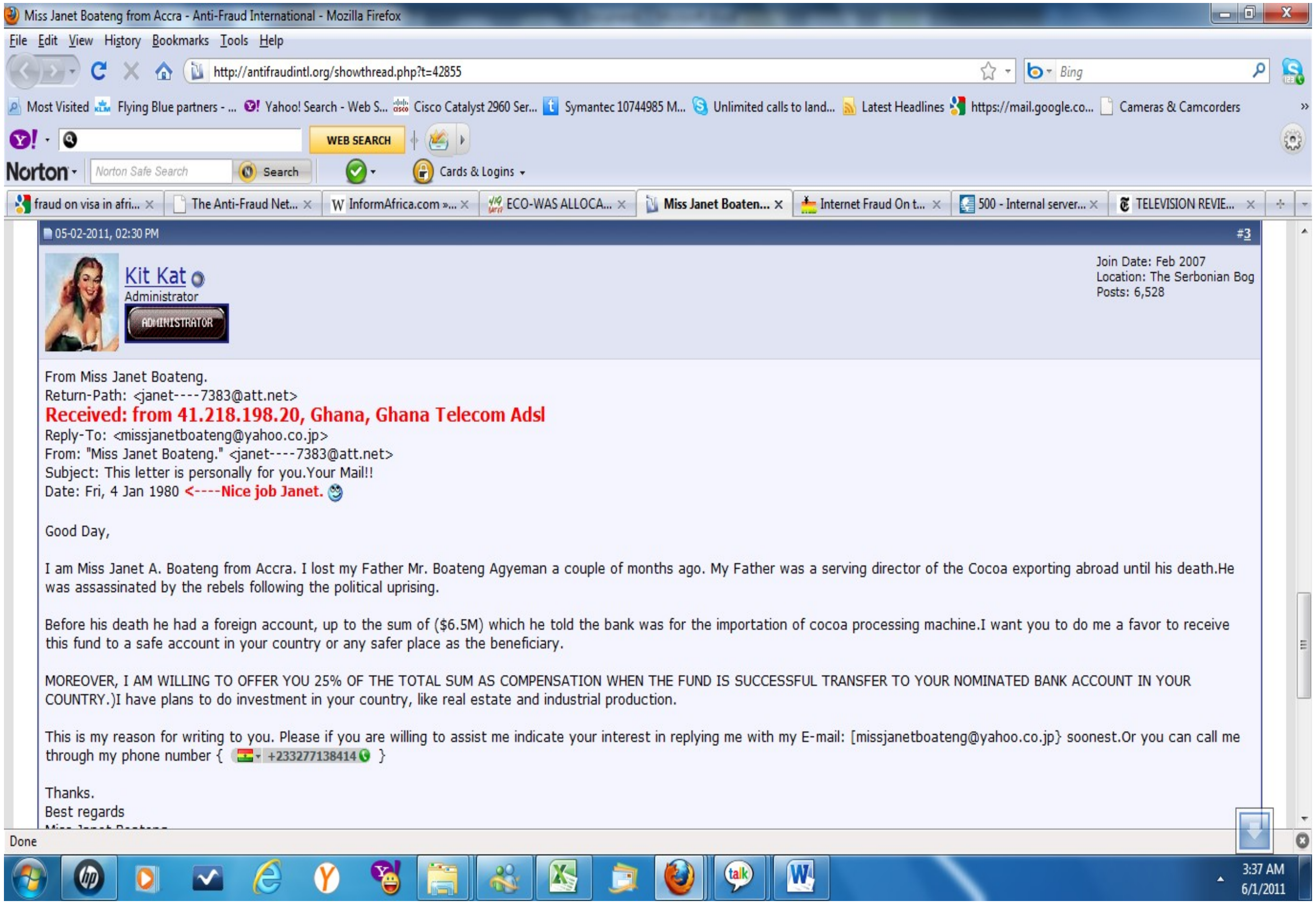
AfNOG

The African Network Operators' Group

Incident Response

CASE 1



05-02-2011, 02:30 PM #3

Kit Kat
Administrator
ADMINISTRATOR

Join Date: Feb 2007
Location: The Serbonian Bog
Posts: 6,528

From Miss Janet Boateng.
Return-Path: <janet----7383@att.net>
Received: from 41.218.198.20, Ghana, Ghana Telecom Adsl
Reply-To: <missjanetboateng@yahoo.co.jp>
From: "Miss Janet Boateng." <janet----7383@att.net>
Subject: This letter is personally for you.Your Mail!!
Date: Fri, 4 Jan 1980 **<----Nice job Janet.**

Good Day,

I am Miss Janet A. Boateng from Accra. I lost my Father Mr. Boateng Agyeman a couple of months ago. My Father was a serving director of the Cocoa exporting abroad until his death.He was assassinated by the rebels following the political uprising.

Before his death he had a foreign account, up to the sum of ($6.5M) which he told the bank was for the importation of cocoa processing machine.I want you to do me a favor to receive this fund to a safe account in your country or any safer place as the beneficiary.

MOREOVER, I AM WILLING TO OFFER YOU 25% OF THE TOTAL SUM AS COMPENSATION WHEN THE FUND IS SUCCESSFUL TRANSFER TO YOUR NOMINATED BANK ACCOUNT IN YOUR COUNTRY.)I have plans to do investment in your country, like real estate and industrial production.

This is my reason for writing to you. Please if you are willing to assist me indicate your interest in replying me with my E-mail: [missjanetboateng@yahoo.co.jp} soonest.Or you can call me through my phone number { +233277138414 }

Thanks.
Best regards

- Law enforcement
- ISP
-Cybercafe
- Company

CASE 2 : AfNOG BANK

You are a Forensic Expert (or Law enforcement officer).

A Bank has a data breach (or Credit card Fraud) and call you.

You arrive at the scene and acquire evidence and Now tryning to understand what happen.

CASE 3 : AfNOG Company financial information

- Your are a Forensics Expert.
- You have been called by AfNOG because the President is concerned that the financial informations has been altered.
- They gave you the CEO’s Computer for your investigations.

CASE 4: Cellphone involved in investigation

- Your are a Law enforcement officer.

- You doing an investigation on a crime scene and you found a cellphone.

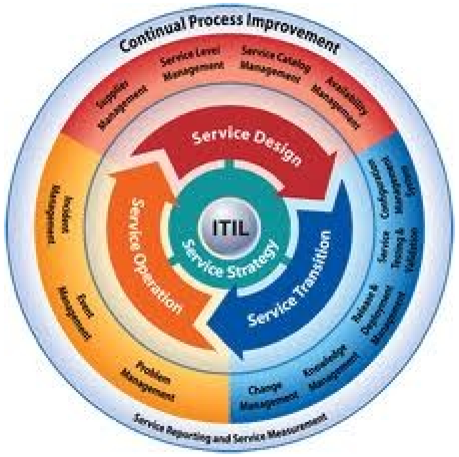
- What will you do?

Incident Definition (review)

An 'Incident' is any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

Incident Management objective (review)

The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.



Information Technology Infrastructure Library

Activities of the Incident Management process

- Incident detection and recording
- Classification and initial support
- Investigation and diagnosis
- Resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking and communication

Computer Security Incident Response Capability

- Events
  - Denial of Service
  - Malicious Code
  - Unauthorized Access
  - Inappropriate Usage

Need for Incident Response

- The following are benefits of having an incident response capability:
  - Responding to incidents systematically so that the appropriate steps are taken
  - Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services
  - Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
  - Dealing properly with legal issues that may arise during incidents.

Incident Response Policy

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and their consequences within the context of the organization
- Organizational structure and delineation of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting certain types of incidents
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

Incident Response Plan

- Mission Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization
- Metrics for measuring the incident response capability
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

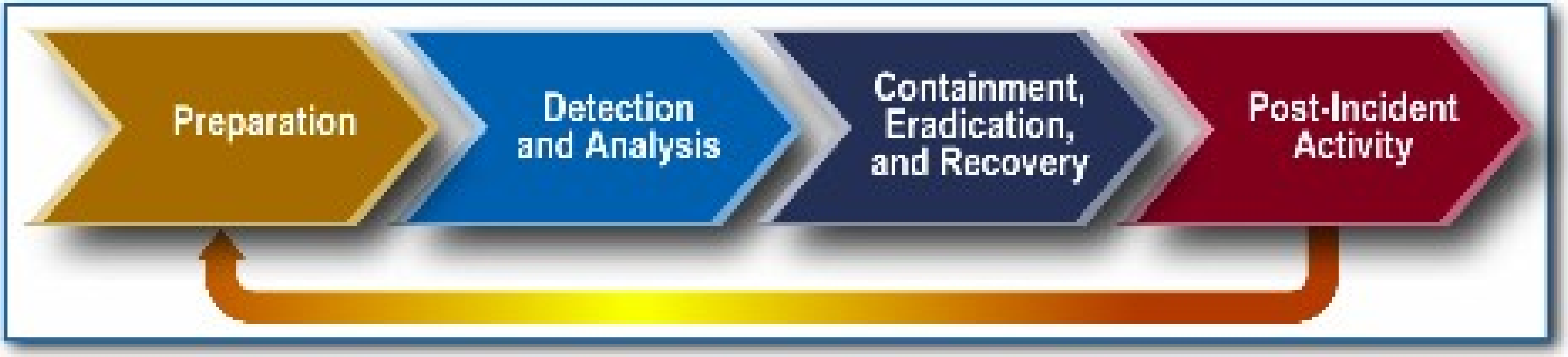
Incident Response Procedure

- Sharing information with outside parties.
- The media.
- Law Enforcement.
- Incident reporting organizations.
- Other outside parties.

Recommendations

- Establish a formal incident response capability.
- Create an incident response policy.
- Develop an incident response plan based on incident response policy.
- Develop incident response procedures.
- Establish policies and procedures regarding incident-related information sharing.
- Provide pertinent information on incidents to the appropriate organizations.
- Consider the relevant factors when selecting an incident response team.
- Select people with appropriate skills for the incident response team.
- Identify other groups within the organization that may need to participate.
- Determine which services the team should offer.

Handling an Incident



Incident Analysis

- Profile networks and systems.
- Understand normal behaviors.
- Use centralized logging and create a log retention policy.
- Perform event correlation.
- Keep all host clocks synchronized.
- Maintain and use a knowledge base of information.
- Use Internet search engines for research.
- Run packet sniffers to collect additional data.
- Consider filtering data.
- Consider experience as being irreplaceable.
- Create a diagnosis matrix for less experienced staff.
- Seek Assistance from others.

Incident Communitation Plan

- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- System owner
- Human resources (for cases involving employees)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- CERT

Criteria for determining an appropriate strategy

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Evidence Gathering and Handling

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored.

Identify the Attacker

- Validating the attackers IP address.
- Scanning the attackers system.
- Researching the attacker through search engines.
- Using incident databases.
- Monitoring possible attacker communication channels.

Lessons Learned

- Exactly what happened, and at what times?
- How well did people involved perform in dealing with the incident?
- Were the documented procedures followed?
- Were they adequate? What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would you do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Evidence Retention

- Prosecution
- Data retention
- How is data moved
- Cost

Recommendations

- Acquire tools and resources that may be of value during incident handling.
- Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure.
- Identify precursors and indications through alerts generated by several types of computer security.
- Establish mechanisms for outside parties to report incidents.
- Require a baseline level of logging and auditing on all systems, and higher baseline levels on all critical systems.
- Profile networks and systems.

Recommendations

- Understand the normal behaviors of networks, systems and applications.
- Use centralized logging and create a log retention policy.
- Perform event correlation.
- Keep all host clocks synchronized.
- Maintain and use a knowledge base of information.
- Create a diagnosis matrix for less experienced staff.
- Start recording all information as soon as the team suspects that an incident has occurred.
- Safeguard incident data.

Recommendations

- Prioritize incidents by business impact, based on the criticality of the affected resources and the technical effect of the incident.
- Include provisions regarding incident reporting in the organization’s incident response policy.
- Establish strategies and procedures for containing incidents.
- Follow established procedures for evidence gathering and handling.
- Capture volatile data from systems as evidence.
- Obtain system snapshots through full forensic disk images.
- Hold lessons learned meetings after major incidents.

Basic Incident Handling

Live Response

EXERCISE TASK

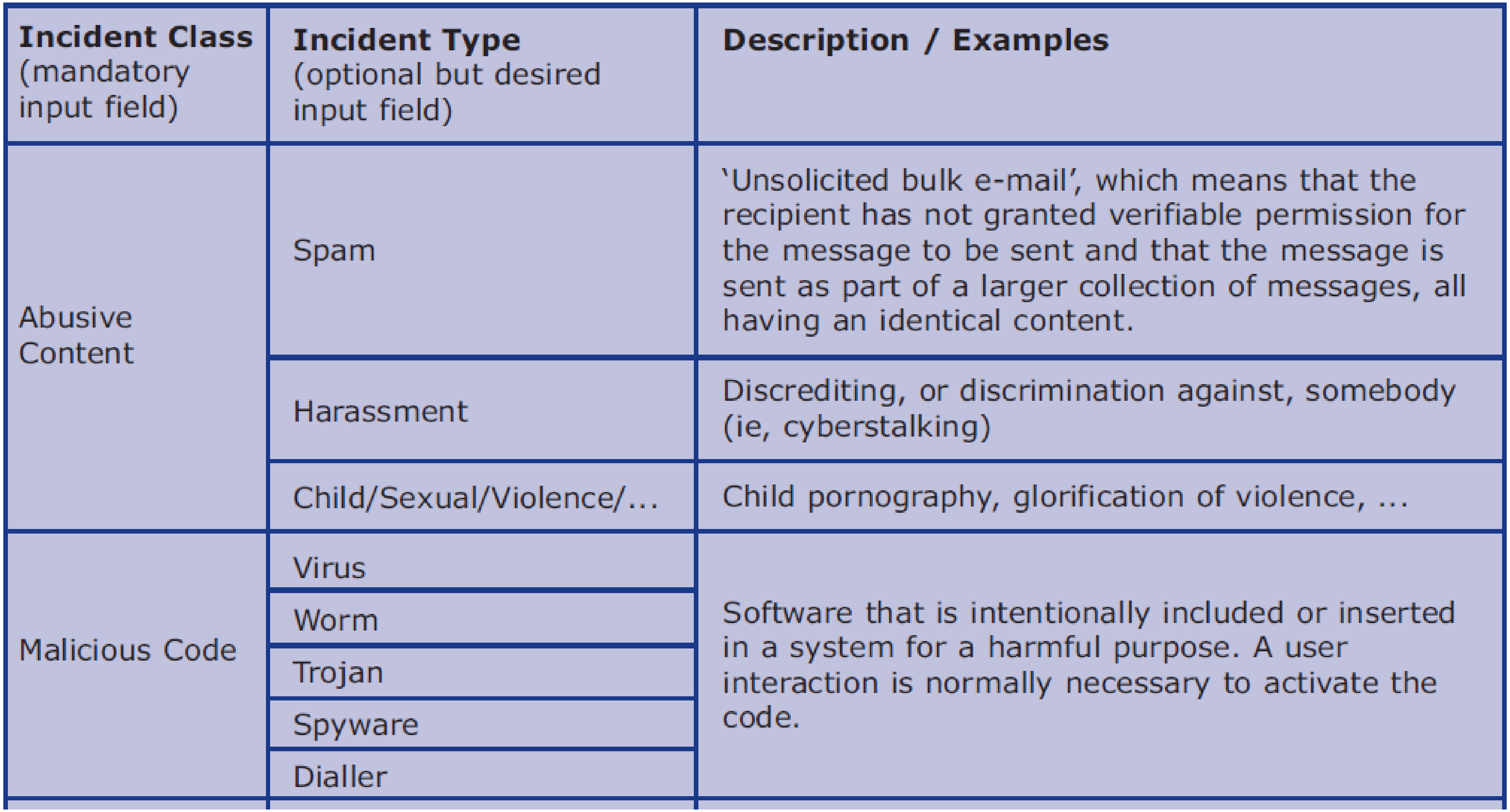
You are an incident response investigator working for AfNOG CERT.

your team is quite often approached about all security incidents happening in your country. You maintain good relationships with other providers and have secure and effective ways of sharing information with them.

You start your work at 9 am with reports in your mailbox. Read through them and try to understand what really happened and what are the reporters' expectations. How are you going to handle them? Whom will you contact and what information will you share?

For each report, assign ONE type from your classification scheme and give a priority of high, medium or low, determining the order in which you would handle the incidents. Make sure you are ready to explain your decisions and keep in mind that you are the decision-maker here – there is no single correct answer.

Incident Class



Incident Class (mandatory input field)	**Incident Type** (optional but desired input field)	**Description / Examples**
Abusive Content	Spam	'Unsolicited bulk e-mail', which means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discrediting, or discrimination against, somebody (ie, cyberstalking)
	Child/Sexual/Violence/...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	

Incident Class (cnt)

Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kinds of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, …).
	Sniffing	Observing and recording network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (eg, lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as a CVE name (eg, buffer overflow, backdoors, cross side scripting, etc).
	Login Attempts	Multiple login attempts (Guessing or cracking passwords, brute force).
	New Attack Signature	An attempt using an unknown exploit.

Classification and Priority

Analyse and Assign priorities

#	Report Subject	Classification	Priority	Suggested Actions

Live Response

Introduction

- Collection of data that will be used to confirm that there were an incident.
- Can be volatile and non volatile.
- Volatile data will not be present when we leave the scene or when we switch Equipment off.
- Non Volatile data exists even if the power is cyced can be Systems logs, files duplicated or extracted from disk etc…
- Obtained by running command and / or tools

Analyzing Volatile Data (windows)

Informations that help determine the « who », « how » and possibly « why » of the incident:

- Systems Date and Time
- Current Network Connections
- Open TCP or UDP ports
- Executables that are opening TCP/UDP ports
- Cached Netbios Name Tabe
- Users Currently logged On
- Internat Routing Table
- Routing Processes
- Running services
- Scheduled Jobs
- Open Files
- Process Memory dumps

Analyzing Volatile Data (Unix like OS)

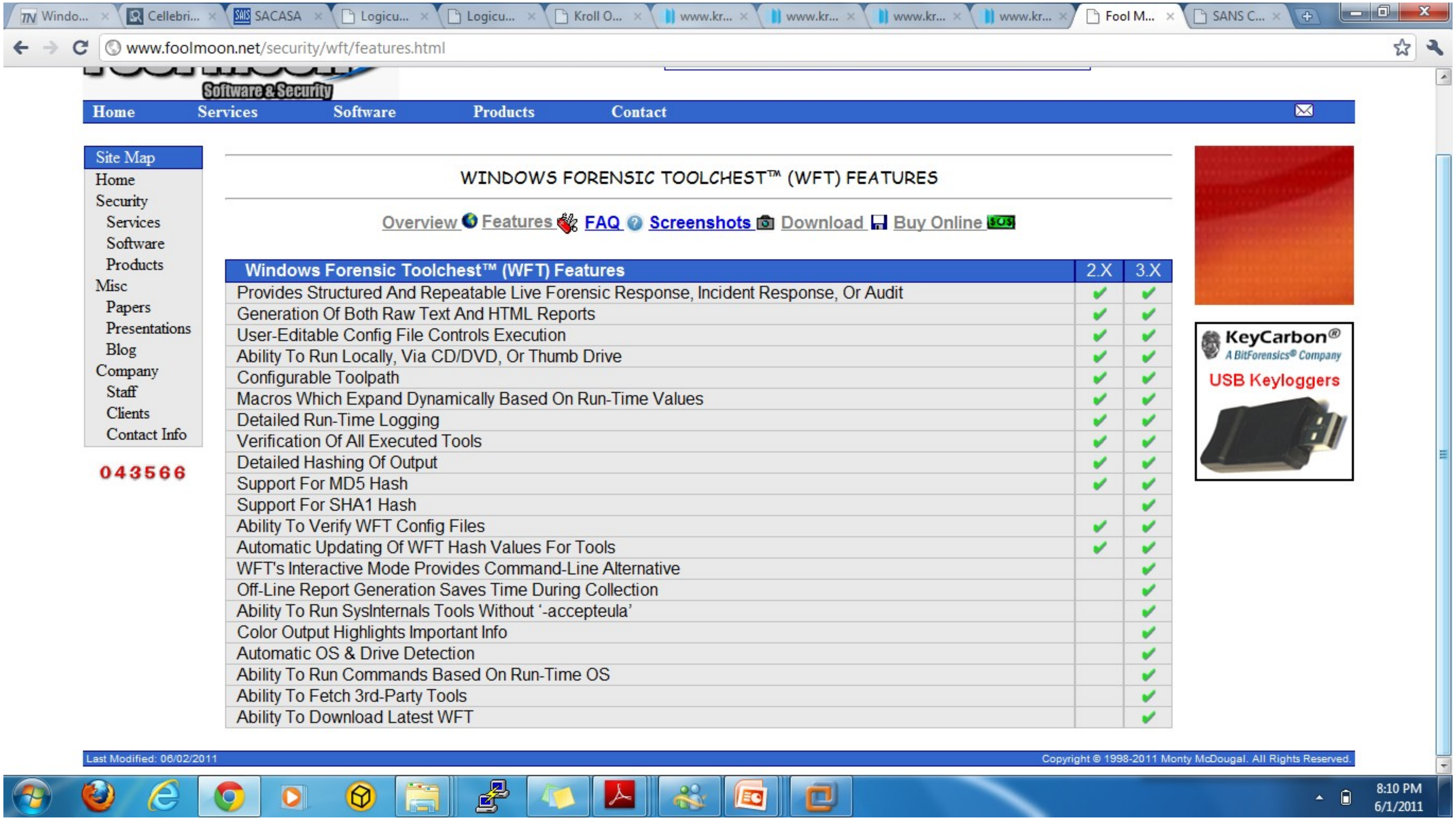
Some commands are similar to windows.

- System time and date
- Current network connections
- Open TCP and UDP ports
- Executables opening TCP and UDP ports
- Running processes
- Open files
- Internal routing table
- Loaded kernel modules
- Mounted file systems

Tools

- The COFEE, which stands for Computer Online Forensic Evidence Extractor, is a USB "thumb drive" that was quietly distributed to a handful of law-enforcement agencies last June. Microsoft General Counsel Brad Smith described its use to the 350 law-enforcement experts attending a company conference Monday.The device contains 150 commands that can dramatically cut the time it takes to gather digital evidence, which is becoming more important in real-world crime, as well as cybercrime. It can decrypt passwords and analyze a computer's Internet activity, as well as data stored in the computer.
- It also eliminates the need to seize a computer itself, which typically involves disconnecting from a network, turning off the power and potentially losing data. Instead, the investigator can scan for evidence on site.

Tools (I will run wft –noslow)



WINDOWS FORENSIC TOOLCHEST™ (WFT) FEATURES

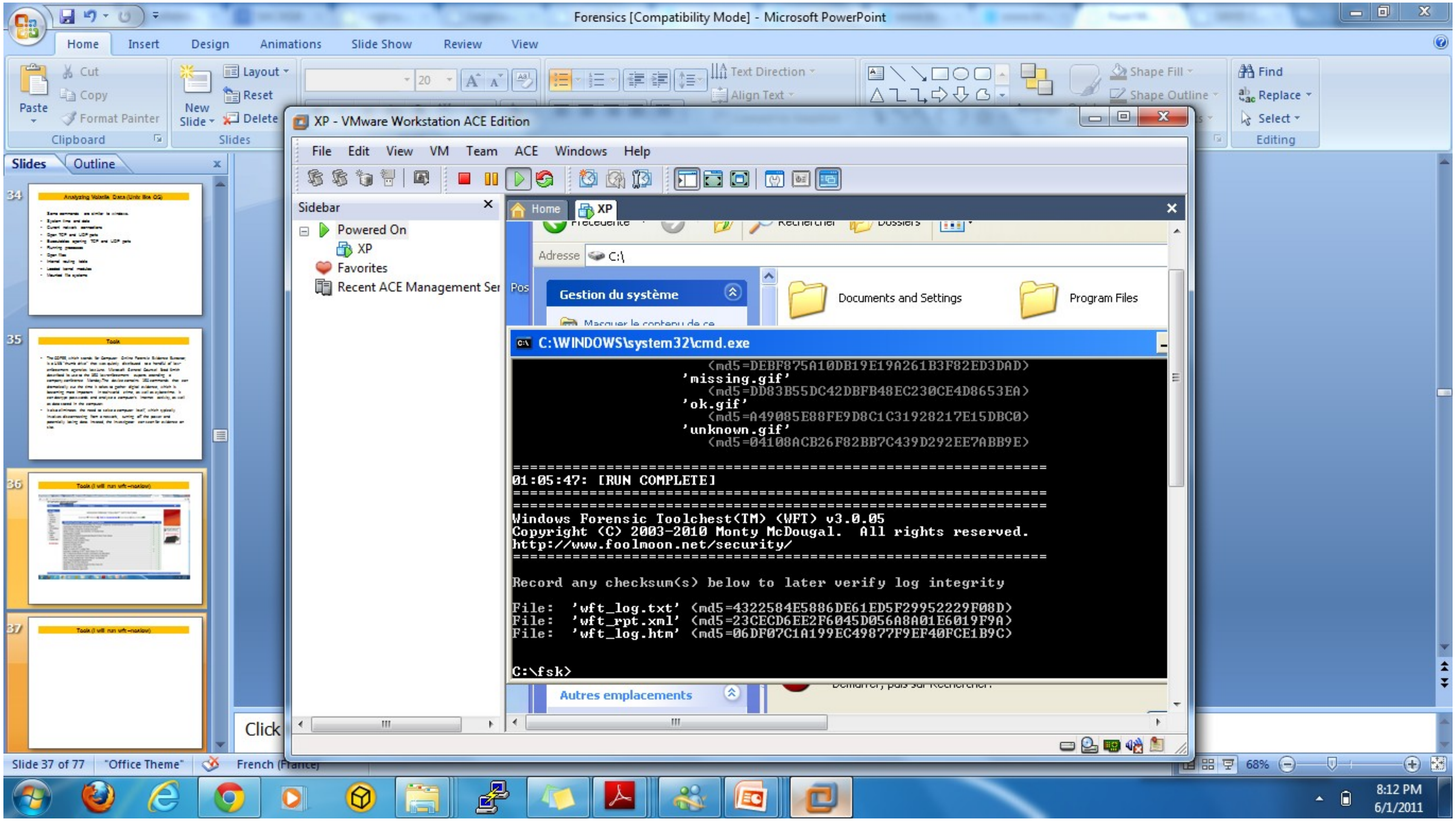
Overview Features FAQ Screenshots Download Buy Online

Windows Forensic Toolchest™ (WFT) Features	2.X	3.X
Provides Structured And Repeatable Live Forensic Response, Incident Response, Or Audit	✓	✓
Generation Of Both Raw Text And HTML Reports	✓	✓
User-Editable Config File Controls Execution	✓	✓
Ability To Run Locally, Via CD/DVD, Or Thumb Drive	✓	✓
Configurable Toolpath	✓	✓
Macros Which Expand Dynamically Based On Run-Time Values	✓	✓
Detailed Run-Time Logging	✓	✓
Verification Of All Executed Tools	✓	✓
Detailed Hashing Of Output	✓	✓
Support For MD5 Hash	✓	✓
Support For SHA1 Hash		✓
Ability To Verify WFT Config Files	✓	✓
Automatic Updating Of WFT Hash Values For Tools	✓	✓
WFT's Interactive Mode Provides Command-Line Alternative		✓
Off-Line Report Generation Saves Time During Collection		✓
Ability To Run SysInternals Tools Without '-accepteula'		✓
Color Output Highlights Important Info		✓
Automatic OS & Drive Detection		✓
Ability To Run Commands Based On Run-Time OS		✓
Ability To Fetch 3rd-Party Tools		✓
Ability To Download Latest WFT		✓

Last Modified: 06/02/2011

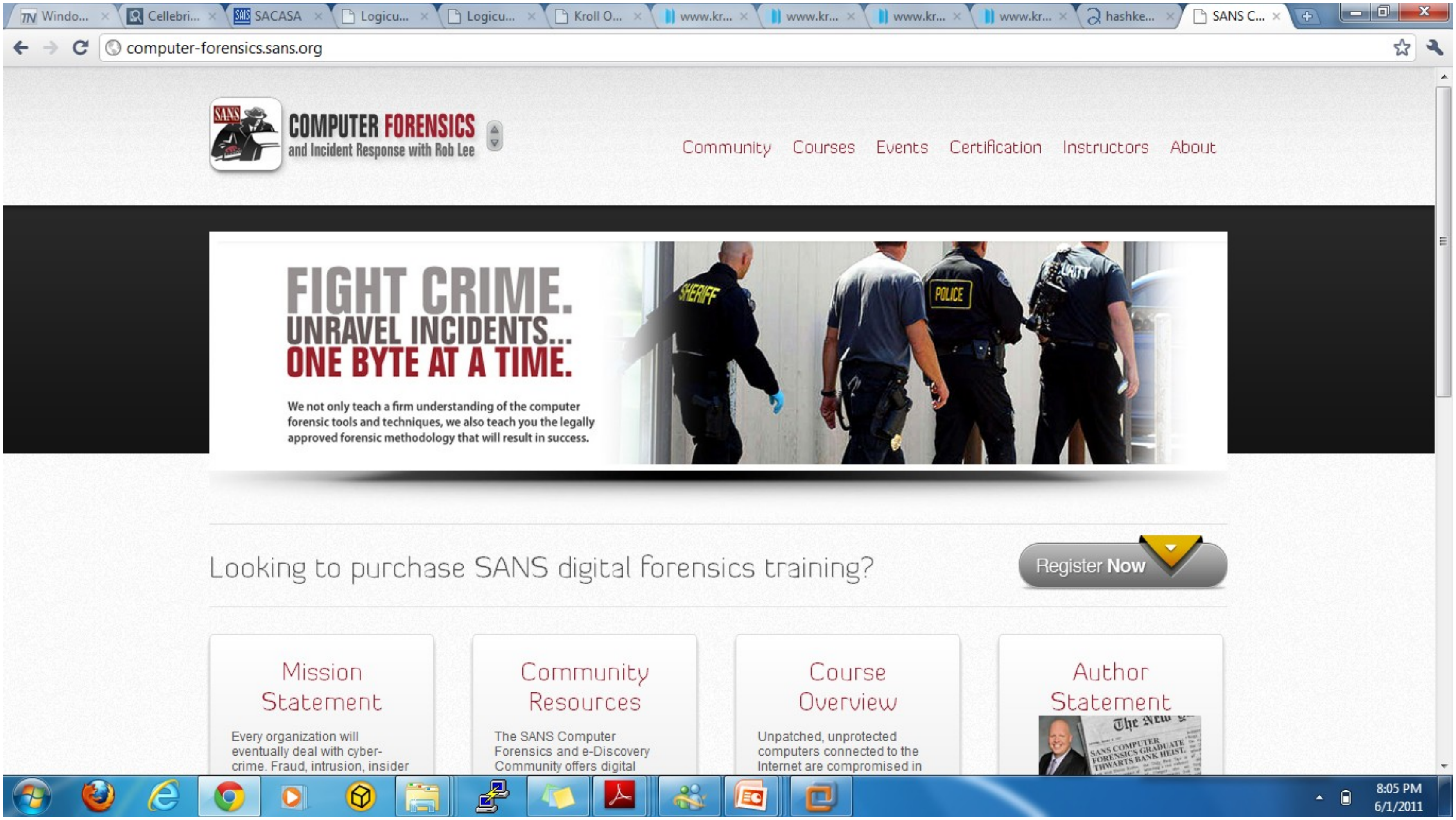
Copyright © 1998-2011 Monty McDougal. All Rights Reserved.

Tools (I will run wft –noslow)



```
                       <md5=DEBF875A10DB19E19A261B3F82ED3DAD>
                    'missing.gif'
                       <md5=DD83B55DC42DBFB48EC230CE4D8653EA>
                    'ok.gif'
                       <md5=A49085E88FE9D8C1C31928217E15DBC0>
                    'unknown.gif'
                       <md5=04108ACB26F82BB7C439D292EE7ABB9E>

===============================================================
01:05:47: [RUN COMPLETE]
===============================================================
===============================================================
Windows Forensic Toolchest(TM) (WFT) v3.0.05
Copyright (C) 2003-2010 Monty McDougal.  All rights reserved.
http://www.foolmoon.net/security/
===============================================================

Record any checksum(s) below to later verify log integrity

File:  'wft_log.txt' <md5=4322584E5886DE61ED5F29952229F08D>
File:  'wft_rpt.xml' <md5=23CECD6EE2F6045D056A8A01E6019F9A>
File:  'wft_log.htm' <md5=06DF07C1A199EC49877F9EF40FCE1B9C>


C:\fsk>
```

Tools



FIGHT CRIME.
UNRAVEL INCIDENTS...
ONE BYTE AT A TIME.

We not only teach a firm understanding of the computer forensic tools and techniques, we also teach you the legally approved forensic methodology that will result in success.

Looking to purchase SANS digital forensics training?

Mission Statement

Every organization will eventually deal with cyber-crime. Fraud, intrusion, insider

Community Resources

The SANS Computer Forensics and e-Discovery Community offers digital

Course Overview

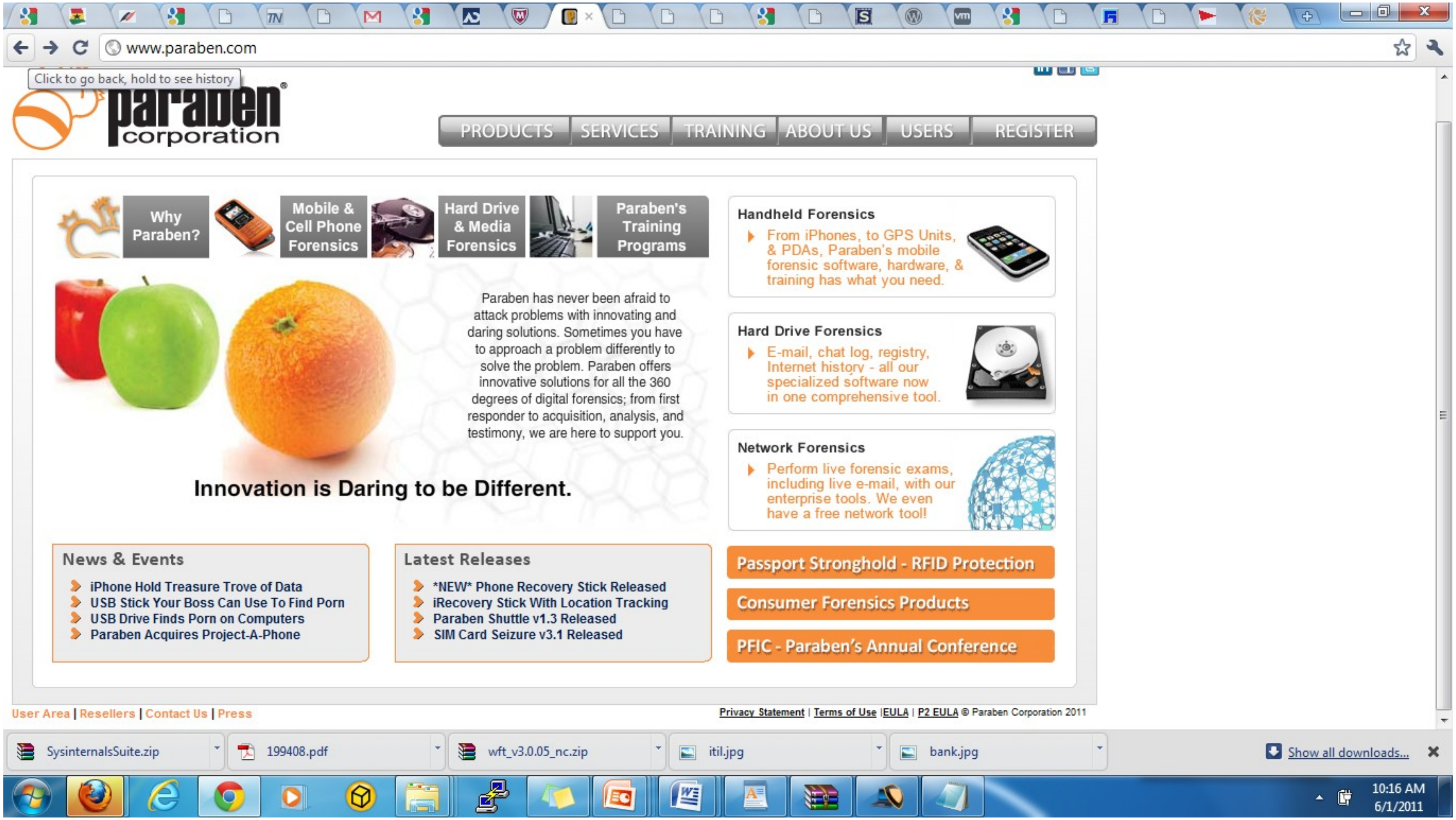
Unpatched, unprotected computers connected to the Internet are compromised in

Author Statement

The New

SANS COMPUTER FORENSICS GRADUATE THWARTS BANK HEIST.

Tools


www.paraben.com
Click to go back, hold to see history
paraben corporation
PRODUCTS
SERVICES
TRAINING
ABOUT US
USERS
REGISTER
Why Paraben?
Mobile & Cell Phone Forensics
Hard Drive & Media Forensics
Paraben's Training Programs

Paraben has never been afraid to attack problems with innovating and daring solutions. Sometimes you have to approach a problem differently to solve the problem. Paraben offers innovative solutions for all the 360 degrees of digital forensics; from first responder to acquisition, analysis, and testimony, we are here to support you.

Innovation is Daring to be Different.

Handheld Forensics

- From iPhones, to GPS Units, & PDAs, Paraben's mobile forensic software, hardware, & training has what you need.

Hard Drive Forensics

- E-mail, chat log, registry, Internet history - all our specialized software now in one comprehensive tool.

Network Forensics

- Perform live forensic exams, including live e-mail, with our enterprise tools. We even have a free network tool!

News & Events

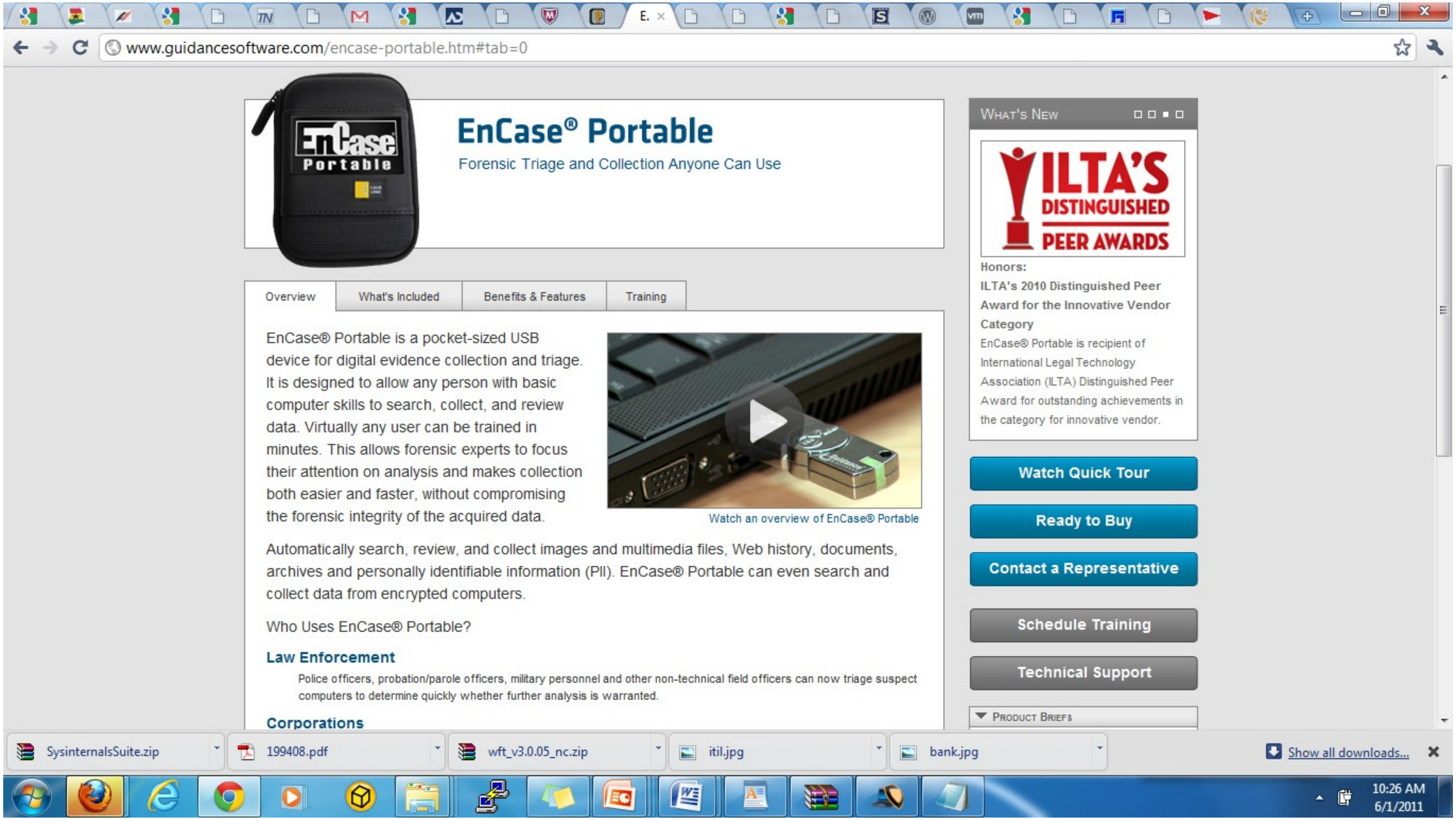
- iPhone Hold Treasure Trove of Data
- USB Stick Your Boss Can Use To Find Porn
- USB Drive Finds Porn on Computers
- Paraben Acquires Project-A-Phone

Latest Releases

- *NEW* Phone Recovery Stick Released
- iRecovery Stick With Location Tracking
- Paraben Shuttle v1.3 Released
- SIM Card Seizure v3.1 Released

Passport Stronghold - RFID Protection
Consumer Forensics Products
PFIC - Paraben's Annual Conference
User Area | Resellers | Contact Us | Press
Privacy Statement | Terms of Use |EULA | P2 EULA © Paraben Corporation 2011
SysinternalsSuite.zip
199408.pdf
wft_v3.0.05_nc.zip
itil.jpg
bank.jpg
Show all downloads...
10:16 AM
6/1/2011

Tools



EnCase® Portable

Forensic Triage and Collection Anyone Can Use

EnCase® Portable is a pocket-sized USB device for digital evidence collection and triage. It is designed to allow any person with basic computer skills to search, collect, and review data. Virtually any user can be trained in minutes. This allows forensic experts to focus their attention on analysis and makes collection both easier and faster, without compromising the forensic integrity of the acquired data.

Watch an overview of EnCase® Portable

Automatically search, review, and collect images and multimedia files, Web history, documents, archives and personally identifiable information (PII). EnCase® Portable can even search and collect data from encrypted computers.

Who Uses EnCase® Portable?

Law Enforcement

Police officers, probation/parole officers, military personnel and other non-technical field officers can now triage suspect computers to determine quickly whether further analysis is warranted.

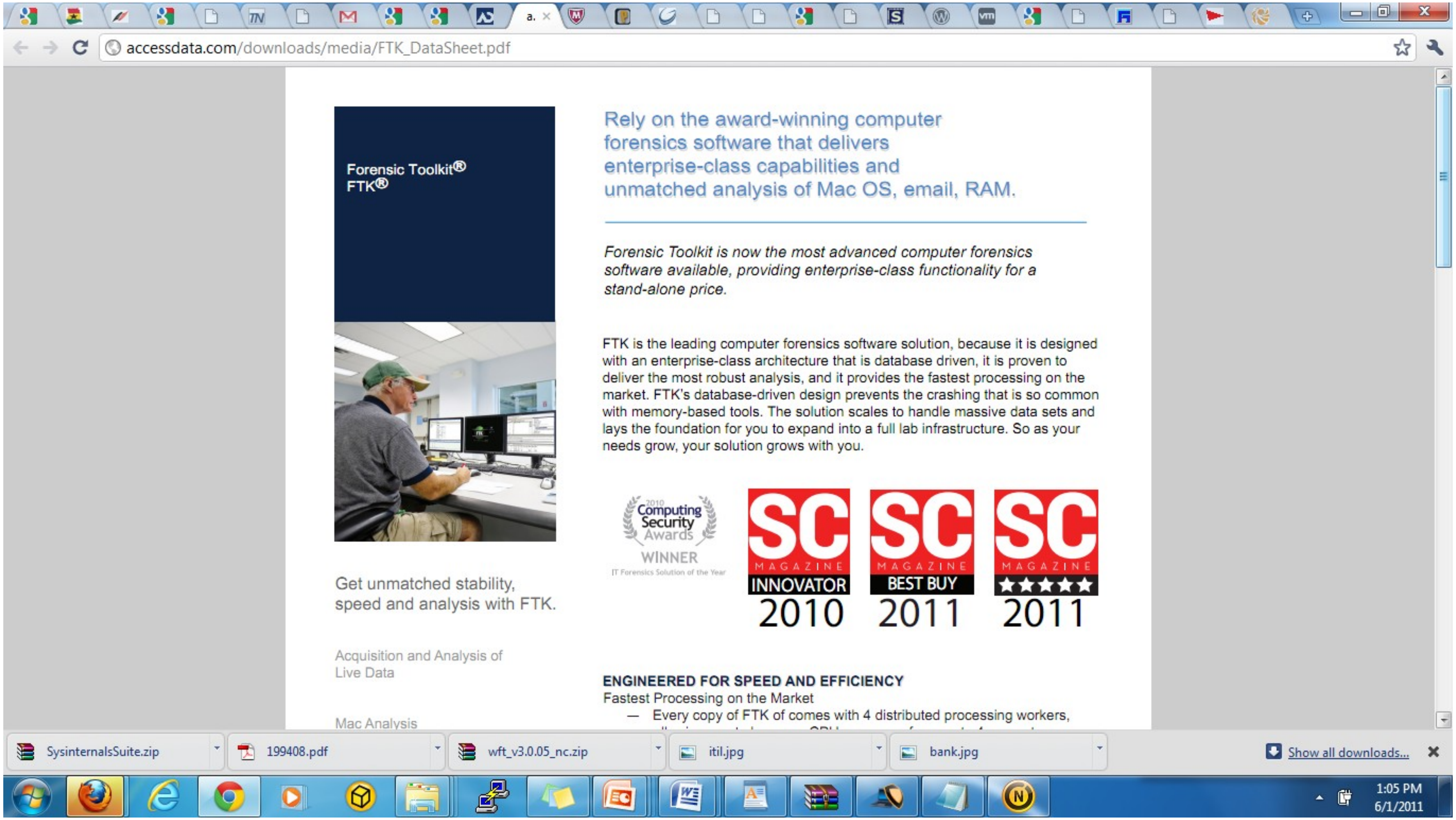
Corporations

Honors:

ILTA's 2010 Distinguished Peer Award for the Innovative Vendor Category

EnCase® Portable is recipient of International Legal Technology Association (ILTA) Distinguished Peer Award for outstanding achievements in the category for innovative vendor.

Tools



accessdata.com/downloads/media/FTK_DataSheet.pdf

Forensic Toolkit®
FTK®

Get unmatched stability, speed and analysis with FTK.

Acquisition and Analysis of Live Data

Mac Analysis

Rely on the award-winning computer forensics software that delivers enterprise-class capabilities and unmatched analysis of Mac OS, email, RAM.

Forensic Toolkit is now the most advanced computer forensics software available, providing enterprise-class functionality for a stand-alone price.

FTK is the leading computer forensics software solution, because it is designed with an enterprise-class architecture that is database driven, it is proven to deliver the most robust analysis, and it provides the fastest processing on the market. FTK's database-driven design prevents the crashing that is so common with memory-based tools. The solution scales to handle massive data sets and lays the foundation for you to expand into a full lab infrastructure. So as your needs grow, your solution grows with you.

2010 Computing Security Awards
WINNER
IT Forensics Solution of the Year
SC MAGAZINE INNOVATOR 2010
SC MAGAZINE BEST BUY 2011
SC MAGAZINE ★★★★★ 2011

ENGINEERED FOR SPEED AND EFFICIENCY
Fastest Processing on the Market
— Every copy of FTK of comes with 4 distributed processing workers,

Transferring Collected data

- There are two main ways data can be transmitted from a victim computer to a forensics workstation.
  - The Swiss army knife (netcat)
    - Creates a TCP channel
    - Start server syntax (nc –v –l –p #### > command.txt)
      - -v = verbose | -l = listen | -p = port
    - Victim request syntax (command | nc ip_address port)
  - Cryptcat
    - Same function as netcat except creates an encrypted channel

Collecting Data with Windows

System Date and Time

- One of the most important information. (Can be easily missed).
- Keeping the system time and noting the offset from a trusted source (such as a reliable NTP server) is a paramount when examining log files or other time-based evidence from multiple servers
- Command:
  - *Date*
  - *Time*

```
**********************
***** Start Date *****
**********************
The current date is: Wed 06/01/2003
Enter the new date: (mm-dd-yy)
**********************
***** Start Time *****
**********************
The current time is: 21:58:19.29
Enter the new time:
```

Current Network Connections

- View a computer’s network connections by issuing the netstat command.

- It could be possibe that the attacker is using your computer against other computers on the internet.

- Netstat –an

Current Network Connections

```
Proto  Local Address              Foreign Address         State
TCP    103.98.91.41:445           95.208.123.64:3762      ESTABLISHED
TCP    103.98.91.41:1033          95.208.123.64:21        CLOSE_WAIT
TCP    103.98.91.41:1174          95.145.128.17:6667      ESTABLISHED
TCP    103.98.91.41:1465          95.208.123.64:3753      ESTABLISHED
TCP    103.98.91.41:3992          95.208.123.64:445       TIME_WAIT
TCP    103.98.91.41:4151          103.98.91.200:2222      ESTABLISHED
TCP    103.98.91.41:60906         95.16.3.23:1048         ESTABLISHED
```

Active Connections

445 = windows netbios – 95.208.123.64 could be connecting to a file share

```
TCP    103.98.91.41:1033          95.208.123.64:21        CLOSE_WAIT
```

The computer is doing FTP on 95.208.123.64

```
TCP    103.98.91.41:1174          95.145.128.17:6667      ESTABLISHED
```

IRC server

Open TCP / UDP ports

- Open TCP and UDP ports
  - Open rouge ports usually denotes a backdoor running on the victim machine.

- Executables opening TCP or UDP ports
  - Fport or Vision v1.0

  Available at www.foundstone.com

```
1224  iroffer      ->  1174  TCP   C:\WINNT\system32\os2\dll\iroffer.exe
1224  iroffer      ->  1465  TCP   C:\WINNT\system32\os2\dll\iroffer.exe
```

An IRC server involved

Cached Netbios Name

- Windows to Version 2003 stores connections specifics by Netbios Name rather than IP.
- Issue the nbstat command during a live response to dump the remote machine’s NetBIOS name cache. Note this will only show the table cache and NOT the complete history of connections.

```
**********************
***** nbtstat -c *****
**********************
Local Area Connection:
Node IpAddress: [103.98.91.41] Scope Id: []
NetBIOS Remote Cache Name Table
 Name              Type       Host Address    Life [sec]
 ----------------------------------------------------------
95.208.123.64  <20>  UNIQUE        95.208.123.64      562
```

USERS CURRENTLY LOGGED ON

- Displaying users logged on can tell us who is accessing ressources.
- Use psloggedon to display currently logged on users or accessing resource shares.
  - Part of pstools available at www.systernals.com

```
********************
***** psloggedon *****
********************


PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
 8/23/2003 3:32:53 PM    JBRWWW\Administrator

Users logged on via resource shares:
10/1/2003 9:52:26 PM    (null)\ADMINISTRATOR
**********************
***** File Times *****
**********************
```

First Analysis

With this someone is logged von the system

Users logged on via resource shares:

10/1/2003 9:52:26 PM (null)\ADMINISTRATOR

Let' s return to our connection

```
 TCP    103.98.91.41:445          95.208.123.64:3762          ESTABLISHED
```

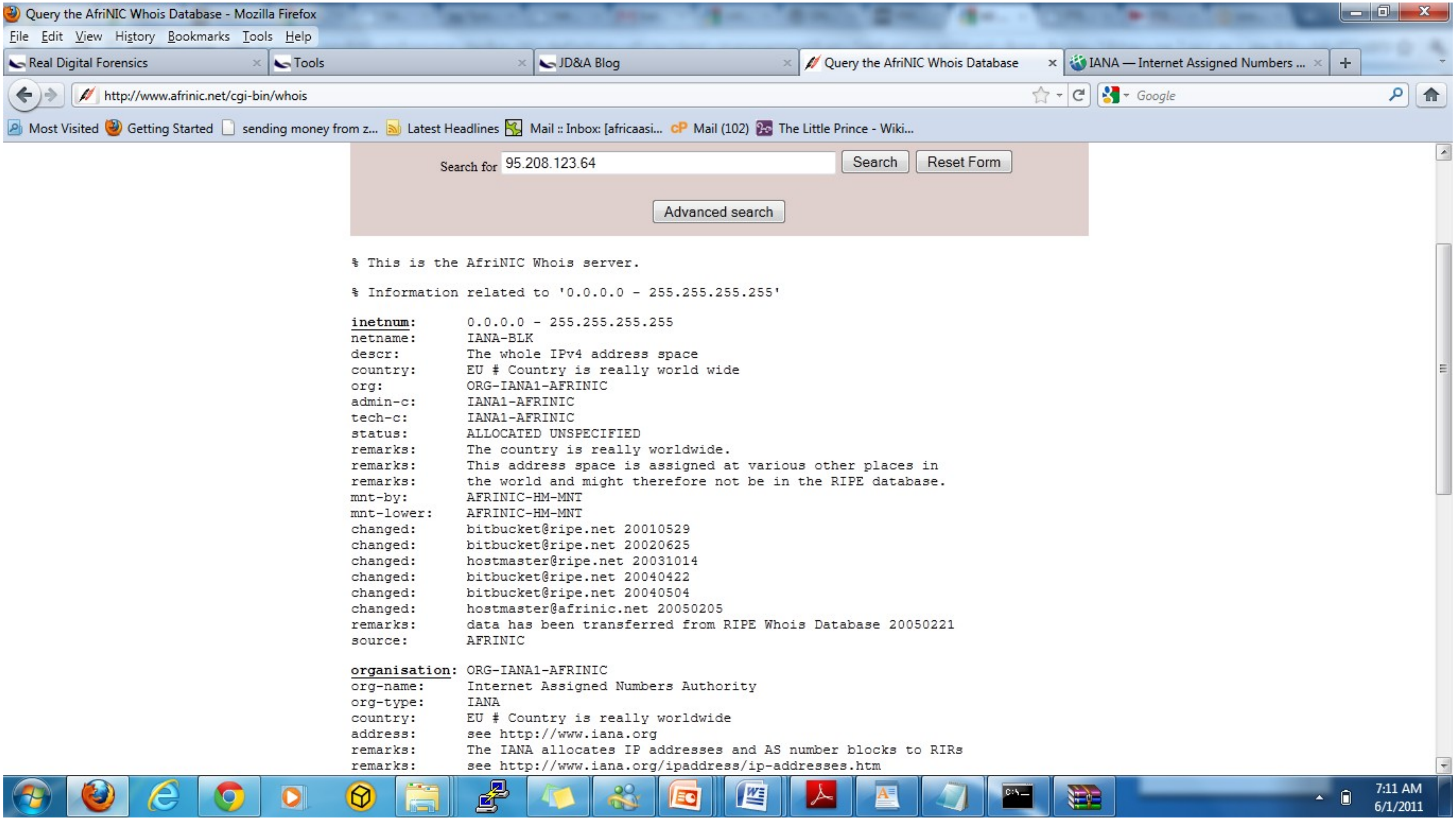
We are sure that the person is **905.208.123.64**

Let's locate the owner of the IP

www.iana.org (search range)

www.afrinic.net (search on whois)

First Analysis



Query the AfriNIC Whois Database - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Real Digital Forensics
Tools
JD&A Blog
Query the AfriNIC Whois Database
IANA — Internet Assigned Numbers ...
http://www.afrinic.net/cgi-bin/whois
Google
Most Visited
Getting Started
sending money from z...
Latest Headlines
Mail :: Inbox: [africaasi...
Mail (102)
The Little Prince - Wiki...
Search
Reset Form
Advanced search
7:11 AM
6/1/2011

Search for 95.208.123.64

```
% This is the AfriNIC Whois server.

% Information related to '0.0.0.0 - 255.255.255.255'

inetnum:      0.0.0.0 - 255.255.255.255
netname:      IANA-BLK
descr:        The whole IPv4 address space
country:      EU # Country is really world wide
org:          ORG-IANA1-AFRINIC
admin-c:      IANA1-AFRINIC
tech-c:       IANA1-AFRINIC
status:       ALLOCATED UNSPECIFIED
remarks:      The country is really worldwide.
remarks:      This address space is assigned at various other places in
remarks:      the world and might therefore not be in the RIPE database.
mnt-by:       AFRINIC-HM-MNT
mnt-lower:    AFRINIC-HM-MNT
changed:      bitbucket@ripe.net 20010529
changed:      bitbucket@ripe.net 20020625
changed:      hostmaster@ripe.net 20031014
changed:      bitbucket@ripe.net 20040422
changed:      bitbucket@ripe.net 20040504
changed:      hostmaster@afrinic.net 20050205
remarks:      data has been transferred from RIPE Whois Database 20050221
source:       AFRINIC

organisation: ORG-IANA1-AFRINIC
org-name:     Internet Assigned Numbers Authority
org-type:     IANA
country:      EU # Country is really worldwide
address:      see http://www.iana.org
remarks:      The IANA allocates IP addresses and AS number blocks to RIRs
remarks:      see http://www.iana.org/ipaddress/ip-addresses.htm
```

Running Process

- We would like to know what process are running. That could show or contain backdoors or further the attacker's efforts into the victims network.
- Processes are can be listed using pslist from the pstools suite (pslist)

```
PSEXESVC    892   8   6   63   1008   0:00:00.010   0:00:00.030
    2:41:47.564
cmd       1272  8  1  25   984  0:00:00.020  0:00:00.030   2:41:15.969
ftp      1372  8  1  39  1176  0:00:00.020  0:00:00.020   2:39:05.861
cmd       1160  8  1  28   976  0:00:00.020  0:00:00.010   2:24:25.536
nc       1424  8  3  40  1012  0:00:00.010  0:00:00.040   2:23:39.800
cmd       1092  8  1  34   968  0:00:00.010  0:00:00.020   2:22:03.992
iroffer   1224  8  5  95  2564  0:00:00.090  0:00:00.200   2:21:30.544
```

Internal Routing Table

- Attackers alter the route tables to redirect traffic in some manner.

- Rerouting traffic can avoid security devices such as firewalls and IDS/IPS.

- Examine the routing table by issuing the netstat command.
  - Syntax (netstat –rn)

- Can also use “route print” on Windows 2k|Windows 2k3 or Windows XP

Running services and Scheduled Job

- Use psservice from the pstools suite to list running services
  - Syntax (psservice)
- Scheduled jobs enable an attacker to run commands when he/she is not even on the compromised machine.
  - Use “at” to display scheduled jobs

```
**************
***** at *****
**************
There are no entries in the list.
```

Open Files

Listing open files may help determine more information pertinent to an investigation.
Use psfile to obtain a list of open files. (psfile)

```
***** psfile *****
******************


PsFile v1.01 - local and remote network file lister
Copyright (C) 2001 Mark Russinovich
Sysinternals - www.sysinternals.com

Files opened remotely on JBRWWW:

[100] \PIPE\psexecsvc
    User:   ADMINISTRATOR
    Locks:  0
    Access: Read Write
[101] \PIPE\psexecsvc-CAINE-2936-stdin
    User:   ADMINISTRATOR
    Locks:  0
    Access: Write
[102] \PIPE\psexecsvc-CAINE-2936-stdout
    User:   ADMINISTRATOR
    Locks:  0
    Access: Read
[103] \PIPE\psexecsvc-CAINE-2936-stderr
    User:   ADMINISTRATOR
    Locks:  0
    Access: Read
```

Memory Dumps

- Traditionally incident response and forensics investigators rarely collect the memory space utilized by suspect processes from Windows systems.

- This is primarily due to the lack of documented methods, techniques, and tools for this process

- But the tool can provide additional information.

- Microsoft provides a utility called userdump.exe for Windows.

Memory Dumps (cnt)

- Dumpchk – Designed to validate a memory dump.
- Available at http://www.microsoft.com/whdc/devtools/debugging/installx86.mspx
- Examine the memory dumps for additional information by searching through the contiguous ASCII strings that are embedded within.
- Use a Unicode-capable Windows version of the strings command. http://www.sysinternals.com/ntw2k/source/misc.html to view Unicode and standard ASCII

Memory Dumps (cnt)

- Dumpchk – Designed to validate a memory dump.

- Available at http://www.microsoft.com/whdc/devtools/debugging/installx86.mspx

- Examine the memory dumps for additional information by searching through the contiguous ASCII strings that are embedded within.

- Use a Unicode-capable Windows version of the strings command. http://www.sysinternals.com/ntw2k/source/misc.html to view Unicode and standard ASCII

Analyzing Nonvolatile Data

- System version and patch level
- File system time and date stamps
- Registry data
- Auditing Policy
- History of logins
- System event logs
- User accounts
- IIS logs
- Suspicious files

System Version and Patch Level

- Knowing which patches are applied to a server will narrow the initial investigation to areas of high probability.

- Psinfo can be used to collect this data

- Syntax (psinfo –h –s d)

OS Hot Fix	**Installed**
Q147222	**8/23/2003**

File System Time and Date Stamps

- Most investigators use the DIR command to capture the file time and date stamps. There is a better tool.
- find command gives a better result
- Syntax (find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n”

Registry Data

- Two main investigative leads that can be discovered by analyzing the registry dump.
  - Programs executed on boot up
  - Entries created by the intruder's tools
- Use Regdump to dump the registry
- Use any text editor to few output from regdump
  - Review the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\
  - Review all three sub-keys: Run | RunOnce | RunOnceEx

Audit Policy

- auditpol to determine the current local audit policy.

```
********************
***** auditpol *****
********************
Running ...

(0) Audit Disabled
System                   = No
Logon                    = No
Object Access            = No
Privilege Use            = No
Process Tracking         = No
Policy Change            = No
Account Management       = No
Directory Service Access = No
Account Logon            = No
```

History of Logins

- To view history of logins the command is

```
******************
***** ntlast *****
******************
 - No Records – Check to see if auditing is on
```

It depend on the Audit Policy

System Event Logs

- System Event Logs
  - Security (generated by audit policy)
  - Application (generated from installed appications)
  - System (message from system services)

- psloglist from PsTools (www.sysinternals.com) to extract these logs into easy to read text format.

- Syntax (psloglist –s –x security)
  - S parameter = single line
  - X parameter = dump extended information

User Accounts

- Use pwdump to dump user accounts and password hashes

- ***** pwdump3 *****
- *******************
- Administrator:500:9DCFD05D3688BBBFAAD3B435B51404EE:CB8C5705F92DE9D8D11642948ECCAB72:::
- Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
- IUSR_JBRWWW:1000:B936986BA1C5636B0F28D0549F4A7C10:137C045C1CACAE4B07C6C3B88BF0CE6D:::
- IWAM_JBRWWW:1001:DA3DF28964893179378B2EB9047FBA87:A2C8D0EC209C60A48DB9365A51565DC4:::

IIS Logs

- Default log location is c:\winnt\system32\logfiles
- Do not use ftp to transfer logs to the forensics workstation. This will modify the log you are trying to preserve.
- Create a netcat TCP tunnel.
- Type c:\winnt\system32\logfiles\w3svc1\logfile.log |nc forensics_workstation_ip port#

Collecting Data in Unix / Like environnement

Unix Live Response

- Volatile information
- Nonvolatile information
- Similar to Windows data collection, commands are different.
  - Use a forensics workstation
  - Use netcat to create a TCP channel for data duplication

Analyzing Volatile Data

- System time and date
- Current network connections
- Open TCP and UDP ports
- Executables opening TCP and UDP ports
- Running processes
- Open files
- Internal routing table
- Loaded kernel modules
- Mounted file systems

System Time and Date

- The system time and date are acquired by issuing the date command

- Syntax (date)

Current Network Connections

- Similar to the Windows Live Response.
- Use the netstat command
- Syntax (netstat –an)
- Netstat –an command also shows all open TCP and UDP ports

Executables Opening TCP or UDP Ports

- Use lsof command to list processes opening TCP or UDP ports.
- Lsof lists the files that the processes have open.

Syntax (lsof –n)

  - (-n) parameter to list raw IP addresses

Running Processes and Open Files

- Show running processes by running the ps command.

- Syntax (ps –aux)

- Shows all running processes on the system with the users running them.

- Show open files by using the same output from the lsof command.

The Internal Routing Table

- Use the same command that was used in the Windows Live Response.

- Syntax (Netstat –rn)

Loaded Kernel Modules

- Review all loaded kernel modules.
- Hackers commonly compromise the kernel and leave Trojan processes behind.
- Use the lsmod command to list loaded modules.
- Syntax (lsmod)

Mounted File Systems

- Mounted file systems is one way a hacker may transfer data to and from their system.
- Two commands can be used to show mounted file systems.
  - Mount
  - df

Analyzing Nonvolatile Data

- System version and patch level
- File system time and date stamps
- File system MD5 checksum values
- Current logged on users
- Login history
- Syslog logs
- User accounts
- User history files
- Suspicious files

System Version and Patch Level

- Use the uname command to list all available operating system information.
- Syntax (uname –a)

File System Time and Date Stamps

- Similar to the Windows Live Response.
- Use find command to delimit the output which then can easily be imported into any spreadsheet program.
- Syntax (find / -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n”)

File System MD5 Checksum Values

- Calculates 128-bit mathematical fingerprint of the contents of a file.
- Calculate and compare MD5 of known MD5 checksums.
- Syntax (find / -type f –xdev –exec md5sum –b {} \;)

Users Currently Logged On / Login History

- /var/run/utmp.log contains current logged on users.
- /var/log/wtmp contains the login history.
- Use the last command to pull the data from the binary log.
- Syntax (last)

Syslog Logs

- Review the /etc/syslog.conf to review all syslog file locations
- Typical file locations:
  - /var/log/messages
  - /var/log/secure
  - /var/log/maillog
  - /var/log/cron
  - /var/log/spooler
  - /var/log/boot.log

User Accounts

- User account information is stored in the /etc/passwd file.

- Validate all users. Any account with / as a root directory or a user ID of 0 should all be validated.

Suspicious Files

- In Windows, an executable cannot be removed. In Unix, everything is a file.
- /proc file system holds the process information
- Does not physically exist on the hard drive
- Exists in memory and references running processes and other system information
- Each process is a subfolder in the /proc folder. Process ID is the integer sub-folder
- Each process folder has a fd subfolder which contains all the open files associated with the particular process.

Putting it all together

- Initial objective was to determine whether or not an incident occurred.
- Volatile and nonvolatile are both important to determine if an incident has occurred.
- Create a timeline of all the evidence collected.
- Unix and Windows similar in data collected and commands executed
- A timeline of events needs to be created, to help trace and document the security event.

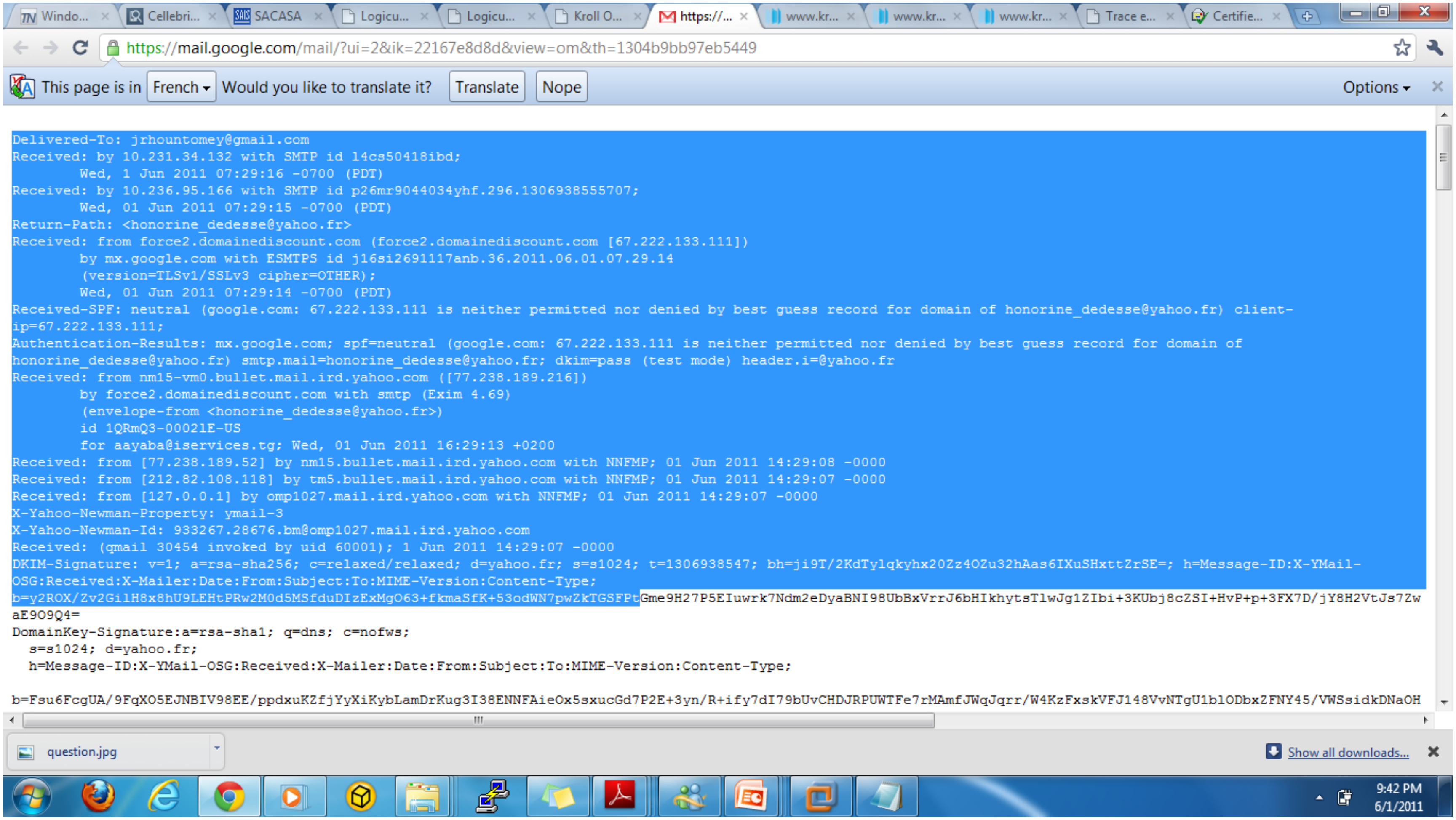
Additional

- Look at the browsing history
- Look for deleted files
- Look at the Network traffic
- Etc…

Tracing email

- Look at the Header
- Trace back with a tool that gives you
  - Date and time opened
  - Location of recipient (per their ISP city /town)
  - Map of location (available on paid subscriptions)
  - Recipients IP address
  - Apparent email address of opening (if available)
  - Referrer details (ie; if accessed via web mail etc)
  - URL clicks
  - How long the email was read for
  - How many times your email was opened
  - If your email was forwarded, or opened on a different computer
- Look DNS Records and RIR for contact informations

Tracing email



```
Delivered-To: jrhountomey@gmail.com
Received: by 10.231.34.132 with SMTP id 14cs50418ibd;
        Wed, 1 Jun 2011 07:29:16 -0700 (PDT)
Received: by 10.236.95.166 with SMTP id p26mr9044034yhf.296.1306938555707;
        Wed, 01 Jun 2011 07:29:15 -0700 (PDT)
Return-Path: <honorine_dedesse@yahoo.fr>
Received: from force2.domainediscount.com (force2.domainediscount.com [67.222.133.111])
        by mx.google.com with ESMTPS id j16si2691117anb.36.2011.06.01.07.29.14
        (version=TLSv1/SSLv3 cipher=OTHER);
        Wed, 01 Jun 2011 07:29:14 -0700 (PDT)
Received-SPF: neutral (google.com: 67.222.133.111 is neither permitted nor denied by best guess record for domain of honorine_dedesse@yahoo.fr) client-
ip=67.222.133.111;
Authentication-Results: mx.google.com; spf=neutral (google.com: 67.222.133.111 is neither permitted nor denied by best guess record for domain of
honorine_dedesse@yahoo.fr) smtp.mail=honorine_dedesse@yahoo.fr; dkim=pass (test mode) header.i=@yahoo.fr
Received: from nm15-vm0.bullet.mail.ird.yahoo.com ([77.238.189.216])
        by force2.domainediscount.com with smtp (Exim 4.69)
        (envelope-from <honorine_dedesse@yahoo.fr>)
        id 1QRmQ3-00021E-US
        for aayaba@iservices.tg; Wed, 01 Jun 2011 16:29:13 +0200
Received: from [77.238.189.52] by nm15.bullet.mail.ird.yahoo.com with NNFMP; 01 Jun 2011 14:29:08 -0000
Received: from [212.82.108.118] by tm5.bullet.mail.ird.yahoo.com with NNFMP; 01 Jun 2011 14:29:07 -0000
Received: from [127.0.0.1] by omp1027.mail.ird.yahoo.com with NNFMP; 01 Jun 2011 14:29:07 -0000
X-Yahoo-Newman-Property: ymail-3
X-Yahoo-Newman-Id: 933267.28676.bm@omp1027.mail.ird.yahoo.com
Received: (qmail 30454 invoked by uid 60001); 1 Jun 2011 14:29:07 -0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.fr; s=s1024; t=1306938547; bh=ji9T/2KdTylqkyhx20Zz4OZu32hAas6IXuSHxttZrSE=; h=Message-ID:X-YMail-
OSG:Received:X-Mailer:Date:From:Subject:To:MIME-Version:Content-Type;
b=y2ROX/Zv2GilH8x8hU9LEHtPRw2M0d5MSfduDIzExMgO63+fkmaSfK+53odWN7pwZkTGSFPtGme9H27P5EIuwrk7Ndm2eDyaBNI98UbBxVrrJ6bHIkhytsTlwJg1ZIbi+3KUbj8cZSI+HvP+p+3FX7D/jY8H2VtJs7Zw
aE9O9Q4=
DomainKey-Signature:a=rsa-sha1; q=dns; c=nofws;
  s=s1024; d=yahoo.fr;
  h=Message-ID:X-YMail-OSG:Received:X-Mailer:Date:From:Subject:To:MIME-Version:Content-Type;

b=Fsu6FcgUA/9FqXO5EJNBIV98EE/ppdxuKZfjYyXiKybLamDrKug3I38ENNFAieOx5sxucGd7P2E+3yn/R+ify7dI79bUvCHDJRPUWTFe7rMAmfJWqJqrr/W4KzFxskVFJ148VvNTgU1blODbxZFNY45/VWSsidkDNaOH
```

Cooperation with Law Enforcement

Cooperation with Law Enforcement

Task 1 - Identifying and reporting cyber crimes

Task 2 - CERT advises an incident reporter in a cyber crime case

Task 3 - CERT advises LEA in a cyber crime case

Task 4 - CERT prepares training for LEA