



cybex

Working for Intelligence



Computer Forensics Problems and Solutions ?

- What's like working for a Forensic Lab?
- Definition
- Process
- Technology
 - First generation forensic tools → power down required!
 - Complex investigations → geographically dispersed computer systems!
 - Constantly growing size of media → time / space constraints!
 - Moving out of the “disks” into the unknown...
 - Evidence eliminator's, anonymizers...
 - Digital forensics, Bill Gates & My mother
- Laws
 - Internet is no-mans-land → no international legal framework available!
 - From data to evidence...
- Logistics
 - Tried to acquire 100 CDs/discs in one day?



Computer Forensics Problems and Solutions ?

- What's like working for a Forensic Lab?
 - 14/01/2004 1600 hours STAUS: got 10 slides for tomorrows presentation, have to finish quickly and get a haircut.
 - 14/01/2004 1700 hours STAUS: got 20 slides for tomorrows presentation, boss tells me there's an emergency in Madrid! Got to fly today instead of tomorrow and image 2 systems tonight!
 - 14/01/2004 2145 hours STAUS: Flight takes off...
 - 14/01/2004 2245 hours STAUS: Meet HHR manager tells me it'll be 4 systems instead of 2 ☹
 - 14/01/2004 2400 hours STAUS: Starting to copy...
 - 15/01/2004 0300 hours STAUS: Try to do some more slides while imaging takes place (now).
 - 14/01/2004 0500 hours STAUS: Finished copying suspect systems ☺
 - 14/01/2004 0600 hours STAUS: Reach hotel, buy coffee, prepare for a long night and hope tomorrows audience will be comprehensive ☺

All in all... it's FUN!

(well, sort of...)



Computer Forensics Problems and Solutions ?

- Definition

People, processes, tools and measures to gather, analyze and interpret digital data to support or refute certain allegations of misuse involving digital systems.

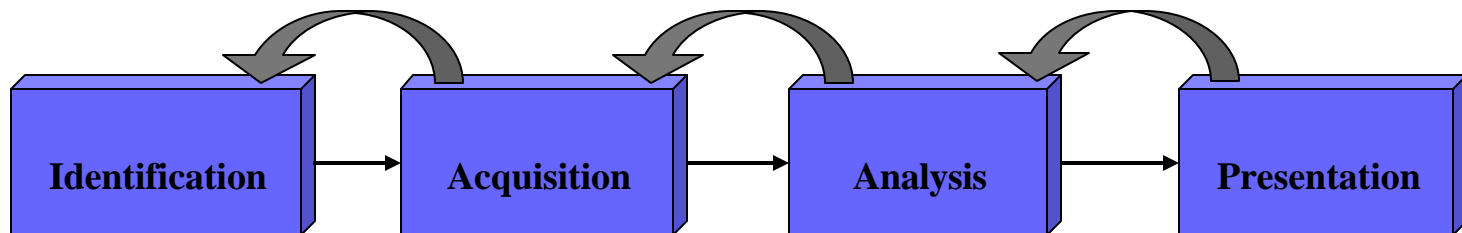
Computer Forensics → Digital Forensics

- Phones, SIM cards, printers, digital cameras, PDAs, GPS systems...

Digital Forensics Problems and Solutions ?

- Process

- Identification
- Acquisition
- Analysis
- Presentation





Digital Forensics Problems and Solutions ?

- Process not recipe! You might have to go back on your steps...
- During Acquisition you could find out you need to rethink your Acquisition Plan to include more data sources.
- During Analysis you could find out references to data sources not acquired.
- During presentation you could be challenged with questions which require you to do further analysis in order to provide satisfactory answers.



Digital Forensics Problems and Solutions ?

- Technology (First generation forensic tools → power down required!)
 - Loss of business continuity → \$\$\$
 - Loss of potentially relevant data → pull-the-plug factor
- Technology (Complex investigations → geographically dispersed computer systems!)
 - Increment in time and costs due to HHRR movement
 - Bloqued HHRR in transit
 - Diminising risks to personal in undercover activities.



Digital Forensics Problems and Solutions ?

Current workarounds to avoid stopping systems

1) Live manual analysis

Inconvenients

- Time constraints to locate and acquire relevant evidence.
- Destruction of digital data unavoidable.
- Exposure to logic bombs rigged by the owner of the system
- Potentially incomplete view of the system (rootkits etc...)



Digital Forensics Problems and Solutions ?

Current workarounds to avoid stopping systems

2) Live automated extraction of relevant data

Inconvenients

- Destruction of digital data unavoidable.
- Exposure to logic bombs rigged by the owner of the system
- Potentially incomplete view of the system (rootkits etc...)
- Extracted information could prove to be not enough as new intelligence is gathered during analysis.



Digital Forensics Problems and Solutions ?

Current workarounds to avoid stopping systems

3) Use of regular preexisting backups

Inconvenients

- No UC! You're seeing half of the picture.
- No access to key files such as: pagefile, hiberfil, printer spoolers, tmp files, NTFS transaction logs...



Digital Forensics Problems and Solutions ?

Current workarounds to avoid stopping systems

4) “Abuse” of high availability solutions

Inconvenients

- Mirroring: We’re leaving a critical system without redundancy as the mirror rebuilds (could take several hours...)
- (LB) Load Balancing: Critical system without redundancy and probably handling more than it can take (sizing not kept up-to-date)
- HA (High Availability): Critical system without redundancy



Digital Forensics Problems and Solutions ?

Current workarounds to avoid moving HRRR around the globe

- Subcontract to a local forensic group the imaging → Very delicate issue here... Will they keep up to your quality standards? Will you be able to use that in court?
- Use local computer expert to fire a dd | nc to your servers → Do you have a local computer expert available? TCP/IP is not rock solid...
Autoresume dd?
- Time..... is money ☺

Digital Forensics Problems and Solutions ?

- Technology (Constantly growing size of media → time / space constraints!)
- Some numbers:
 - 6 users involved
 - 60 GB HDDs
 - 20 CDs/person
 - 1 common file server 100 GB.
 - Over 500 GB aprox / 0.5 TB**
- And this is only the beginning...add some big servers or and multiply by the number of concurrent open cases...



Digital Forensics Problems and Solutions ?

- Technology (Constantly growing size of media → time / space constraints!)
 - Acquisition times!!
 - Hashing & Searching times!!
 - Analysis times!! (70K documents ~) (not only “security” incident response forensics...)
 - “*I need this for yesterday*” → All cases are high priority for the client! Welcome to the jungle.



Digital Forensics Problems and Solutions ?

- Technology (Moving out of “disks” into the unknown...)
 - We know how to handle all kinds of “disks” ✓
 - Serious RAID Systems? San’s? ✗
 - Evidence from networks? ✗
 - Evidence from routers? ✗
 - Evidence eavesdropped during transmission? ✗

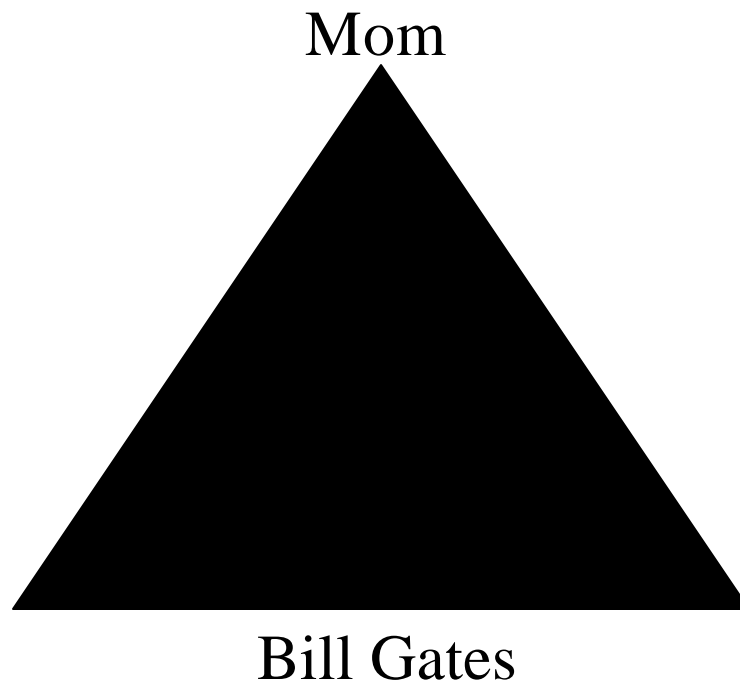


Digital Forensics Problems and Solutions ?

- Technology (Evidence eliminator's, anonymizers, strong crypto...)
 - Evidence Eliminator style programs
 - All kind of anonymizers (some pretty [cool](#))
 - Strong Crypto (BestCrypt, PGP, ScramDisk...)
 - RegCleaners
 - Backdoors
 - Disk Scrubbers
 - Steganography

Digital Forensics Problems and Solutions ?

- Digital forensics, Bill Gates & My mother





Digital Forensics Problems and Solutions ?

- Laws (No international legal framework available!)
 - Hey! That's offside were I come from! Were you from?
 - How evidence must be acquired on foreign countries?
 - Under which legal system would this case be judged?
 - No replacement for thorough regional local support from experts (lawyers)



Digital Forensics Problems and Solutions ?

- Laws (not that there are no guidelines!)
 - NHTCU / ACPO Good Practice for Computer based Electronic Evidence
 - US-DOJ Electronic Crime Scene Investigation, A guide for first responders.
 - US-DOJ Searching and seizing computers and obtaining electronic evidence in criminal investigations
 - IOCE Guidelines for best practice in the forensic examination of digital technology.
 - RFC 3227 Guidelines for evidence collection and archiving.
 - G8 Digital Evidence Principles
 - CTOSE Cyber Tools On-Line Search for Evidence.

Digital Forensics Problems and Solutions ?

- Laws (mmm ok there are guidelines but..)
 - Which should **we** follow? And **why**?



Science → Forensic Science → What courts accept TODAY



Digital Forensics Problems and Solutions ?

- Laws (mmm ok there are guidelines but..)
 - In court no Judge will be a computer expert... He is a legal expert of course!!!
 - He's not there to decide if:
 - TCP/IP syn numbers are enough to prove such and such
 - Word edit time meta-data reflects actual edit time
 - Bin-Laden string un UC has relevance
 - He needs to decide if:
 - Any laws were violated?
 - Was a clause from a contract broken?
 - Can we call this defamation?
 - Was someone responsible for his acts?



Digital Forensics Problems and Solutions ?

- Laws (mmm ok there are guidelines but..)
 - Balance probabilities
 - Accepted test and “procedures” jejeje
 - MD5 hashes, experts and science are only part of the picture! Never, ever, forget it!



Digital Forensics Problems and Solutions ?

- Laws (From data to evidence...)
- Digital Evidence has to be:
 - ✓ Admissible
 - ✓ Authentic
 - ✓ Accurate
 - ✓ Complete



Digital Forensics Problems and Solutions ?

- Laws (From data to evidence...)
 - Digital Evidence has to be: Admissible
 - ✓ Must conform to current legal bindings
 - ✓ Could depend on legal system!
 - ✓ Must be “proving” records



Digital Forensics Problems and Solutions ?

- Laws (From data to evidence...)
- Digital Evidence has to be: Authentic
 - ✓ Must explicitly link data to physical person
 - ✓ Must be self sustained
 - ✓ Strong access controls in place?
 - ✓ Logs and audit in good shape?
 - ✓ Supporting evidence! Colateral evidence! Building confidence! Multiple streams of evidence corroborate each other. Remember “Practical Security” in crypto world? Vernam + 1-time-pad (Red-Phone Moscow ↔ Washington)
 - ✓ Crypto used anywhere?



Digital Forensics Problems and Solutions ?

- Laws (From data to evidence...)
- Digital Evidence has to be: Accurate
 - ✓ Data process reliability determines content reliability.
 - ✓ Timming issues might throw you overboard!



Digital Forensics Problems and Solutions ?

- Laws (From data to evidence...)
 - What's so special about Digital Evidence?
 - ✓ Can be easily altered without leaving a trace
 - ✓ Can and does change withing a computer or while it's transmited
 - ✓ Can be easily changed during evidence collection
 - ✓ Perfect copies can be made
 - ✓ Can't allways be "read" or "touched"
 - ✓ It's FAAAST! No time for peer-review to determine acceptance...



Digital Forensics Problems and Solutions ?

EnCase Enterprise Edition / FIM Edition

Ok, won't go commercial promise but I think you might want to learn about this toy...

- + It provides nice solutions to some of the “problems” identified.
- + It can do some cool things like “nmap -SU -P0 -n 10.0.0.0/24” in seconds... (remember Gibson's nano probes? Make them true 😊)
- + I'm only reseller in Spain, get nothing for other europe sales 😊



NETWORK-ENABLED COMPUTER
FORENSICS FOR FIELD INVESTIGATORS



cybex

Working for Intelligence



Digital Forensics Problems and Solutions ?

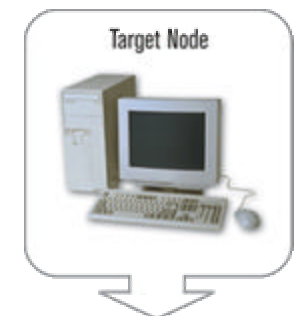
What is EnCase Enterprise Edition (EEE)?

- Based in EnCase Enterprise Edition
 - ✓ Software
 - ✓ EnCase Forensic Edition + Capacity to operate in a networked environment
- It enables examiners to:
 - ✓ Access globally to all systems connected to a network following a forensic methodology.
 - ✓ Preview concurrently multiple systems and imaging of those related to the case.
 - ✓ Access to encrypted mounted volumes of all kind.

Digital Forensics Problems and Solutions ?

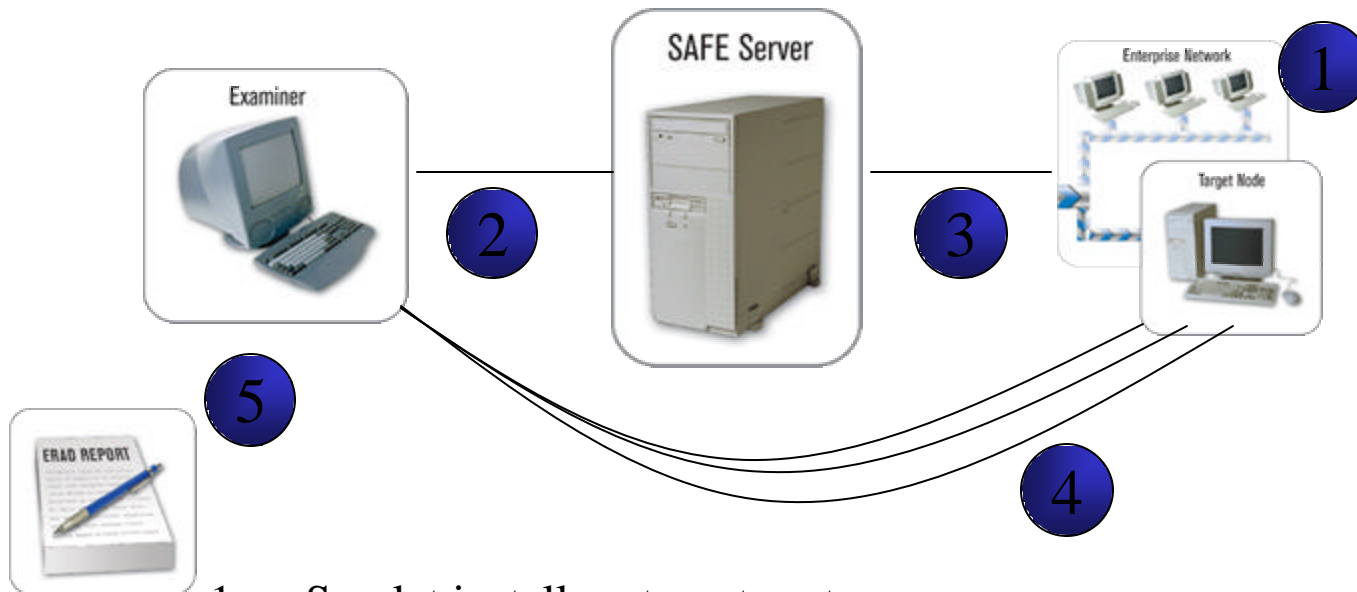
EEE Components

- EnCase SAFE
 - Complex security infrastructure
 - RBAC model
 - Public key authentication
 - PKI
 - AES
 - Transactional log of events
- EnCase Examiner
 - Based in EnCase Versión 4
 - Remote analysis enables after authenticating against a SAFE
- EnCase Servlets
 - 200kb exec distributed on corporate computers.



Digital Forensics Problems and Solutions ?

EEE Interconnection

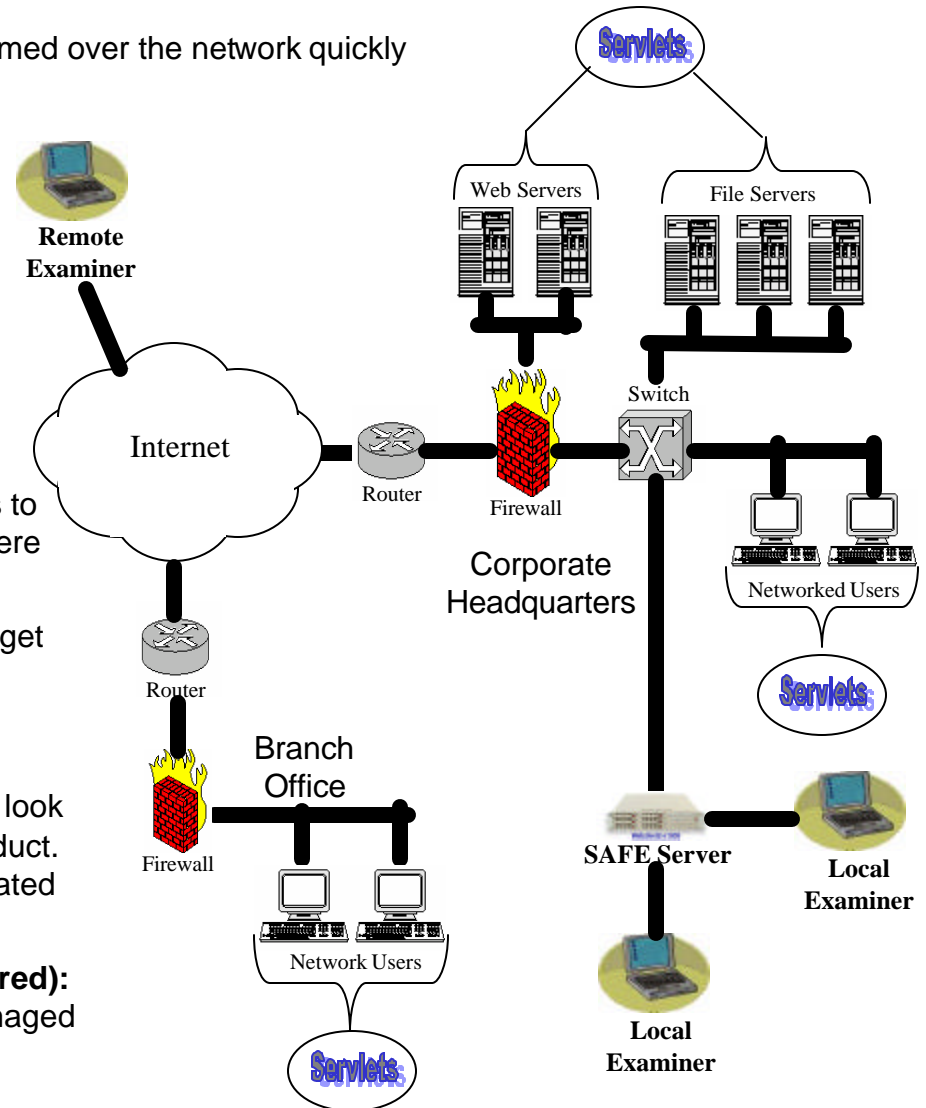


1. Servlet install on target systems
2. Examiner authenticates against the SAFE
3. SAFE authorizes access to Servlet
4. Examiner connects to Servlets through any TCP/IP network.
5. Report generation integrated.

Digital Forensics Problems and Solutions ?

- EEE allows forensics investigations to be performed over the network quickly and without disrupting normal business.

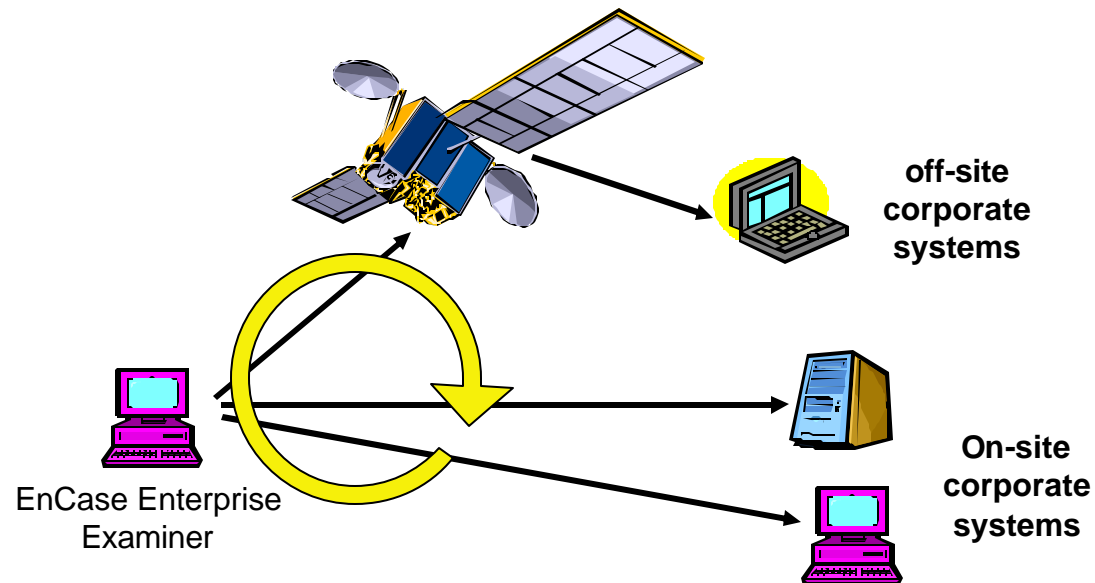
- EEE incorporates four basic elements:
 - **SAFE Server:** The SAFE Server allows users to pull disk images from target machines anywhere on the network.
 - **Servlets:** Servlets are agents deployed on target hosts. Because we do not charge by agent, customers are encouraged to deploy agents throughout their network.
 - **Examiners:** Examiners for EEE are similar in look and feel to examiners for the stand alone product. Remote examination enabled when authenticated by the SAFE.
 - **EnCase Concurrent Connection (Not pictured):** Determine the number of hosts that can be imaged at any given moment.



Digital Forensics Problems and Solutions ?

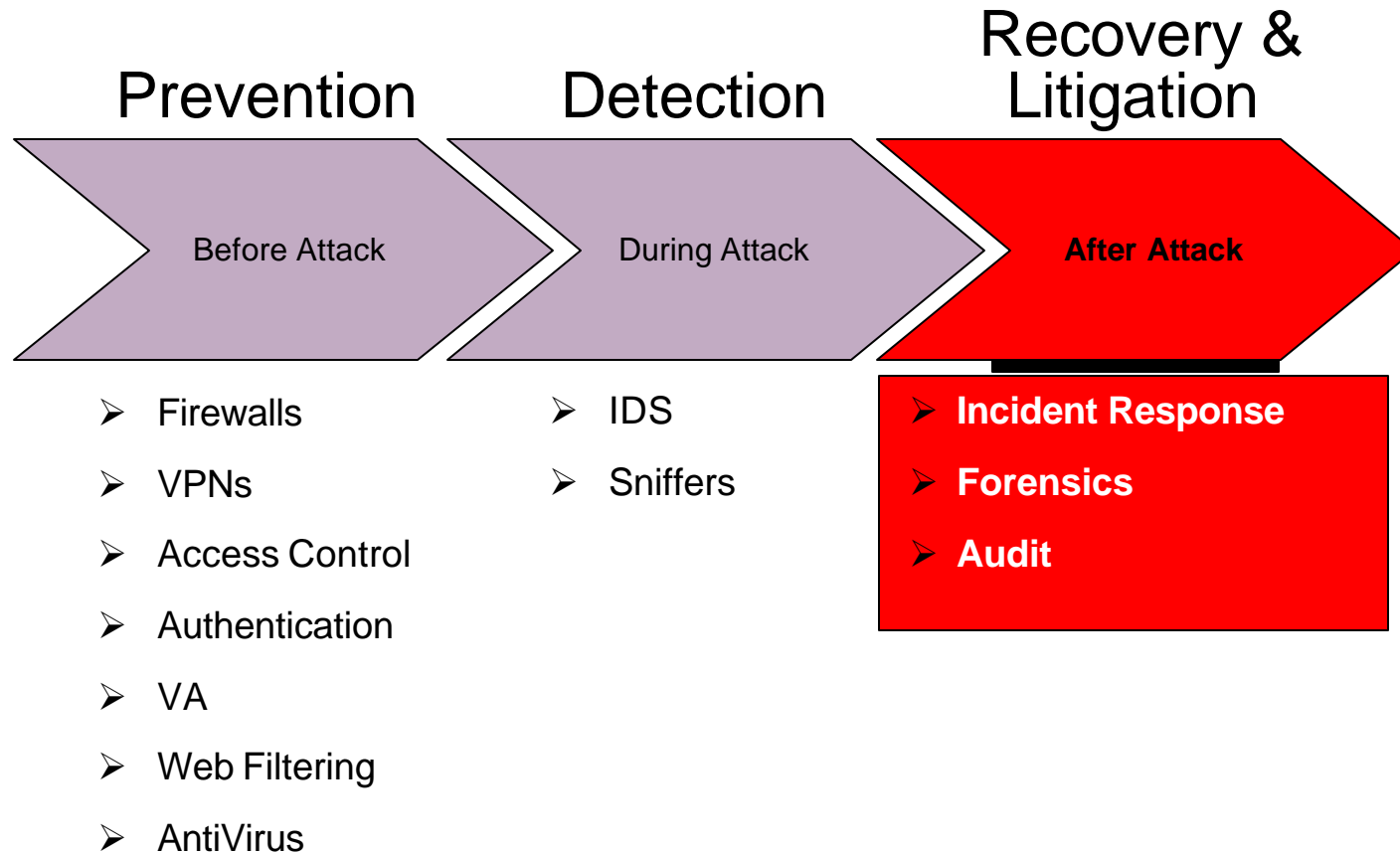
Concurrency

- EEE allows examiners to deploy the power of EnCase on any networked system in minutes.



Digital Forensics Problems and Solutions ?

Enterprise Security Timeline:





Digital Forensics Problems and Solutions ?

Incident Response:

Time sensitive investigations targeting a specific group of hosts following a network attack. Investigations incorporate the scanning of live systems and processes in order to determine at a tertiary level what systems were compromised and the extent of the changes made.

Forensics:

An in-depth investigation of a given host's memory, including deleted and hidden files, partitions, and partially over-written material in order to determine the activity that has occurred on the machine. The investigation must be conducted in a forensics manner in order to preserve the admissibility of the recovered material in the event of prosecution.

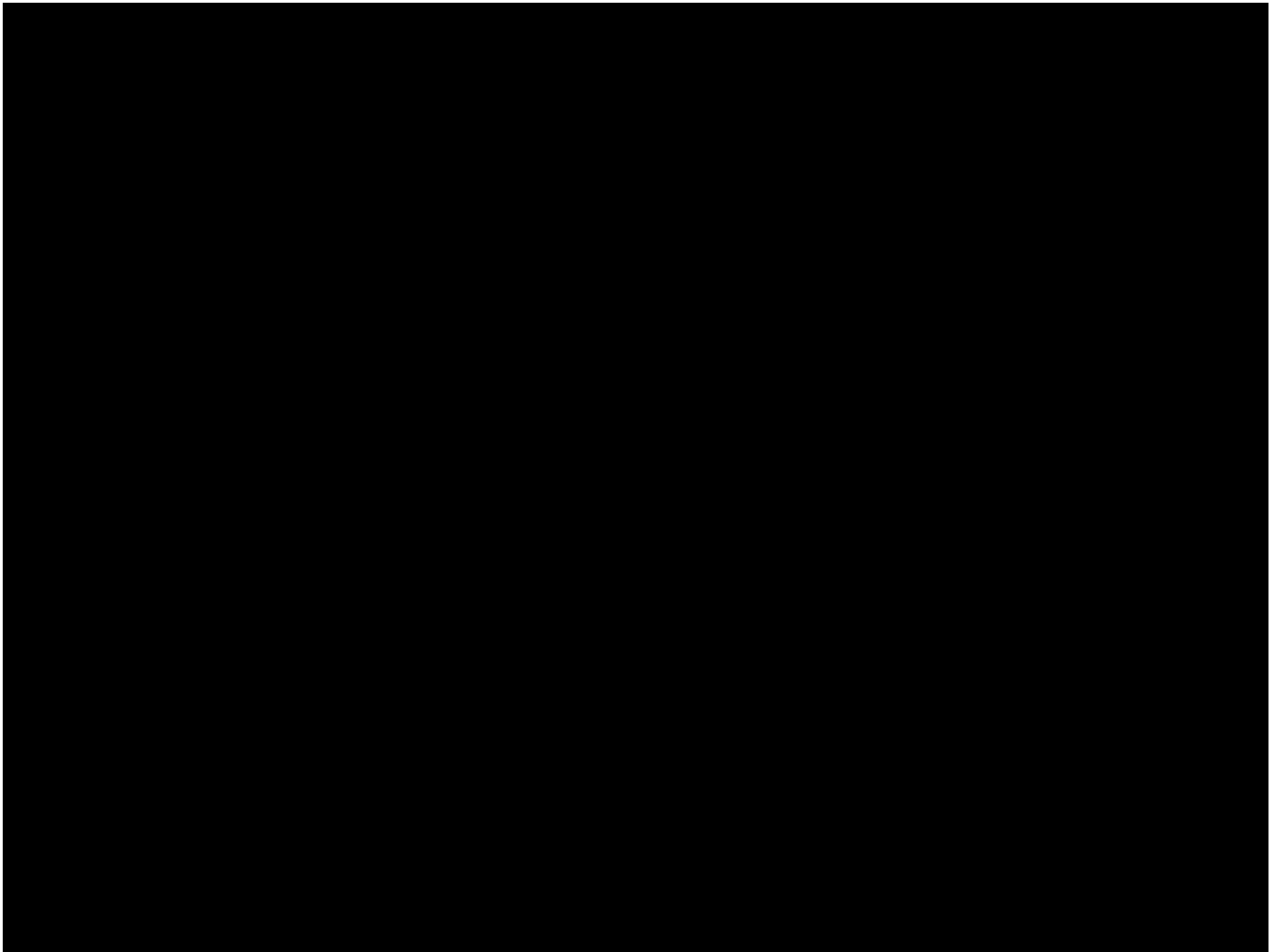
Audit:

A wide sweeping investigation of a large group of machines in order to recover or locate specific material that has been hidden or simply misplaced.



Digital Forensics Problems and Solutions ?

Questions & Answers?





cybex

Working for Intelligence