

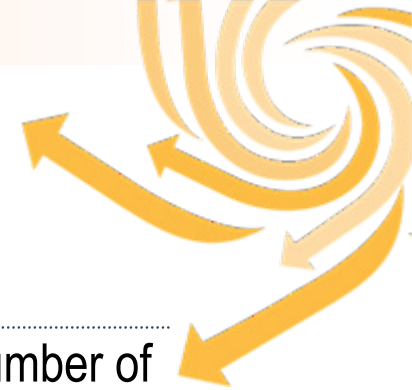


CYBERSECURITY FORENSICS WORKSHOP

Reviewing the Results of the Forensic Analysis

Ian M Dowdeswell
Incident Manager, Q-CERT

Caveats



- ▶ This is not an actual crime – it has been fabricated to illustrate a number of law enforcement and forensic processes and issues.
- ▶ The evidence and the case may not be sufficiently ‘watertight’ to take to court.
- ▶ We are concerned primarily with collection of electronic evidence but it should be emphasised that law enforcement agencies will collect all relevant evidence such as paper documents and non-electronic items.
- ▶ In this example the analysts have accompanied the law enforcement officer – this may not always be the case and analysis may need to be conducted ‘off-site’.
- ▶ This is an awareness and teaching case study, rather than a forensic lesson.



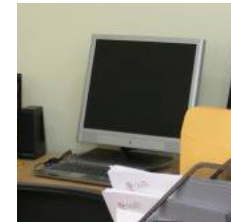
Remember the 'Scene of the Crime'?



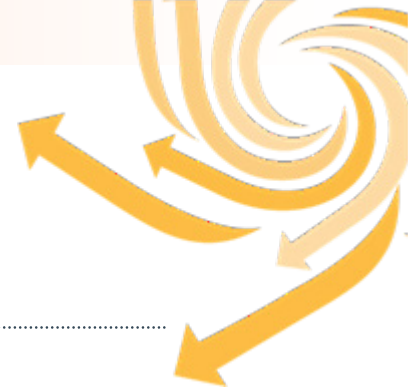
The exhibits at the scene of the 'crime'

On scoping the case and the IT at the scene the analysts focuses on :

- ▶ Office Administrator's workstation, including her hard drive.
- ▶ An additional hard-drive attached to the workstation.
- ▶ Office Administrator's USB 'stick' (aka 'thumb drive' or 'flash drive'), which she was given by the Network Administrator but was not reclaimed before she left the company (later found at OA's home).



Objective of the investigation



- ▶ Hostile takeover bid suggests that a rival company has been fed some confidential information.
- ▶ CCTV evidence suggests that confidential documents may have been shredded. (Issues of paper and electronic crimes, which may influence the search warrant)
- ▶ CCTV also suggests that inappropriate use of company IT may have occurred.
- ▶ Task of the investigator is to determine whether or not activity has taken place on the administrator's IT equipment that may have contributed towards criminal activity.

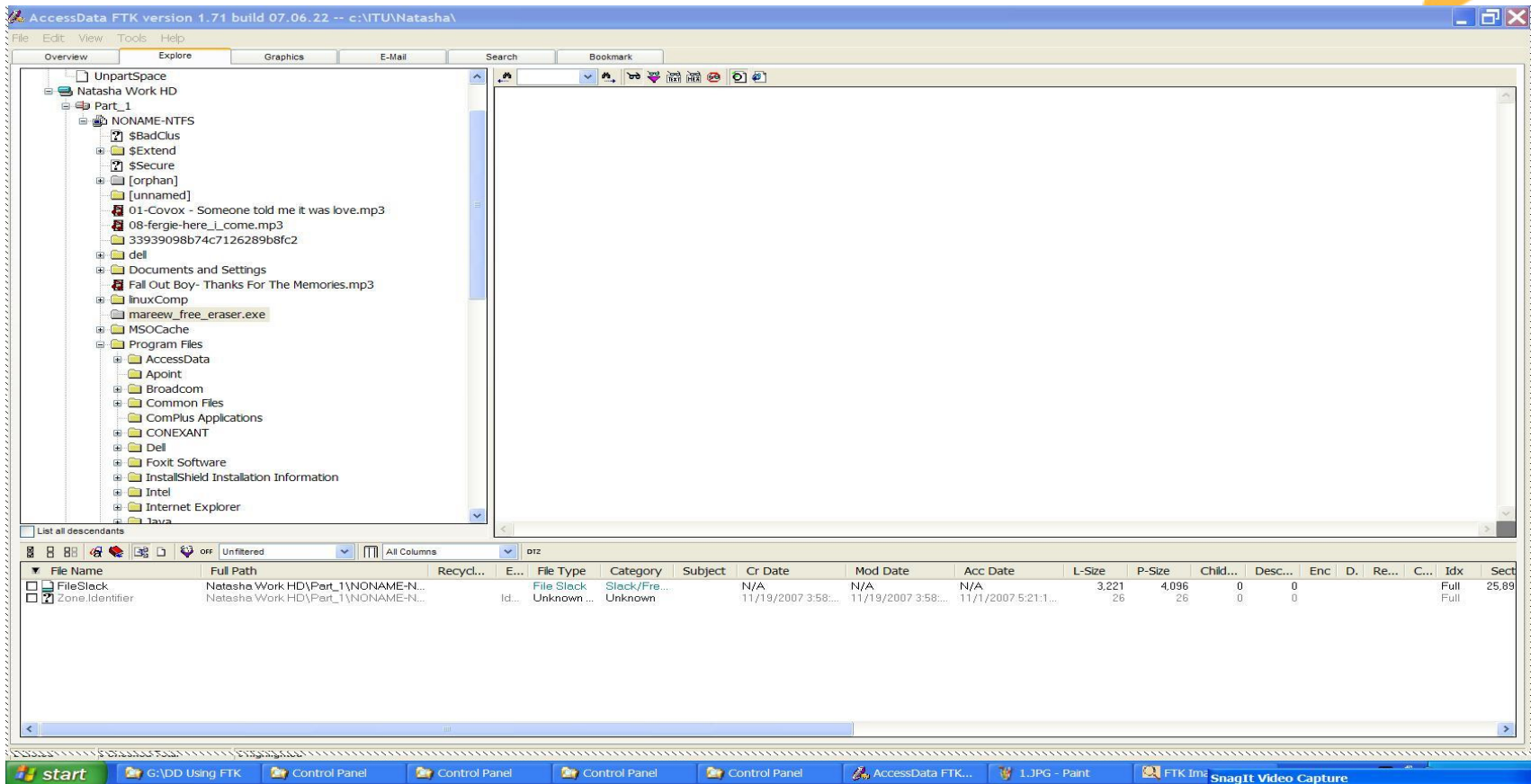


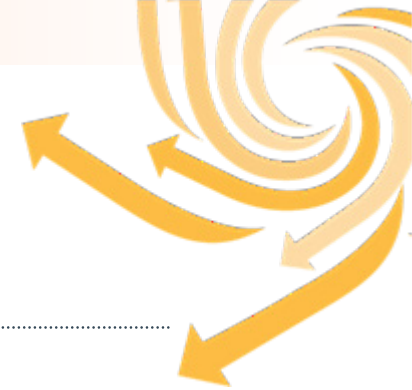
Forensic Procedures (1)

- ▶ The investigator makes a forensic copy of the hard drives and conducts an investigation of the discs, using standardised forensic investigation procedures and a tool such as '*FTK*'.
- ▶ He finds.....

Forensic Procedures (1) – Screen Shot

- ▶ A copy of an eraser software application (plus music files).





Forensic Procedures (2)

- ▶ Analysis of the hard disc also shows that a file was 'wiped', called:

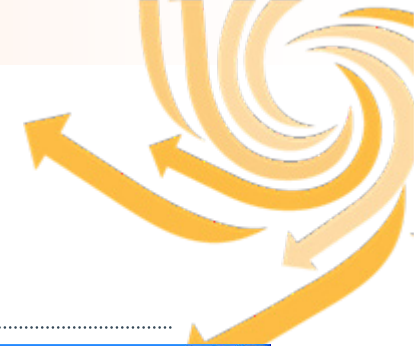
Khalid Acme's Widgets Limit - Annual Financial Report.pdf

- ▶ The file is recovered and verified as a true copy using an MD5 hash.



Forensic Procedures (2) – screen shot

Erased Annual Financial Report



AccessData FTK version 1.71 build 07.06.22 -- c:\NTU\usb\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items	File Status	File Category
Evidence Items: 1	KFF Alert Files: 0	Documents: 2
File Items	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 66	Bad Extension: 0	Databases: 0
Checked Items: 0	Encrypted Files: 0	Graphics: 2
Unchecked Items: 66	From E-mail: 0	Multimedia: 2
Flagged Thumbnails: 0	Deleted Files: 4	E-mail Messages: 0
Other Thumbnails: 2	From Recycle Bin: 0	Executables: 2
Filtered In: 66	Duplicate Items: 2	Archives: 1
Filtered Out: 0	OLE SubItems: 0	Folders: 2
Unfiltered	Flagged Ignore: 0	Slack/Free Space: 51
Filtered	KFF Ignorable: 0	Other Known Type: 0
All Items	Actual Files	Data Carved Files: 0
		Unknown Type: 4

How to Read a FINANCIAL REPORT

Image 1 / Image 2

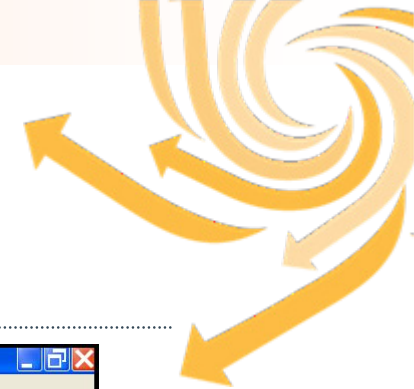
File Name	Full Path	Ext	File Type
<input type="checkbox"/> ericon p990.pdf	I:\NO NAME-FAT16\ericon p990.pdf	pdf	Acrobat Portable
<input type="checkbox"/> Khalid Acme's Widgets ...	I:\NO NAME-FAT16\Khalid Acme's Widgets Limit-Financial Report.pdf	pdf	Acrobat Portable

2 Listed 0 Checked Total I:\NO NAME-FAT16\Khalid Acme's Widgets Limit-Financial Report.pdf

start SnagIt AccessData FTK... unttitled - Paint 4:50 PM

Forensic Procedures (3)

- ▶ Analysis of the OS 'swapfile' dump, using '*FTK AccessData*', shows the following information.....



Forensic Procedures (3) – Screen Shot (2)

AccessData FTK version 1.71 build 07.06.22 -- c:\VTU\Natasha\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Indexed Search Live Search

Search Term: [] Add Import Options

Indexed Words Search Items Hits Files

2 Hits - [pagefile.sys_03] Natasha Work HD\Part_1\NONAME-NTFS\pagefile.sys_03

2 Hits - [pagefile.sys_02] Natasha Work HD\Part_1\NONAME-NTFS\pagefile.sys_02

al report of biggest <<compattor>> in the country Second 20 K US\$ taransfer to account number i will mentond it later

what do you think

----- Original Message -----

From: moneer moustafa <moneer_kamal@yahoo.com>

To: Natasha Gameova <natasha.gameova@yahoo.com>

Sent: Tuesday, February 19, 2008 3:39:33 PM

Subject: Re: important information

Hi

File Name	Full Path	Recycl...	E...	File Type	Category	Subject	Cr Date
CA0R0BY.J.xml	Natasha Work HD\Part_1\NONAME-NTFS\Documents and Settings\Natasha.CLASSROOM24\Local Settings\Temporary Internet Files\ContentIE5\9MVM1KP\CA...			xml XML	Document		11/3/2007 5:48:2...
pagefile.sys_02	Natasha Work HD\Part_1\NONAME-NTFS\pagefile.sys_02			sys Unknown ...	Unknown		12/2/2007 3:14:5...
pagefile.sys_03	Natasha Work HD\Part_1\NONAME-NTFS\pagefile.sys_03			sys Unknown ...	Unknown		12/2/2007 3:14:5...
pagefile.sys_04	Natasha Work HD\Part_1\NONAME-NTFS\pagefile.sys_04			sys Unknown ...	Unknown		12/2/2007 3:14:5...

SWAPFILE

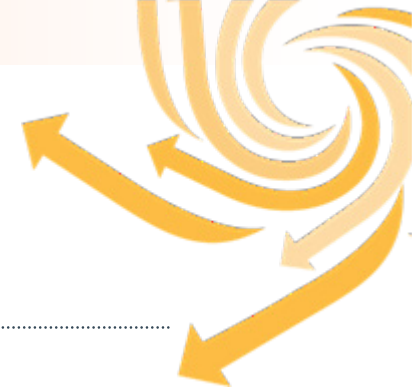
4 Listed 0 Checked Total Natasha Work HD\Part_1\NONAME-NTFS\pagefile.sys_02

start G:\DD Using FTK Control Panel Control Panel Control Panel AccessData FTK... untitled - Paint 8:21 AM



Forensic Procedures (4)

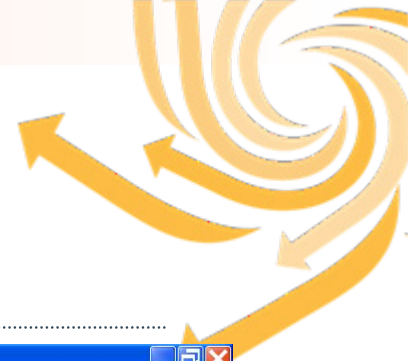
- ▶ This clearly demonstrates that Ms. Gameova has offered to sell information to 'Moneer', who we can quickly identify as the CIO for Hamid's Widgets.



Forensic Procedures (5)

- ▶ We mentioned that investigation of the hard disc identified a number of MP3 files downloaded from the internet.
- ▶ The date and time of download is consistent with the CCTV footage of Raquel Moroni using the machine.
- ▶ Examination of these files reveals no further suspicious activity but it is in violation of the company policy – what action needs to be taken depends on the Board.
- ▶ However, consider how actions may be different if these files implied further criminal activity such as resale of videos etc..





Forensic Procedures (5) – screen shot MP3 files

AccessData FTK version 1.71 build 07.06.22 -- c:\ITU\usb\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items	File Status	File Category
Evidence Items: 1	KFF Alert Files: 0	Documents: 2
File Items	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 66	Bad Extension: 0	Databases: 0
Checked Items: 0	Encrypted Files: 0	Graphics: 2
Unchecked Items: 66	From E-mail: 0	Multimedia: 2
Flagged Thumbnails: 0	Deleted Files: 4	E-mail Messages: 0
Other Thumbnails: 2	From Recycle Bin: 0	Executables: 2
Filtered In: 66	Duplicate Items: 2	Archives: 1
Filtered Out: 0	OLE Subitems: 0	Folders: 2
Unfiltered	Flagged Ignore: 0	Slack/Free Space: 51
All Items	KFF Ignorable: 0	Other Known Type: 0
Actual Files	Data Carved Files: 0	Unknown Type: 4

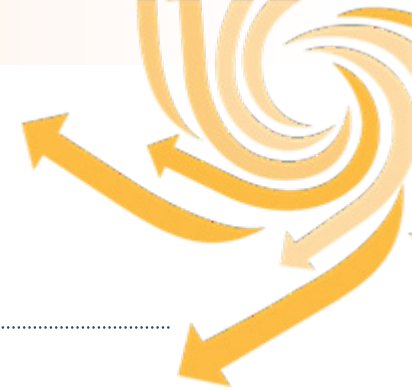
Unfiltered All Columns dr2

File Name	Full Path	Ext	File Type
<input type="checkbox"/> 01-Covox - Someone tol...	I:\NO NAME-FAT16\01-Covox - Someone told me it was love.mp3	mp3	MP3, MPEG Vers
<input type="checkbox"/> Fall Out Boy- Thanks For...	I:\NO NAME-FAT16\Fall Out Boy- Thanks For The Memories.mp3	mp3	MP3, MPEG Vers

2 Listed 0 Checked Total 0 Highlighted

start SnagIt AccessData FTK... AFR.JPG - Paint 4:53 PM



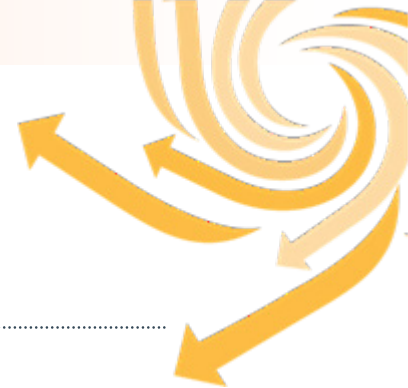


Forensic Procedures (6)

- ▶ The investigator has shown that the AFR was emailed to the OA's personal Yahoo email address. He believes that the OA may have relevant information on her home IT.
- ▶ This information is handed to CID who take the decision to obtain a warrant and conduct an analysis at Ms. Gameova's home.



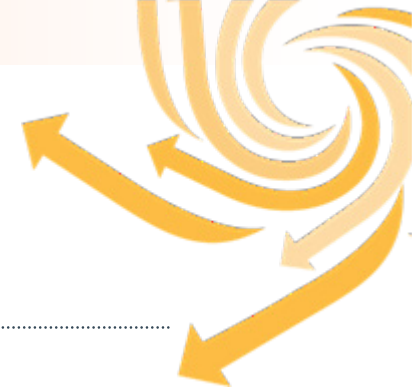
'Home' Forensic Investigation (1) Potential 'crime scene' at Ms. Gameova's apartment:



'Home' Forensic Investigation (1)

Fortuitously, the laptop is 'live' and logged on to 'Yahoo mail'. The investigators decide to conduct a 'live investigation'





'Home' Forensic Investigation (2)

- ▶ They politely draw her away from her machine, while the investigator conducts a 'live investigation'.
- ▶ He finds the following evidence.....



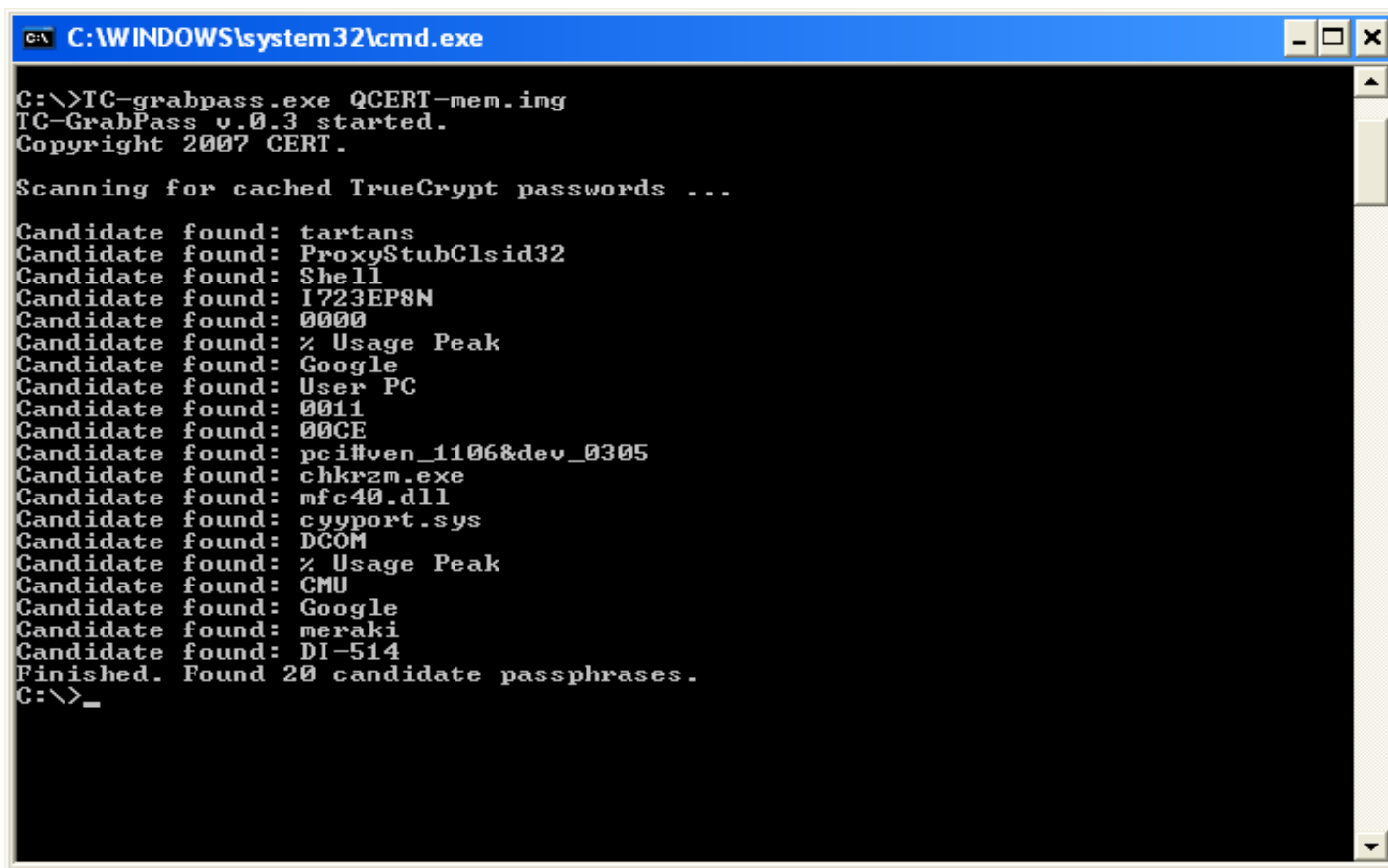


'Home' Forensic Investigation (3)

- During the initial analysis of the laptop, an encrypted volume was identified.
- 'Live analysis' of the memory dump produced a set of encryption password keys for the volume.



'Home' Forensic Investigation (3) – screen shot



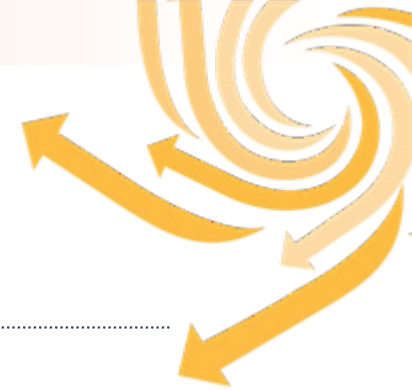
```
C:\WINDOWS\system32\cmd.exe
C:\>IC-grabpass.exe QCERT-mem.img
IC-GrabPass v.0.3 started.
Copyright 2007 CERT.

Scanning for cached TrueCrypt passwords ...

Candidate found: tartans
Candidate found: ProxyStubClsid32
Candidate found: Shell
Candidate found: I723EP8N
Candidate found: 0000
Candidate found: % Usage Peak
Candidate found: Google
Candidate found: User PC
Candidate found: 0011
Candidate found: 00CE
Candidate found: pci#ven_1106&dev_0305
Candidate found: chkrzm.exe
Candidate found: mfc40.dll
Candidate found: cyport.sys
Candidate found: DCOM
Candidate found: % Usage Peak
Candidate found: CMU
Candidate found: Google
Candidate found: meraki
Candidate found: DI-514
Finished. Found 20 candidate passphrases.
C:\>_
```

Results from analysis looking for possible TrueCrypt passwords in a captured memory image.

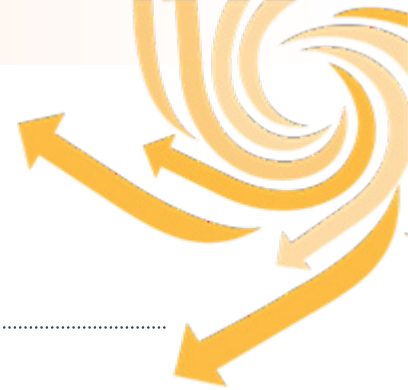




'Home' Forensic Investigation (4)

- Further analysis of the encrypted volume identified the APR file.
- A copy of the financial report verified by MD5 hash as being a true copy.





'Home' Forensic Investigation (5)

- Analysis of the Yahoo email 'inbox' items folder screen shows that the 'Moneer' has agreed to the transaction.



'Home' Forensic Investigation (6) – 'inbox' screen shot

(0 unread) Yahoo! Mail, natasha.gameova - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://us.mg3.mail.yahoo.com/dc/launch

YAHOO! MAIL natasha.gameova Available
Sign Out, My Account, Mail Classic

Yahoo! | My Yahoo! | News Search the Web... Search

Check Mail New

Search Mail... Go

Yahoo! Tech
Tech made easy

Inbox Drafts Sent Spam Trash (1) Contacts Add 0 Online Calendar Notepad All Feeds Add My Folders Add

Home **Inbox** 3 messages Mobile | Options | Help

Delete Reply Forward Spam Move Print More Actions View

	From	Subject	Date	Size
<input type="checkbox"/>	moneer moustafa	Re: important information	Wed, 2/20/08 1:46 PM	14KB
<input type="checkbox"/>	moneer moustafa	Re: important information	Wed, 2/20/08 1:37 PM	9KB
<input type="checkbox"/>	moneer moustafa	Re: important information	Tue, 2/19/08 3:39 PM	5KB

Re: important information Compact Header | Full Message View

moneer moustafa <moneer_kamal@yahoo.com> Add To: Natasha Gameova <natasha.gameova@yahoo.com>

OK

Money will be transferred at end of day

please send the report at 6:00 PM Exactly

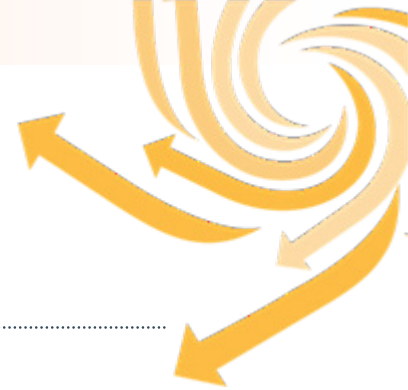
Regards

----- Original Message -----
From: Natasha Gameova <natasha.gameova@yahoo.com>
To: moneer moustafa <moneer_kamal@yahoo.com>
Sent: Wednesday, February 20, 2008 1:42:56 PM
Subject: Re: important information

TODAY: 11/4 No events. Click the plus sign to add an event.

Done

start (0 unread) Yahoo! M... (0 unread) Yahoo! M... Local Disk (C:) Sent Items - Paint Internet 2:58 PM



'Home' Forensic Investigation (6)

- Similarly the Yahoo email 'sent' folder screen confirms the transfer of file and bank details.

Note: even if the OA was 'logged out' of Yahoo, it is possible to retrieve username and password and log back in.



'Home' Forensic Investigation (5) – 'sent' screen shot

Microsoft Internet Explorer window: (0 unread) Yahoo! Mail, natasha.gameova

Address: http://us.mg3.mail.yahoo.com/dc/launch?...rand=ds0o4kq0883jn

Yahoo! MAIL: natasha.gameova Offline

Home | Sent 3 messages | Re: important inform

To	Subject	Sent	Size
moneer moustafa	Re: important information	Wed, 2/20/08 1:42 PM	11KB
moneer moustafa	Re: important information	Tue, 2/19/08 3:42 PM	6KB
Moneer_kamal@yahoo.com	important information	Tue, 2/19/08 3:30 PM	2KB

Re: important information
 Natasha Gameova <natasha.gameova@yahoo.com> To: moneer moustafa <moneer_kamal@yahoo.com>

Hi

Find Attachd the part of the report

second my account information

Michael Liwes

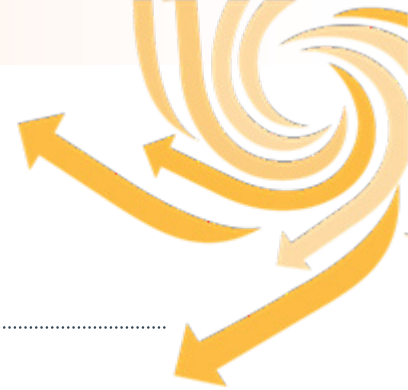
01503070123
 SZDB Bank

For My Mobile let see after transfer the money

Regards

System tray: Done, Internet, 2:56 PM

Summary



▶ Investigation reveals:

- The OA (Ms. Gameova) made an unauthorised copy of the Annual Financial Report (AFR) on her workplace computer.
- She emailed the document to her personal 'Yahoo' email account and made a further unauthorised copy on a USB stick, which she took home, contravening company security policy.
- She downloaded a copy of a software eraser from the software company's website and used it to delete the AFR file on her office workstation. This action is also in contravention of company policy.



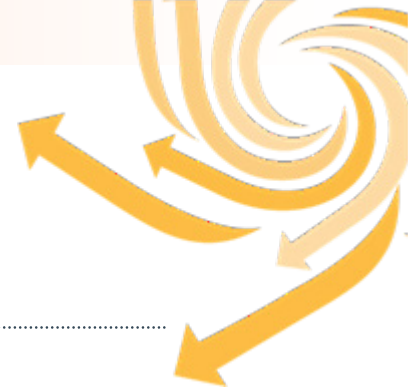
Summary (2)

▶ Investigation reveals:

- The OA also copied the AFR on the USB stick to her home PC.
- This file was then sent to Hamid's Widgets Inc. (who may have used the information to decide to make a hostile bid for Khalid Acme's Widgets Limited).
- In return Ms. Gameova received a sum of QR 20k from Hamid's Widgets Inc..



Summary (3)



► Investigation further reveals:

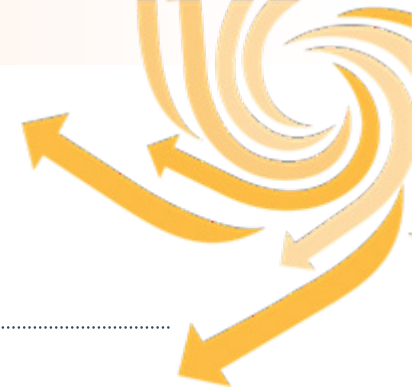
- The OA workplace workstation has numerous MP3 music files, This is in contravention of company security policy.
- Furthermore, extensive periods have been spent browsing the internet from Ms. Gameova's machine, during working hours. During these periods, inappropriate files have been downloaded from the Internet. This is again in contravention of company policy.
- Neither of these activities are relevant to the investigation on behalf on CID, as they are not directly related to the actual criminal activity.
- They are of course indication of lax company enforcement of security policy and may, indirectly, have contributed to the decision by the perpetrator to take action.



Summary (4)

- ▶ CID now how sufficient electronic evidence to :
 - Determine that criminal activity has taken place and coupled with other evidence, such as CCTV footage, papers, testimony from witnesses etc., they may decide to forward the case for prosecution.

Conclusions

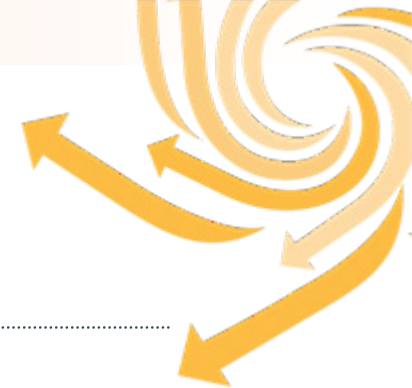


We have :

- ▶ Given a presentation of an Incident in the form of a structured walk-through of a modern office scenario, where a cybercrime may have occurred.
- ▶ Identified critical junctures in the investigation and which cyberforensics techniques are appropriate at each point, by description or by demonstration.
- ▶ Presented Forensically-Safe Techniques for Crime Scene Investigation
- ▶ Discussed Live Memory Acquisition and Analysis, where the crime scene contains evidence that can only be acquired while the machines are running, and file systems are “open”.
- ▶ Demonstrated Device Imaging and Analysis
- ▶ Discussed Cyber-Forensics and the Role of Expert Witnesses
- ▶ Emphasised engagement with Law Enforcement as one of the highest priorities for national incident response teams, worldwide.



Incident Management Points of Contact



Report Incidents by:

Website (using proforma):

www.qcert.org

Email:

incidents@qcert.org

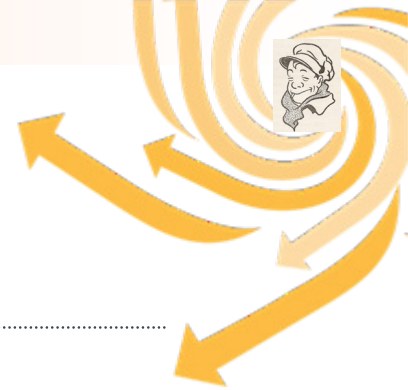
Phone:

+974 493 3408

Fax:

+974 483 9953





Questions?

Questions

