName 'Peter Stephenson')
  )
  (Tool
    (ProgramName 'SafeBack')
    (VersionNumber '3.0')
  (
  (BeginTime 17:00 1 Jan 1998)
 (EndTime 20:14 1 Jan 1998)
  (Target
    (HostName 'Server1')
  )
  (ReferAs 0x12345678)
```

Source: "A New Approach to Complex Digital Investigations" by Peter Stephenson, 2003

Fragment of Earlier Example Expressed in DIPL

Preservation

Server logs preserved

```
(PreserveCustody
  (Evidence
    (ReferTo 0x12345678)
  )
)
(ManageCase
  (Initiator
    (RealName 'Peter Stephenson')
  )
  (CaseName 'Case123')
  (BeginTime 20:25 1 Jan 1998)
)
)
(ExtractData
  (Evidence
    (FileName 'server.log')
    (ReferAs 0x87654321)
  )
  (Target
    (ReferTo 0x12345678)
  )
  (PreserveCustody
    (Evidence
      (ReferTo 0x87654321)
    (BeginTime 20:45 1 Jan 1998)
    )
)
```

Fragment of Earlier Example Expressed in DIPL

Collection
Entry in case file
SafeBack used

```
(ManageCase
    (Initiator
      (RealName 'Peter Stephenson')
    )
    (CaseName 'Case123')
    (BeginTime 21:05 1 Jan 1998)
  )
(TraceAuthority
  (ApprovedSoftware
    (Tool
      (ProgramName 'SafeBack')
      (VersionNumber '3.0')
    )
    (Citation
      (CaseName 'joe v volcano')
    )
  )
```

Source: "A New Approach to Complex Digital Investigations" by Peter Stephenson, 2003

Fragment of Earlier Example Expressed in DIPL

Collection

Policies reviewed for authority to proceed

```
(ApprovedMethod
    (Certification
      (Certifier
        (RealName 'NTI')
      (CertType 'NTI Training')
      (CertNumber 'Course 1-1-95')
      (Observer
        (RealName 'Peter Stephenson')
      )
    )
  )
(Policy
    (PolicyName 'Information Privacy Policy')
    (PolicyDate '1 Jan 1990')
    (Observer
      (RealName 'Peter Stephenson')
    )
  )
```

Fragment of Earlier Example Expressed in DIPL

Collection

Entry in case file

Conduct interviews

```
(ManageCase
  (Initiator
    (RealName ‘Peter Stephenson’)
  )
  (CaseName ‘Case123’)
  (BeginTime 21:05 1 Jan 1998)
)
)
(Interview
  (Initiator
    (RealName ‘Peter Stephenson’)
  )
  (Subject
    (RealName ‘Jane Sneaker’)
  )
  (BeginTIme 08:30 2 Jan 1998)
  (EndTime 10:45 2 Jan 1998)
 (ManageCase
    (Initiator
      (RealName ‘Peter Stephenson’)
    )
    (CaseName ‘Case123’)
    (BeginTime 21:05 1 Jan 1998)
  )
)
```

cetic
Your Connection to ICT Research

Benefits of the Formal Approach

- Describes a repeatable digital forensic process in a structured manner
- Allows independent analysis and verification of a forensic investigation including the interpretation of the attack process
- Formally documents the total investigative process
  - Pre-attack activities
    - As interpreted by the investigator
  - Investigative process
  - Attack activities
    - As interpreted by the investigator
  - Post-attack activities
    - As interpreted by the investigator
  - Documentation, evidence management, procedural issues
- Allows verification of the investigative process during the investigation and may help suggest ways to plug holes in the EEDI process
  - Gaps in the chain of evidence
- May be fed into a model checker for formal modeling of the process

Source: "A New Approach to Complex Digital Investigations" by Peter Stephenson, 2003

Analysis Technologies

cetic
Your Connection to ICT Research

Digital Forensics Tools

- Depending on the scope and requirements of the digital forensics analysis, a number of tools are used for each specific analysis. Most common features are:
  - Disk copying/imaging tools for copying the contents of hard and removable storage media drives.
  - Data recovery tools for restoring deleted data items.
  - Search and analysis tools for analyzing data under examination so as to locate specific content or event.

- Some commonly available tools are described in the following slides.
  - This is a non-exhaustive list of the available tools
  - No commercial interest is involved in the selection of these tools!

DIGITAL INTELLIGENCE

17165 W. Glendale Drive
New Berlin, WI 53151
866-DIGINTEL (866-344-4683)
Outside the US: 262-782-3332

www.DigitalIntelligence.com

DRIVESPY is a forensic DOS shell. It is designed to emulate and extend the capabilities of DOS to meet forensic needs.

Commercial Customers $249.95 ORDER
SKU: S1000

Law Enforcement Personnel / Agencies $199.95 ORDER
SKU: S1050

About DriveSpy

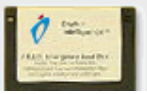
THIS PROGRAM IS A DOS APPLICATION THAT WILL NOT FUNCTION IN WINDOWS

Whenever appropriate, DRIVESPY will use familiar DOS commands (CD, DIR, etc) to navigate the system under investigation. When beneficial, DRIVESPY will extend the capabilities of the associated DOS commands, or add new commands as necessary. DRIVESPY provides a familiar DOS-like prompt during system navigation. (DRIVESPY does not use drive letters in the prompt, but rather a Drive/Part combination (i.e "D0P1:\WINDOWS\SYSTEM") to eliminate confusion in the event where the resident operating system has not assigned a drive letter to the drive being processed (i.e examining a FAT32 partition under DOS 6.22)).

SC MAGAZINE RECOMMENDED

04/13/01 - SC Magazine's testing of Forensic Software identifies DRIVESPY as the ONLY product reviewed which found ALL the hidden information in their test suite. This included forensic software products costing almost 10 times as much as DRIVESPY!

DriveSpy Processes



- Large Hard Drives (Greater than 8.4 Gb)

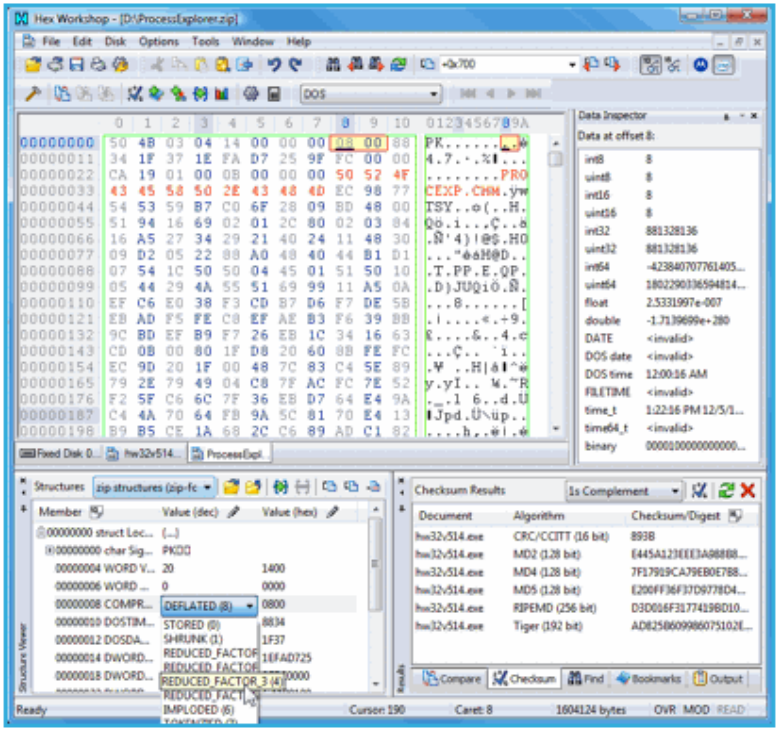
BREAKPOINT SOFTWARE

486F 6D65 206F 6620 7468 6520 4865 7820 576F Home of the Hex Wo
726B 7368 6F70 2048 6578 2045 6469 746F 7200 rkshop Hex Editor.

Hex Workshop

Awards & Reviews

The Hex Workshop Hex Editor by BreakPoint Software is a complete set of hexadecimal development tools for Microsoft Windows 2000 and later. Hex Workshop combines advanced binary editing and data interpretation with the ease and flexibility of a modern word processor. With the Hex Workshop, you can edit, cut, copy, paste, insert, fill and delete binary data. You can also work with data in its native structure and data types using our integrated structure view and smart bookmarks. Data editing is quick and easy with our extensive features that allow you to: jump to file or sector location, find or replace data, perform arithmetic and logical operations, binary compare files, generate checksums and digests, view character distributions and export data to RTF or HTML for publishing.



Click to enlarge

SNAPBACK
TRUE IMAGE BACKUP

true image backup

Home / Register / Products / OEM / Purchase / Downloads / Support / Resellers / Company / My SnapBack

You are not logged in
Username
Password
Login Forgotten Password?
Create account

Up and running in 3 minutes !

Isn't it crazy to know that you have a current backup but it's going to take you nearly two days to get up and running again? SnapBack backups can be restored by a total novice in just a few minutes.

SnapBack® Exact is a server-based backup and restore program for Windows servers that features full open file management, remote administration and backup scheduling. It copies an actual byte-by-byte True Image® copy of the server hard drives to tape while the backup is running and files are open and being modified. With TapeDisk you can restore single files as easy as copying files from a CD-Rom and with the simple Disaster Recovery Disk you can be up and running again in minutes.
more >>

---

latestnews

16th August 2007
SNAPBACK EXACT 5.20b RELEASED
A point release of SnapBack Exact has been released - 5.20b. This version fixes a compatibility issue with Windows 2003 Server and is a strongly recommended upgrade. **Read the Release Notes**

more >>

20th March 2006
SNAPBACK EXACT 5.20a RELEASED
A major new version of SnapBack has been released - 5.20a.

It is fully compatible with Windows 2003 as well as XP and 2000.

Read the Release Notes

Secure Computing Magazine Said -

"SnapBack Live! is our other Recommended product, which again convinced us that it may provide that little bit of extra appeal from the administrator's point of view."

EnCase® Forensic

Unsurpassed Digital Data Collection and Analysis

From the simplest requirements to the most complex, EnCase® Forensic is the premier computer forensic application on the market. It gives investigators the ability to image a drive and preserve it in a forensic manner using the EnCase evidence file format (LEF or E01), a digital evidence container validated and approved by courts worldwide.

EnCase Forensic also contains a full suite of analysis, bookmarking and reporting features. Guidance Software and third party vendors provide support for expanded capabilities to ensure that forensic examiners have the most comprehensive set of utilities.

Key Benefits & Features

Key Benefits

- Unsurpassed court acceptance
- Recognized worldwide as the de facto standard for computer forensics
- Analyze target machines at a deeper level

Key Features

- Advanced search options
- Internet and email support
- Court validated Logical Evidence File format
- Multiple viewers

RESOURCES

Brochures

EnCase® Forensic Total Offering (PDF)
EnCase® Forensic for Law Enforcement (PDF)
EnCase® Forensic Features (PDF)
More Brochures

Whitepapers

Restore Validation (PDF)
Fastbloc® Validation (PDF)
More Whitepapers
Request a Quote

FORENSIC FAMILY
BUNDLED SOLUTIONS
MODULES AND ADD-ONS
DEMO
WEBINARS
EVENTS
SOLUTIONS
TRAINING

R-Tools Technology Inc.

R-Tools Technology Inc. is the leading provider of powerful data recovery, undelete, drive image, data security and PC privacy utilities for the Windows OS family. Our mission is to give our customers around the world the system tools to bring about a visible and substantial increase in viability, production, and ease of use at the lowest possible cost to the customer.

Data Recovery

Our flagship self-service data recovery and undelete software products are the efficient alternative solutions to costly and time-consuming in-lab data recovery services. They allow our customers to recover data from all popular file systems in situations ranging from accidental file deletion, formatted hard drives, and damaged or deleted partitions to total erasure by a virus.

Drive Imaging and Backup

Based on the latest hard disk image creation technologies, our new R-Drive Image product creates drive image files with various compression levels on the fly without leaving Windows OS. It is one of the best backup solutions yourfor preventing loss of your data after a fatal system failure.

Data Security and Privacy

PC privacy and disk cleaning software protects your PC from examination, spying, or simple snooping into your off-line and Internet activities and destroys the data of those activities beyond recovery by hardware or software tools. What's more, wiping and cleaning unneeded files dramatically free up hard drive space and speed up the system.

R-Tools also continued to buff and bolster the performance and features of other high-performance utilities in its line-up of recovery solutions. R-Crypto, is now available ***free of charge*** for home users.
This data encryption utility protects a user's confidential information and personal data against unauthorized access, whether on a desktop, notebook or removable data storage device.

We are committed to providing fast, efficient, and affordable software

Solutions
- Data Recovery
- Mac Recovery
- File Undelete
- Drive Image
- Data Security
- Disk Encryption
- E-Mail Recovery
- PC Privacy
- Disk Cleaning
- Linux Recovery

Products
- R-Studio
- R-Studio for Mac
- R-Undelete
- R-Drive Image
- R-Firewall
- R-Crypto
- R-Mail
- R-Word
- R-Excel
- R-Wipe & Clean
- R-Linux

Download
Sales Policy
Technical Support
Purchasing Request
Volume Licensing
Distribution
R-TT Forum
R-TT FAQ
R-TT Directory

Contact Us Feedback Site Map

AccessData
A Pioneer in Digital Investigations Since 1987

SOLUTIONS PRODUCTS SERVICES TRAINING NEWS SUPPORT COMPANY TECHNOLOGY PARTNER

FORENSIC TOOLKIT®

Forensic Toolkit
Enterprise
eDiscovery
SilentRunner
Lab
Classified Spillage Solution
Mobile Phone Examiner
Decryption Tools

Request More Information

Distributed Processing: Impressive Test Results!

In testing, AccessData fully processed a massive data set, including **62,649,383 items**, of which there were well over 2 million emails and a total of 97,431 archive files that needed to be broken out. The compressed size of this data set was 1.28 terabytes. A data set this large would normally be divided into batches, with each batch being processed separately on stand-alone machines. This could take a month to process, using traditional tools, depending on the hardware used. However with AccessData's distributed processing technology, it only took **6 days, 5 hours**.

Learn More >

Forensic Toolkit® (FTK®) is recognized around the world as the standard in computer forensics investigation technology. This court-validated digital investigations platform delivers cutting-edge analysis, decryption and password cracking all within an intuitive, customizable and user-friendly interface. FTK 3 is built for speed, analytics and enterprise-class scalability. Known for its intuitive interface, email analysis, customizable data views and stability, FTK lays the framework for seamless expansion, so your computer forensics solution can grow with your organization's needs. Forensic Toolkit 3 is now the most advanced computer forensics solution available, providing functionality that normally only organizations with tens of thousands of dollars could afford. However, we are committed to making our technology available to all investigators and analysts, whether they are in law enforcement, education, a government agency, a Fortune 500 corporation, or practicing digital investigations as service provider.

PRODUCT FEATURES

An Integrated Computer Forensics Solution

- Create images, analyze the registry, conduct an investigation, decrypt files, crack passwords, identify steganography, and build a report all with a single solution.
- Recover passwords from 100+ applications; harness idle CPUs across the network to decrypt files and perform robust dictionary attacks.
- KFF hash library with 45 million hashes.

Enterprise-class Architecture

BROCHURES

AD Forensics Brochure >
What's New in FTK 3 >
Explicit Image Detection >
Laci Peterson Case Study >
AD Legal Brief >
FTK 3 System Spec Guide >
FTK 3 Quick Install Gui

WHITE PAPERS

LEGAL JOURNAL: Rules of Digi Evidence & AD Technology >
The Importance of Memory S and Analysis >

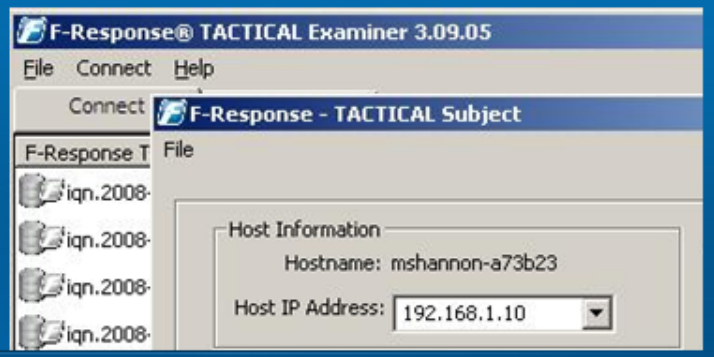
FTK 3 Series:
- UI Performance >
- Mac Analysis >
- Live, Remote Data Acquisiti
- Explicit Image Detection >

Tips & Tricks:
- Case Portability >
- FTK Field Mode >
- Oracle Adjuster >

F-Response
Extend Your Arsenal

F-Response TACTICAL

Our newest streamlined, simplified, multi-platform, and vendor neutral solution to live analysis, acquisition, and authentication.
(Now Available!)
Learn More



" For file server, mail server, production server acquisition F-Response has been a godsend. The ability to perform physical acquisition without interruption to a server is brilliant and it's also come in very handy when we've encountered disks in servers that cannot be acquired with other tools. In fact, F-Response has pretty much become the first and foremost tool in my arsenal whenever I encounter file servers, raid arrays etc. "

Chris Bowen, McGrathNicol - http://www.mcgrathnicol.com/

F-Response - Extend Your Arsenal

The First Truly Vendor Agnostic Solution for Forensics and eDiscovery

F-Response® provides read-only access to the full physical disk(s) of virtually any networked computer, plus the physical memory (RAM) of most Microsoft Windows® systems. F-Response enables Live forensics and eDiscovery to be conducted over IP networks using the investigators tools of choice.

F-Response uses a patent-pending process based on well documented industry standards to create a secure, read-only connection between the examiner's computer and the computer under inspection. F-Response was designed to be completely vendor neutral.

If your analysis software reads a hard drive, it will work with F-Response.

F-Response makes the storage devices on the computer under examination completely accessible to the examiner's computer where they appear as local, raw, physical storage devices. The F-Response connection is

Recent News

F-Response TACTICAL Released
F-Response now supports HP Unix
F-Response 3.09.05 has earned "Compatible with Windows 7" status
F-Response selected by the SPO Korea
F-Response for AIX and Solaris now available

From Our Blog

Eoghan Casey's Handbook of Digital Forensics & Investigation
Using F-Response on something other than Windows
New IBM hardware arrives
TACTICAL reviewed on Forensic4Cast
2009, A Year in Review

Frequently Asked Questions

Non-technical issues

Computer Crime

- Hard to predict for the following reason
  - Low computer literacy among lawyers, police agents, jurors, etc.
  - Tangible evidence like fingerprints and physical clues may not exist
  - Forms of asset different
    - Is computer time an asset?
  - Juveniles
    - Many involve juveniles

Source: “TEL2813/IS2820 Security Management” by James B D Joshi

Page last updated at 14:49 GMT, Tuesday, 8 December 2009

'Dangers' of a free market in forensic science

By Paul Burnell
File on 4

'Luke' (not his real name) was sentenced to three years in jail when a court decided he had "kicked another man's head like a football".

The FSS announced major redundancies earlier this year

Part of the evidence heard in court was based on the spots of the assaulted man's blood which were found on his shoe.

Luke claims he had gone to stop another man assaulting the victim, saying the blood on his shoe: "Put me at the scene of the crime, which I never denied anyway."

After his conviction, Luke's family hired private forensic science provider Forensic Access who carried out a further test and called a blood pattern analysis (BPA).

'Vital' test

According to Dave King, Business Manager of Forensic Access the test came to a stark conclusion. "We can see from photos in the case file there is only a small amount of blood," he says. "There is no way that piece of footwear could have made contact with somebody's head."

Mr King said that the BPA would have doubled the cost of the forensic evidence, adding it was why he believed the test was not

Some excerpts from a Belgian FCCU case-study

Who investigates ICT crime ?

- Prosecutors / Examining Judges
- Specialised police forces (nat'l & Internat'l)
- Legal expert witnesses
- Specialised forensic units of consulting firms
- Associations defending commercial interests

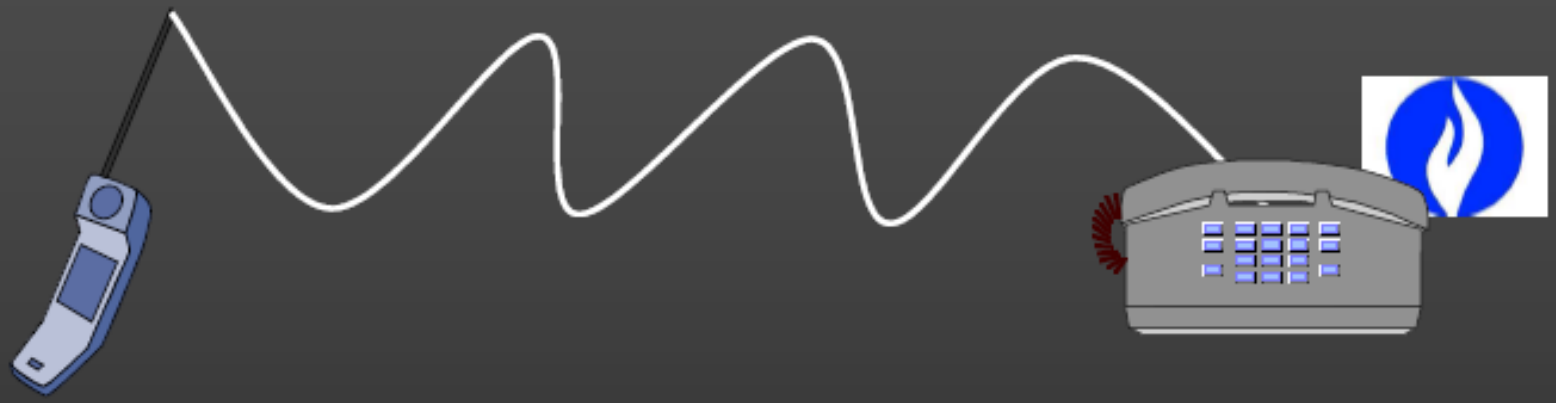
Investigative problems - tracking

- Victims : **Unfamiliar** and fear for "**Corporate image**"
  => belated complaints – trashed / no more traces
- Rather "**unknown**" world for **police & justice**
  => Delay before involvement specialised units
  Limited ICT investigation capacity (technical & police skills)
- **Multiplication and integration** of
  services / providers / protocols / devices
- **Lack** of harmonised **international** legislation & instruments
- Anonymous / hacked connections – subscriptions - WIFI
- **Intermediate** systems often cut track to purpetrator

Investigative problems – evidence gathering

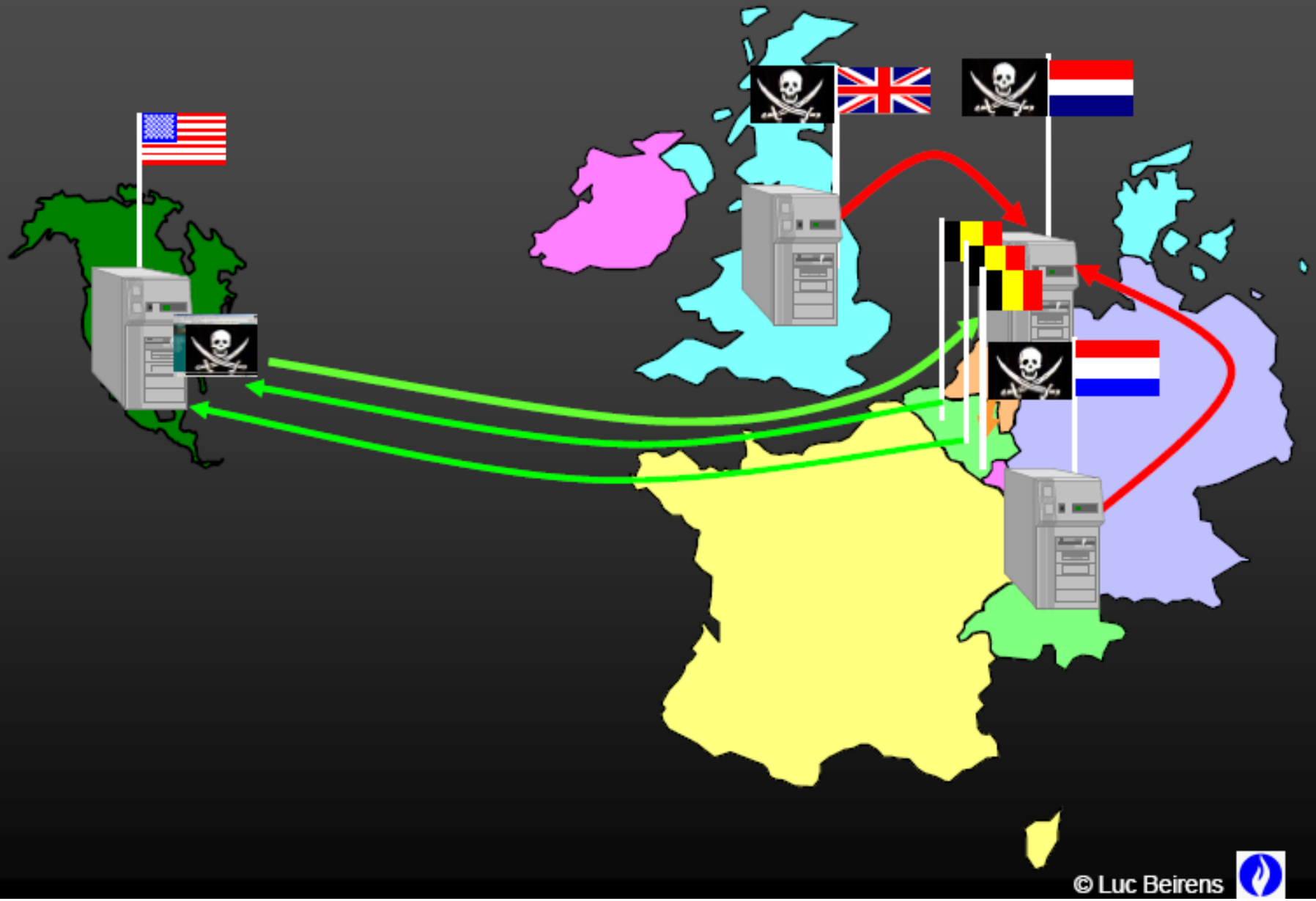
- **Delocalisation** of evidence
- Exponential growth of **storage capacity**
  => time consuming :
  - backups & verification processes
  - Analysis
- New legislation / jurisprudence imposes more **rigorous procedures** for evidence gathering in cyber space
- **Bad ICT-security** :
  give proof of the source and the integrity of evidence

Brussels, we have a problem ...



- Complainer
  - Hello, can you help ?
  - We are a **Belgian hosting firm**
  - We have a problem
  - Our **webservers** are **hacked**
  - & several **websites** of our **Belgian customers** have been **defaced**
- Politie
  - OK
  - A few questions to start our file …
  - Who, where, what, when …

Who is where ?

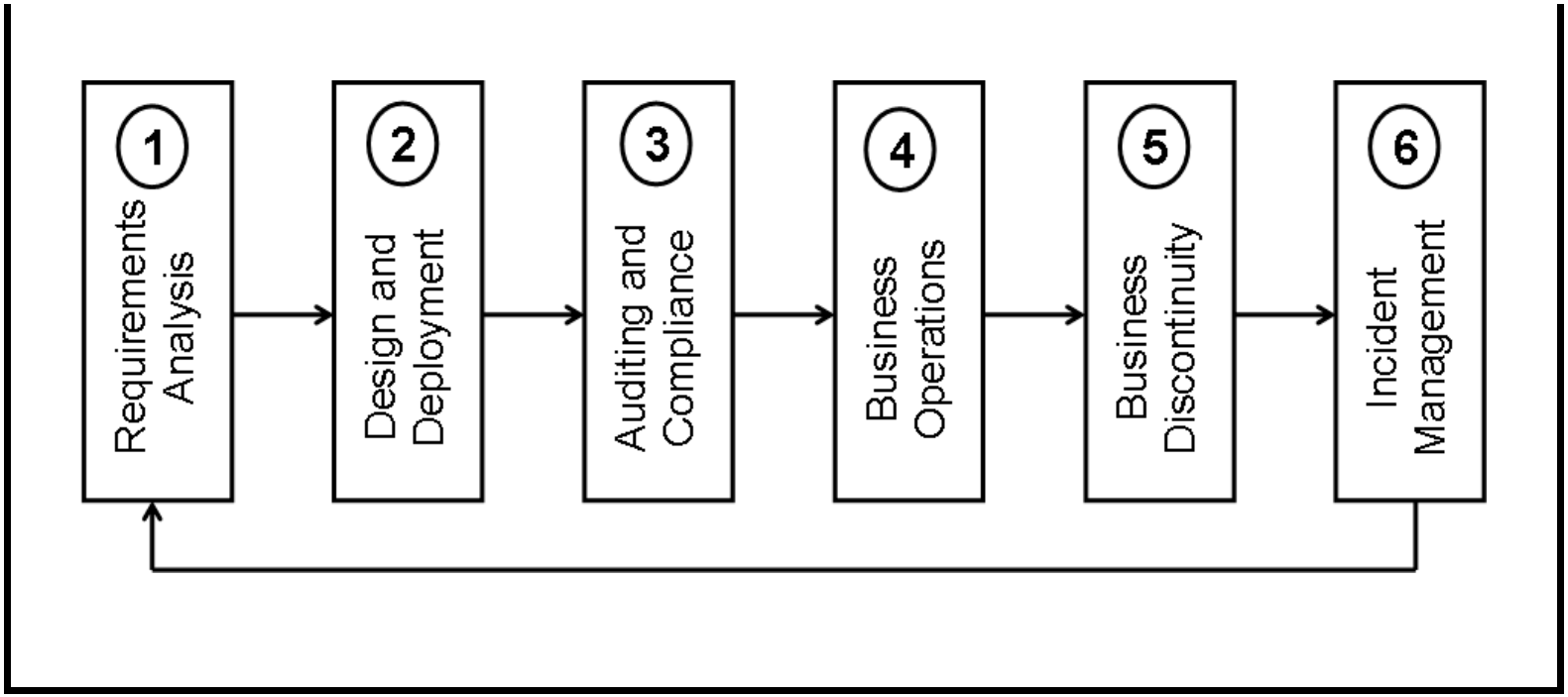


Who / where / what

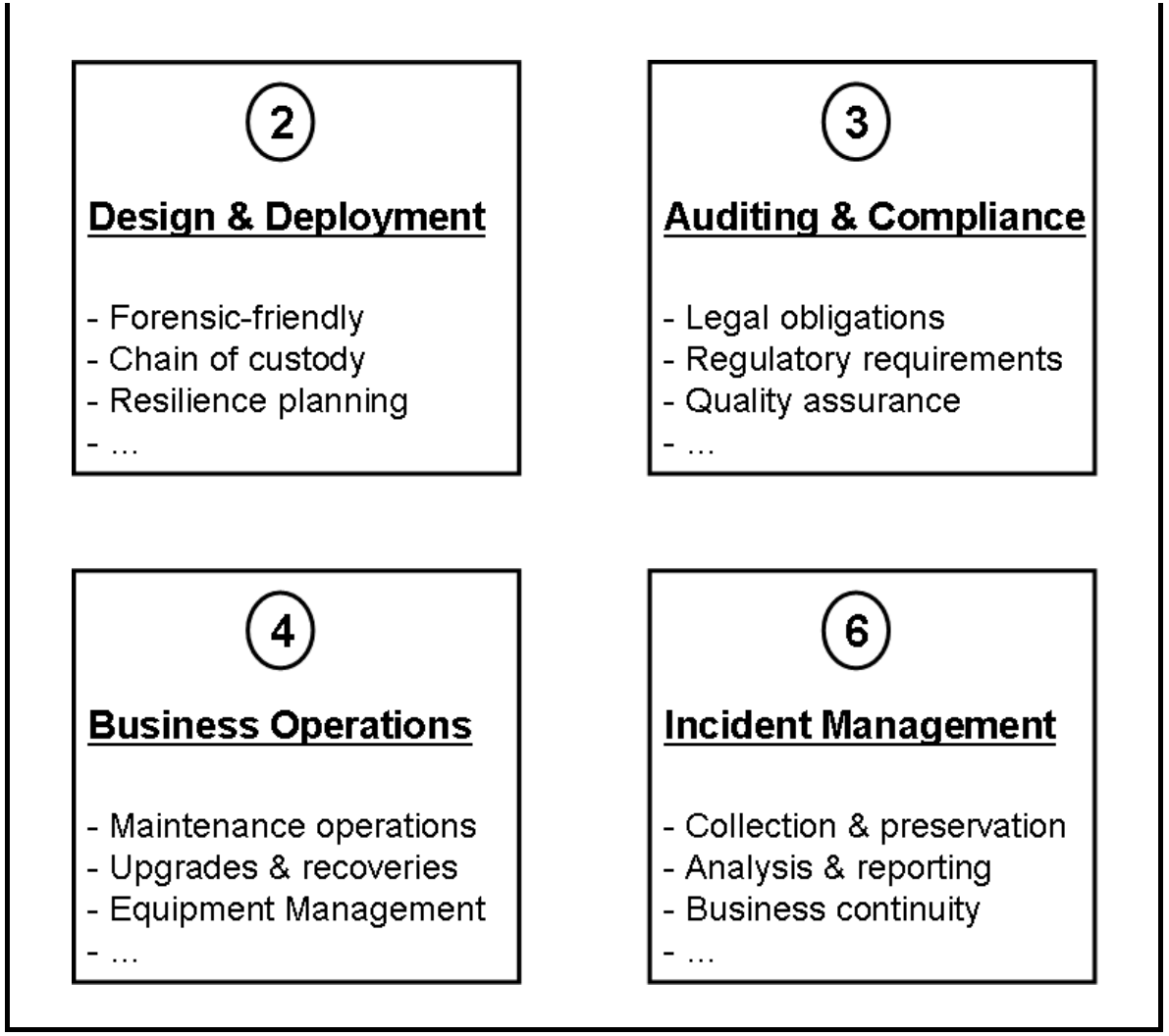
- In Belgium
  - Hosting firm : **nothing** in Belgium
  - Customer : **nothing** in Belgium
  - Hacked firm : **nothing** in Belgium
- In the USA
  - Hacked webserver
  - Defaced website
- In the Netherlands
  - Hacked server
- In the UK
  - Hacker ?
- In the Luxemburg
  - Hacker ?

Digital Forensics in Corporate ICT Infrastructure

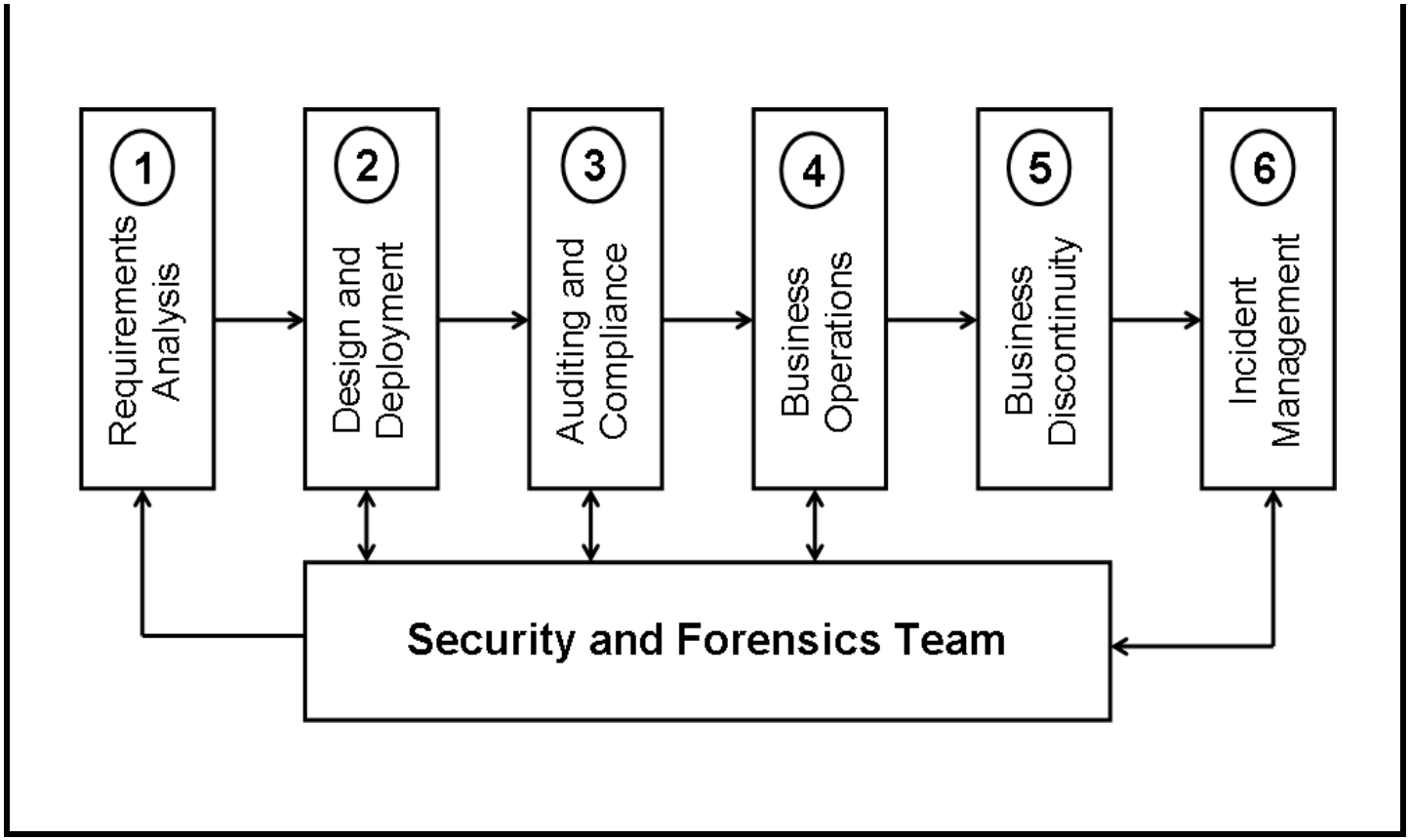
Corporate ICT Operations



Operational Improvements by Digital Forensics

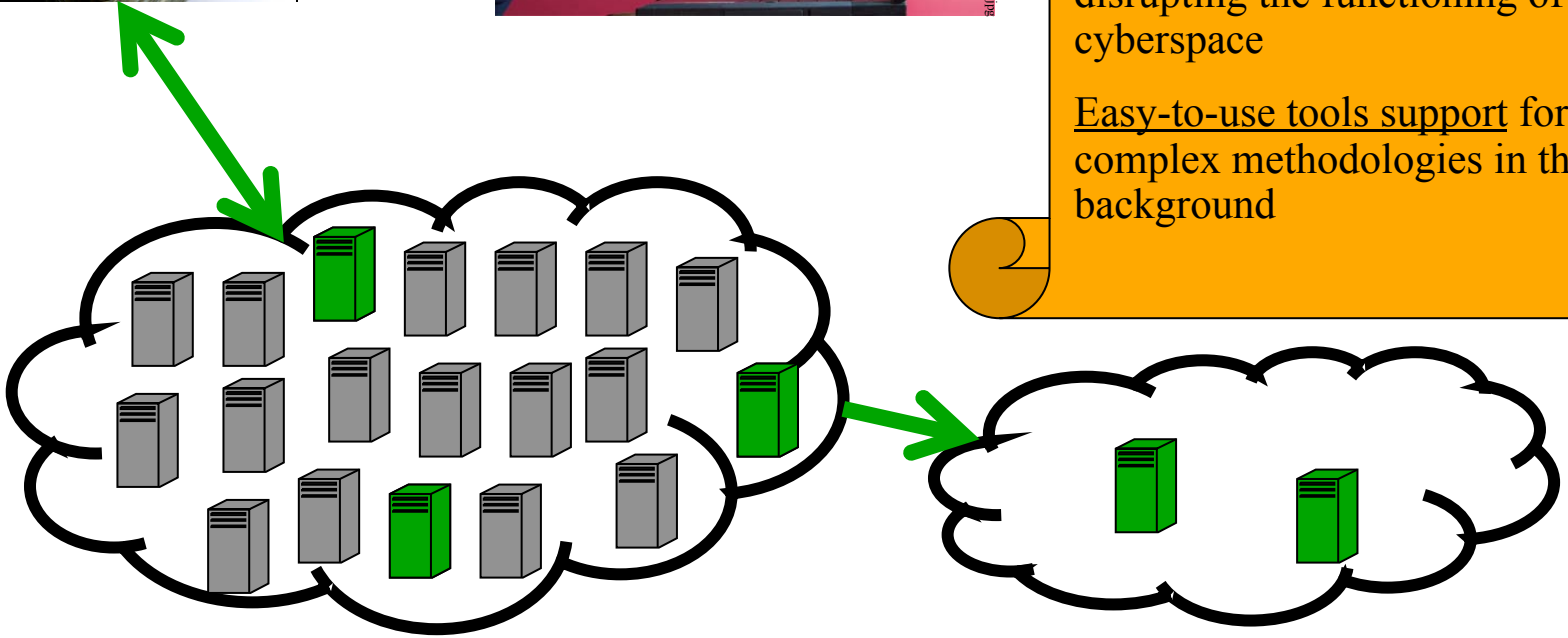


Security & Forensics Team



Future Challenges

A real-life scenario



Forensics analysis methodologies for massive, highly distributed systems with dynamically changing boundaries

Identification & isolation/ quarantine techniques to cordon-off the affected zone without disrupting the functioning of the cyberspace

Easy-to-use tools support for complex methodologies in the background

Potential Impact

- **Nowadays**
  - ENRON scandal*
  - FBI gathered and analyzed **31 TB** of digital data
    - 1 TB = 250 million pages
    - 16 kilometers high stack if printed on both sides of the page.
  - FBI's Computer Forensics Lab processed data from 130 computers, thousands of e-mails, and more than 10 million pages of docs.
  - Length of investigation = **5 years**

- **Tomorrow**
  - Clouds, virtualization will drive cybercrime #
  - Businesses and law enforcement agencies can't cope this wave with classical digital analysis approaches.
  - We have to address this shortcoming by enabling the security and forensics stakeholders to cope the post-accident scenario.
  - Beneficiaries will not only be the Cybercrime units but also the safeguarding of commercial and personal interests of the technology users.

** Statistics taken from the FBI website http://www.fbi.gov/page2/may07/rcfl050707.htm*

 # Trend Micro Report: The Future of threats and Threat Technologies – How the Landscape is Changing http://affinitypartner.trendmicro.com/media/34716/trend_micro_2010_future_threat_report_final.pdf

cetic
Your Connection to ICT Research

Novelty in the area of investigations

- Digital Forensics framework for the emerging infrastructures (Clouds, Future Internet, …) by using virtualization techs.
  - Research on the 'need to know' parameters and their optimization
  - Development of corresponding tools
  - Auditing and compliance issues of Digital Forensics
- Tradeoff between privacy requirements and digital traces
  - Compliance with the EU Privacy directive and national laws
  - Harmonization of cross-border and cross-organizational issues of data access
- Collaborations with the stakeholders of the virtualization infrastructures
  - E.g. provision of finer grained details to a specific kind of public (such as CERTs, CSIRTs, CCUs, …)
    - Something similar to mobile phone's tracking
    - Study of the performance parameters

cetic
Your Connection to ICT Research

Challenges of Digital Forensics in the Future Internet based Systems

- **Access Control**
  - Monitoring of access logs
- **Steganalysis**
  - Efficient data analysis tools
- **Multitenancy**
  - Isolation of software execution environments
- . . .

Digital Forensics Framework for SMEs using Virtualization Technologies

- **Tools support**
  - General strategy
- **Threats landscape**
  - Preparation phase
- **Reactivity**
  - Detection phase
- **Perimeter demarcation**
  - Preservation phase
- **Semantics support**
  - Analysis phase
- **Resilience**
  - Recovery phase
- **Feedback**
  - Reporting phase

Your Connection to ICT Research

"… when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived."

(Edmond Locard, 1910)

Your Connection to ICT Research

Thank you

SYED NAQVI, PHD

R&D Project Manager

Software & Services Technologies Dept.

syed.naqvi@cetic.be