Information Technologies and Fraud

Florin Gogoasa
CISA, CFE, CGEIT, CRISC
ACFE Romania – Founder and Board member

Managing Partner
Blue Lab Consulting

©2012 Association of Certified Fraud Examiners, Inc.

AGENDA

Information Technologies for Fraud investigation

A. Intelligence and e-discovery
B. Digital forensics

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

TECHNOLOGIES

More and more Information Technologies are used to deal with:

- Fraud prevention
- Fraud investigation / examination
- Forensics

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

E–DISCOVERY VS. DIGITAL FORENSICS

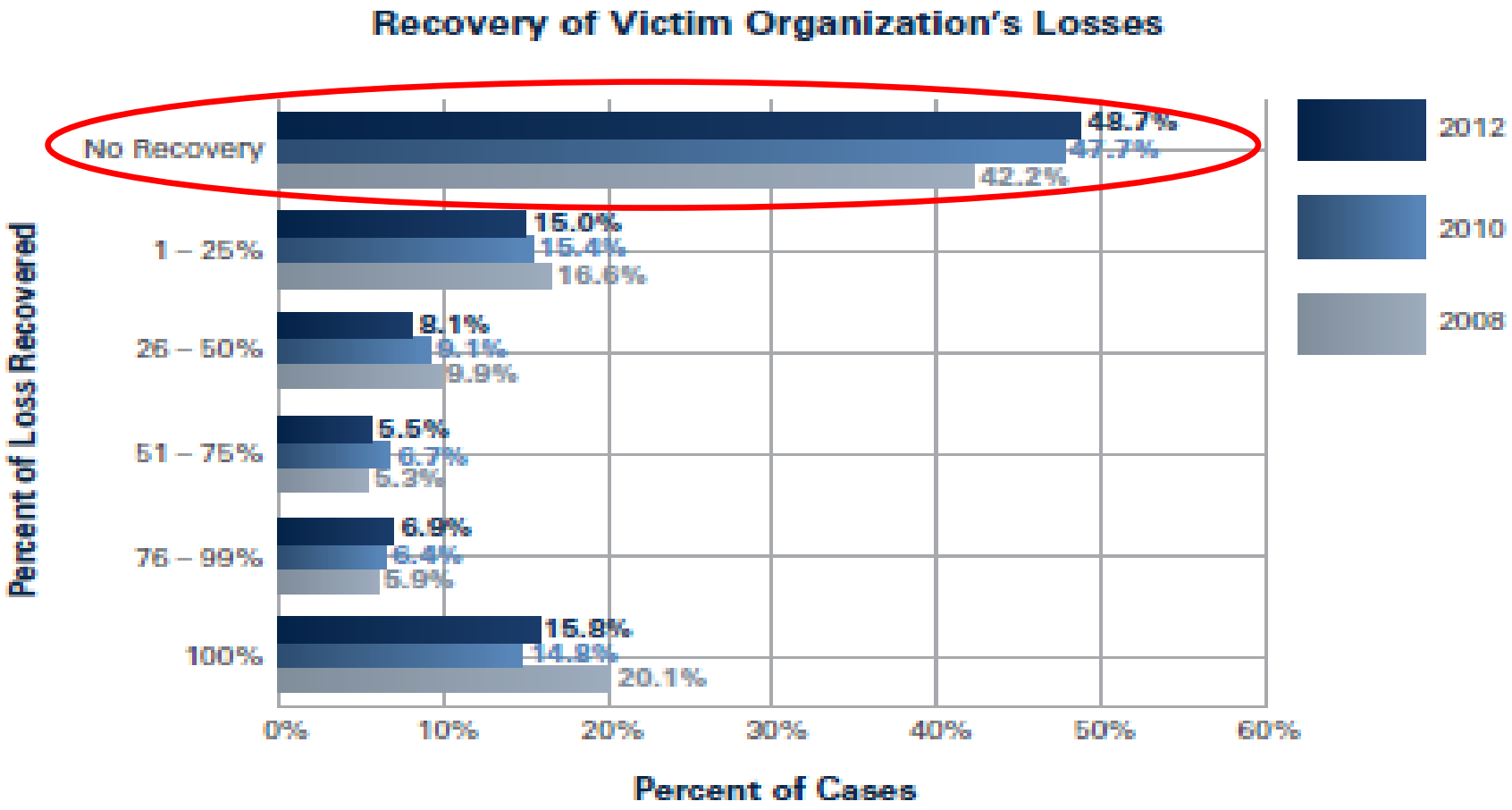
Digital forensics, also called cyber forensics, and e-discovery are two different disciplines used to target computer based evidence in a legal investigation.

Digital forensics = recovery and investigation of material found in digital devices, often in relation to computer crime.

E-discovery = electronic discovery (or e-discovery or eDiscovery) refers to discovery in civil litigation which deals with the exchange of information in electronic format.

ACFE Association of Certified Fraud Examiners ©2012 Association of Certified Fraud Examiners, Inc.

FRAUD RECOVERY STATISTICS



ACFE Association of Certified Fraud Examiners ©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE

There are many ways to research for information related to suspect activities and/or employees:

- Internet: Google and other search engines
- Job sites, social networks
- Company information systems
- Databases
- Mobile devices tracing and logging
- Access control / video monitoring systems
- Recording, tracking, key logging, HDD copy
- Specialized computers monitoring software

ACFE Association of Certified Fraud Examiners ©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE

There are many data sources to help with intelligence activities in Company information systems:

- Audit trails and security logs
- SIEM application
- Information Leakage Prevention (ILP / DLP) applications Transactions databases
- Archives
- Data warehouses
- Email systems

ACFE Association of Certified Fraud Examiners ©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE

Mobile devices tracking and logging:

- SMS / Chat
- Company centralized phone logs
- GSM Provider activity logs
- GPS tracking
- GSM network location
- Voice recording ??

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE

- Access control / video monitoring systems
  - Access control logs
  - Video surveillance images
- Tracking, key logging, HDD copy,…and recording?
  - HW / SW key loggers
  - HDD forensic image
- Specialized computers monitoring software….

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE ANALYSIS

- Fraud case intelligence tools are rich, data-centric visual analysis environment.
- A combination of data storage, analysis tools, visualization, and dissemination capabilities
- Addresses the analyst's and investigator's multi-tiered challenge of discovering networks, patterns and trends across increasing volumes of structured and unstructured data.

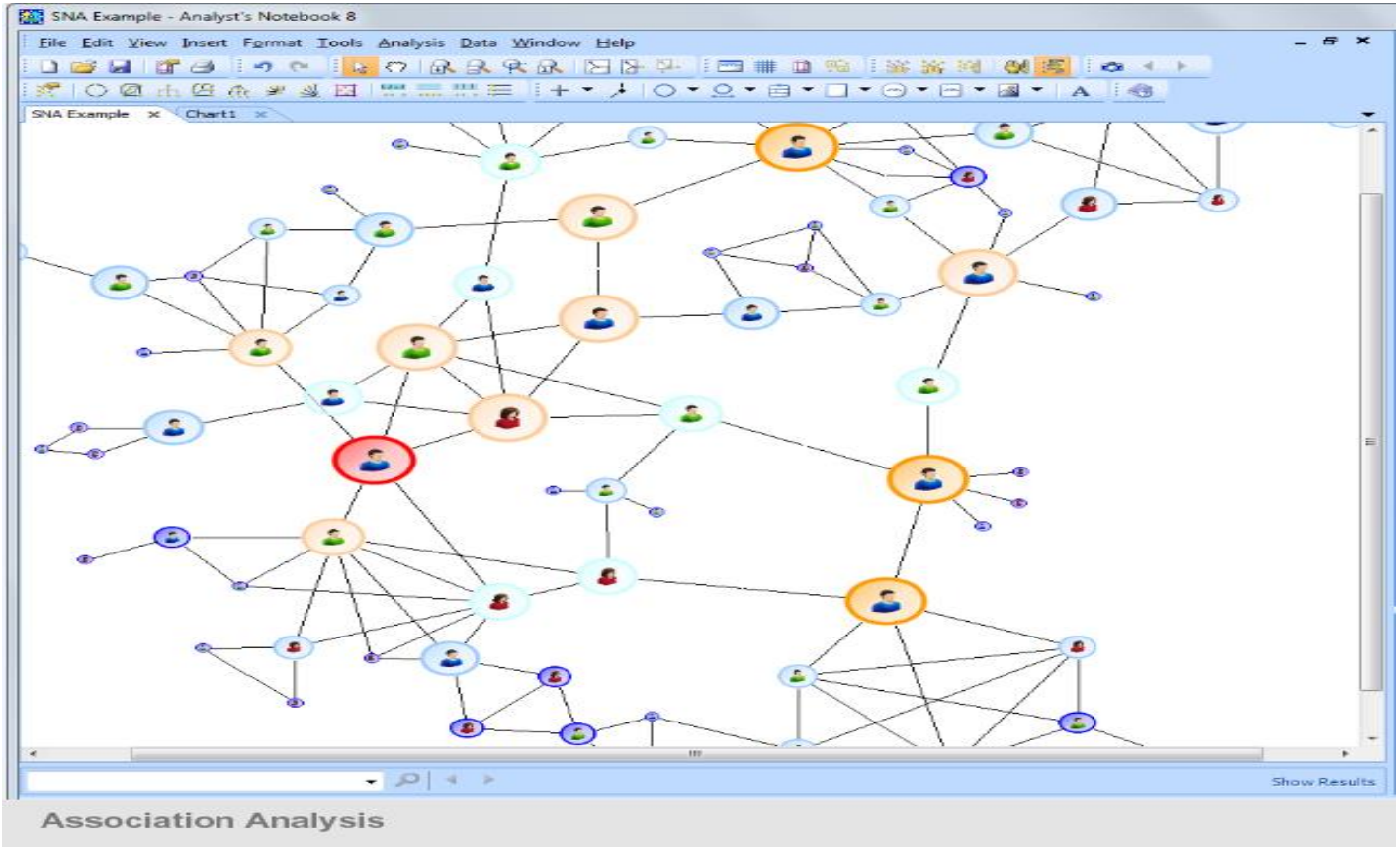
ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE ANALYSIS

- Dedicated data and chart management in a single data-centric analysis environment.
- Rich visualization and analysis underpinned by a local repository improving the detection rate of key information across all existing data.
- Search and discovery across collated data supporting identification of connections across seemingly unrelated data.
- Integrated data management interface to speed data ingestion and sharing.
- Simplify the communication of complex data to enable timely and accurate operational decision-making.

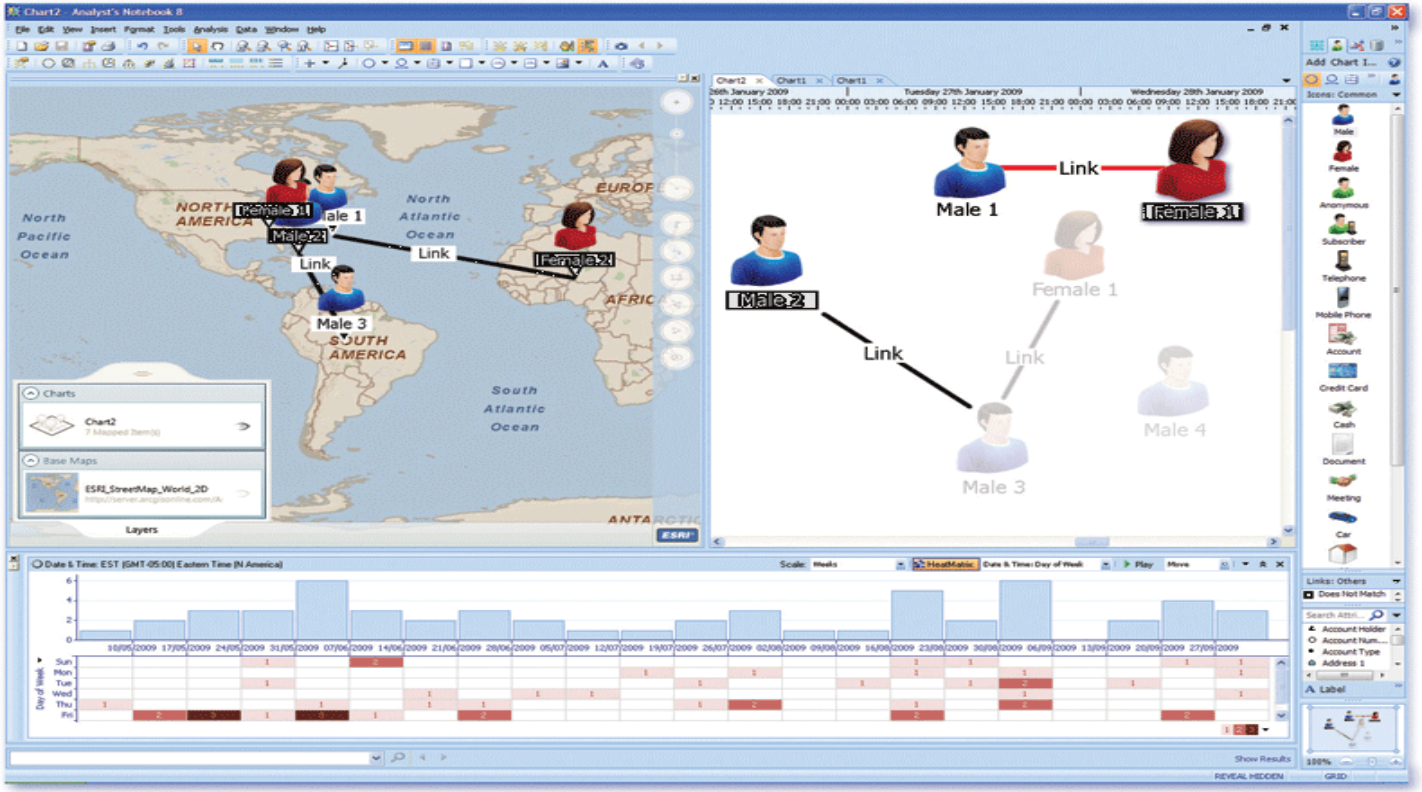
ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE ANALYSIS EXAMPLE



ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

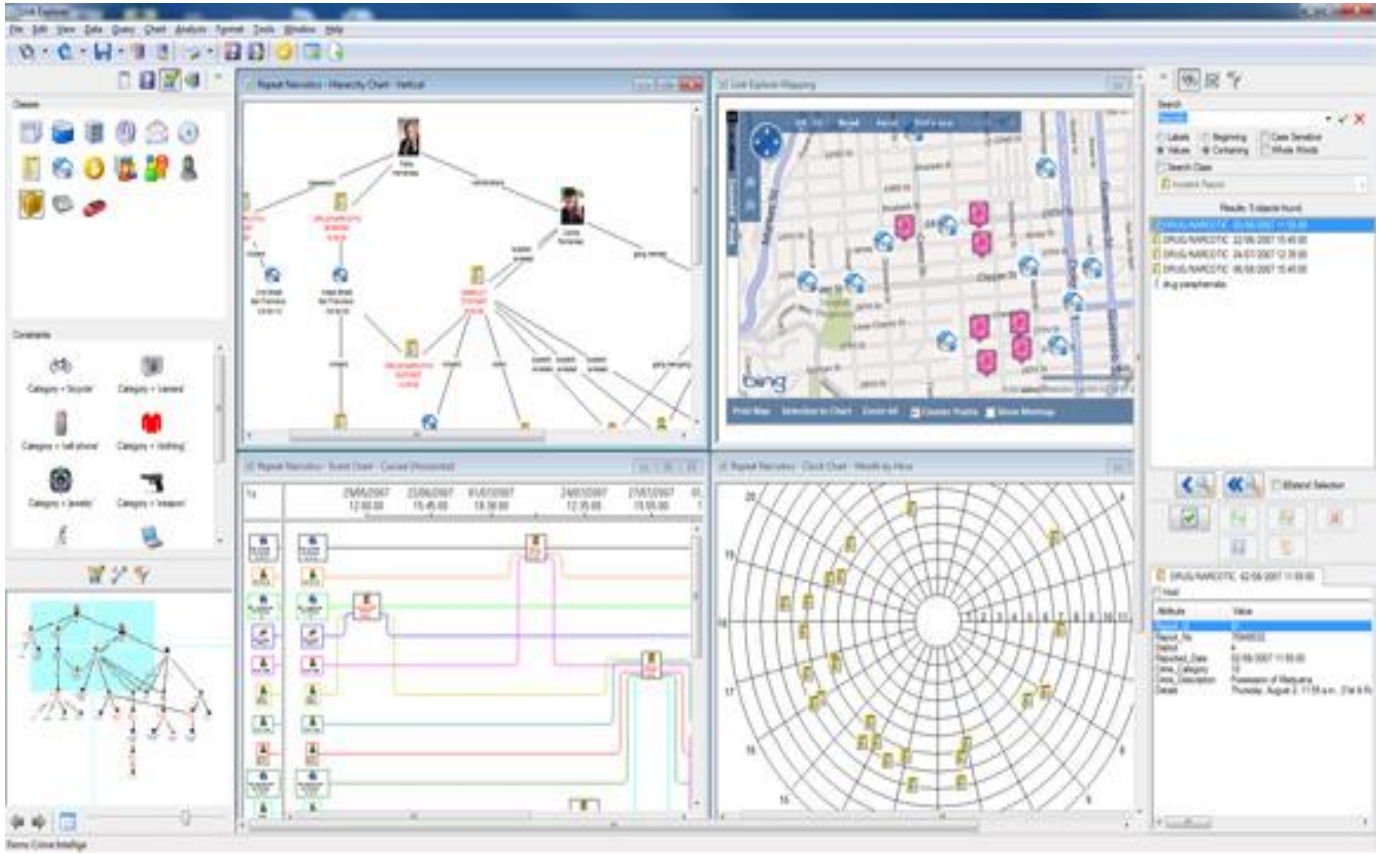
INTELLIGENCE ANALYSIS EXAMPLE



Analyst's Notebook—Esri® Edition offers Esri's ArcGIS server map views and basic geospatial analytical functionalities integrated within the Analyst's Notebook environment

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

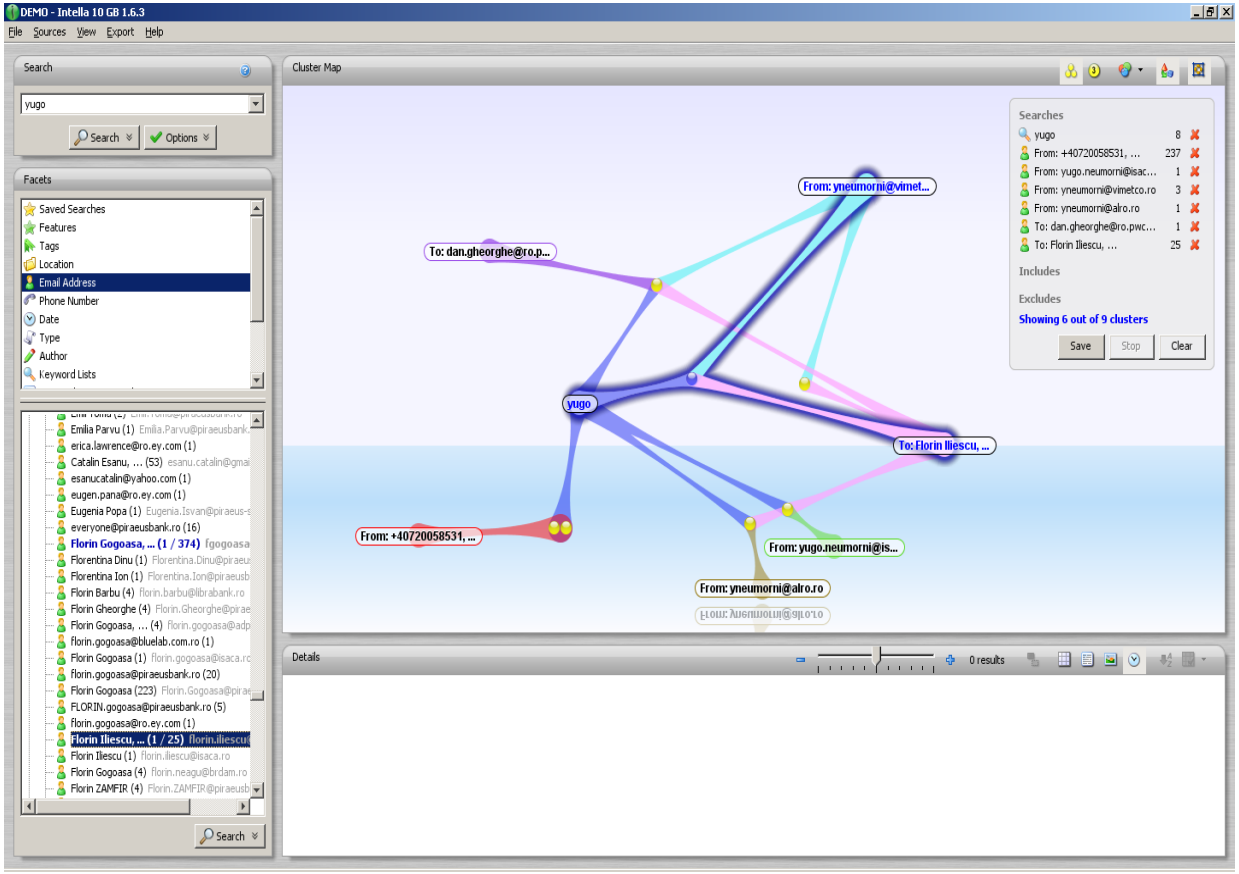
INTELLIGENCE ANALYSIS EXAMPLE



ACFE Association of Certified Fraud Examiners

©2012 Association of Certified Fraud Examiners, Inc.

INTELLIGENCE ANALYSIS EXAMPLE



ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

FORENSICS

- **Forensic accounting**: Forensic accounting or financial forensics is the specialty practice area of accountancy that describes engagements that result from actual or anticipated disputes or litigation. "Forensic" means "suitable for use in a court of law"
- **Digital Forensics**: is the practice of collecting, analyzing and reporting on digital information in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

DEFINITION

- **Forensics**
  1. The art or study of formal debate; argumentation.
  2. The use of science and technology to investigate and establish facts in criminal or civil courts of law.
- **In application it involves the following steps:**
  - Collection
  - Examination
  - Analysis
  - Report or Statement
  - Presentation of Computer Evidence / Report

ACFE Association of Certified Fraud Examiners ©2012 Association of Certified Fraud Examiners, Inc.

COMPUTER FORENSICS

- **93%** of all information produced is digital (Source: UC Berkeley Study)
- Normal tools and processes immediately taint the evidence
- Normal tools are not able to access all potential evidence
- Ability to easily link associated pieces of evidence to provide a chronological history of activity
- Point in time snap shot ability which has minimal impact on operations

Computer Forensics is now a requirement !!

ACFE Association of Certified Fraud Examiners ©2012 Association of Certified Fraud Examiners, Inc.

CONSIDERATIONS

- Computer Forensics produces facts, it is an objective view of what has occurred.
- Computer Forensics can only report what user ID or e-mail address carried out a task, it cannot state that a certain individual carried out a task.
- Analysis can be completed exhaustively BUT this may be deemed illegal or inappropriate activity if out of scope. Specific keywords and actions should be sought for instead and hence defined in a scope letter.
- Evidence on a shared server is difficult to present.

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

METHODOLOGY

- Principle 1
  - No action taken by the Police or their agents should change the data held on a computer or other media.
  - Where possible computer data must be ‘copied’ and that version examined.
- Principle 2
  - In exceptional circumstances it maybe necessary to access the original data held on a target computer.
  - However it is imperative that the person doing so is competent and can account for their actions.

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

METHODOLOGY

- Principle 3
  - An audit trail must exist to show all the processes undertaken when examining computer data.
- Principle 4
  - The responsibility rests with the person in charge of the case to show that a computer has been correctly examined in accordance with the law and accepted practice.

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

WHY COMPUTER FORENSICS?

- Regulatory breaches
- Counterfeiting / fraud
- Extortion
- Industrial Espionage
- Wrongful Termination / Contractual disputes
- Mishandling and theft of IP
- Harassment
- Possession of Inappropriate material
  - Pornography, Illegal Software
  - Illegal music and video
- Matrimonial disputes
- Computer misuse (spam, illegal trading, viruses, denial of service attacks)

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

IT FORENSIC TOOLS

Disk Analysis Tools

- Hard Drive Firmware and Diagnostics Tools
- Linux-based Tools
- Macintosh-based Tools
- Windows-based Tools
- Open Source Tools

Enterprise Tools (Proactive Forensics)

Forensics Live CDs

Personal Digital Device Tools

- GPS Forensics
- PDA Forensics
- Cell Phone Forensics
- SIM Card Forensics

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

Name	Platform	Description
SANS Investigative Forensics Toolkit - SIFT	Ubuntu	Multi-purpose forensic operating system
EnCase	Windows	Multi-purpose forensic tool
FTK	Windows	Multi-purpose tool, commonly used to index acquired media.
Digital Forensics Framework	MANY	DFF is both a digital investigation tool and a development platform
The Coroner's Toolkit	Unix-like	A suite of programs for Unix analysis
COFEE	Windows	A suite of tools for Windows developed by Microsoft, only available to law enforcement
The Sleuth Kit	Unix-like/Windows	A library of tools for both Unix and Windows
Belkasoft Evidence Center	Windows	instant messenger logs, internet browser histories, mailboxes of popular email clients, social network remnants, peer-to-peer data, multi-player game chats, office documents, pictures and videos.
Paraben	Windows	General purpose forensic tool
Open Computer Forensics Architecture	Linux	Computer forensics framework for CF-Lab environment
SafeBack	N/a	Digital media (evidence) acquisition and backup
Windows To Go	n/a	Bootable operating system
Forensic Assistant	Windows	User activity analyzer(E-mail, IM, Docs, Browsers), plus set of forensics tools
OSForensics	Windows	General purpose forensic tool for E-mail, Files, Images & browsers.
X-Way Forensics	Windows	General purpose forensic tool based on WinHex hex editor.

FORENSICS DEMONSTRATION EXAMPLE

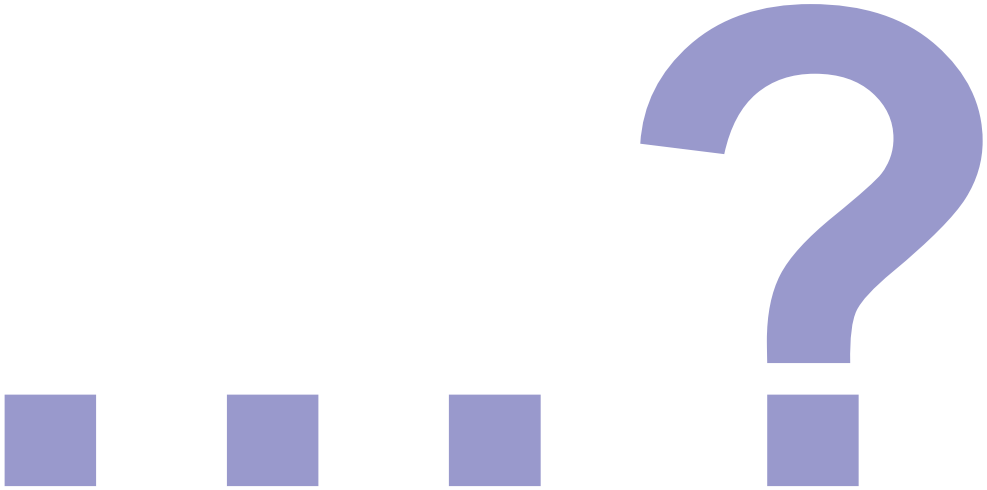
- References to specific companies (e.g. rival company)
- Presence of encrypted files
- Presence of credit card numbers
- Use of non-corporate email, chat rooms, social networks
- Presence of deleted files (documents, pictures, …)
- Files that have deliberately had their file extensions masked
- Specific files artefacts

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

MOBILE FORENSICS TOOLS EXAMPLE

- Paraben Device Seizure
- Cellebrite UFED Mobile Forensics
- Radio Tactics Aceso
- MicroSystemation XRY/XACT[4]
- Oxygen Forensic Suite
- MOBILedit! Forensic
- Elcomsoft iOS Forensic Toolkit
- SAFT Mobile Forensics (Android)

ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.



ACFE Association of Certified Fraud Examiners
©2012 Association of Certified Fraud Examiners, Inc.

THANK YOU !

Florin Gogoasa

CISA, CFE, CGEIT, CRISC
Managing Partner
Blue Lab Consulting
Mobile: 0720058531

florin@bluelab.com.ro

Bd. Magheru nr. 7, sector 1,
Bucuresti, Romania

ACFE Association of Certified Fraud Examiners ©2012 Association of Certified Fraud Examiners, Inc.