
# HACKING PARIS 2014

# EXTREME FORENSICS RELOADES 2Q /2014

**Alvaro Alexander Soto**
**Digital Forensics Lab Director**
**HTCIA/ICFP/ACM/IEEE/ACIS/ISSA**
**asoto@asoto.com**


## INTENDED AUDIENCE

Forensic lab directors / analysts - Law enforcement - Researchers - Tech Enthusiasts – a.k.a. Geeks

Objectives.

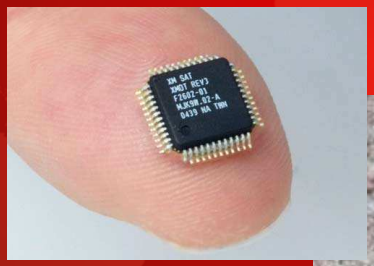
Think beyond traditional forensic tools and general landscape of the new challenges

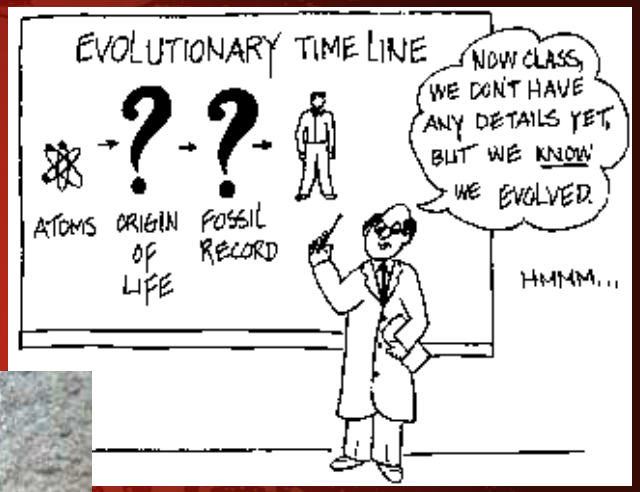
ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

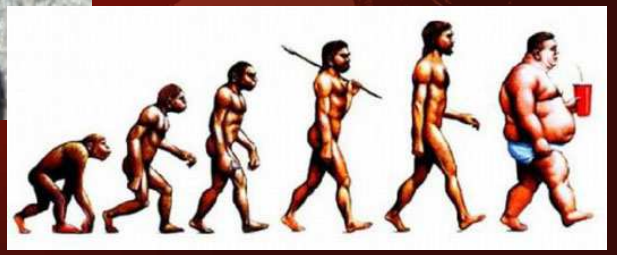
CONFIDENTIAL

WWW.ASOTO.COM

- **Evolution of Digital Forensics…**
  - Pc's..
  - Networks
  - Smartphones
  - Digital Devices
  - Cloud…
  - Next…?





ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM


## CORPORATE - ECONOMIC ESPIONAGE

What is?

Industrial espionage, economic espionage or corporate espionage is a form of espionage conducted for commercial purposes instead of purely national security.[1] Economic espionage is conducted or orchestrated by governments and is international in scope, while industrial or corporate espionage is more often national and occurs between companies or corporations. Wikipedia.

Corporate Espionage vs Counter Terrorism

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM


**Currents**

- USA – CHINA / DOJ / FBI Indict.
- Target..
- Colombia, Andres Sepulveda, Cuba, etc
- 19 countries, FBI, Rent-a-backdoor Creepware 40USD “Full Equipment”
- Statistics USA –Verizon- , COL, KMPG,
- EXECUTIVE Responsibility - NOT I.T.

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Expectations…
# Sometimes you expect this:

Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# …But you get this..

Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Expectation:

Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# But you get this…


Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Expectation…

Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# But you get this…

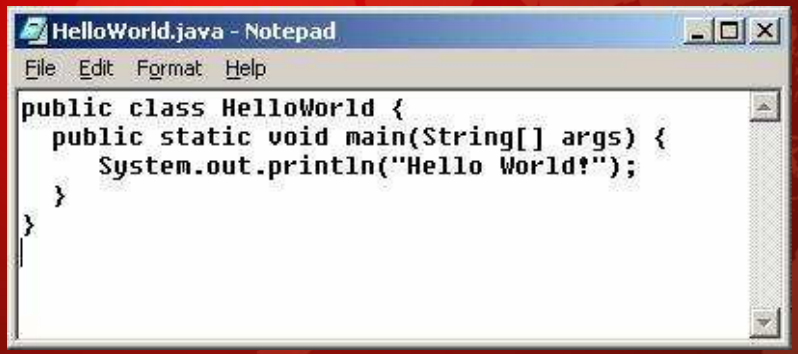
Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# EXPECTATION..



ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

But you get this…

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Sometimes you expect this:

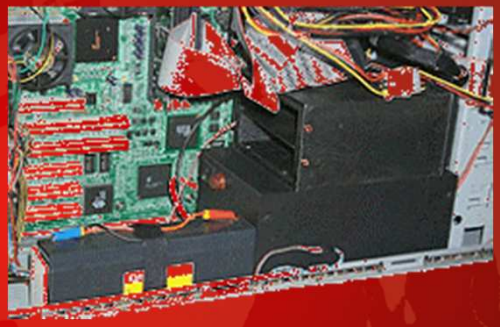
Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS •
DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Get this…

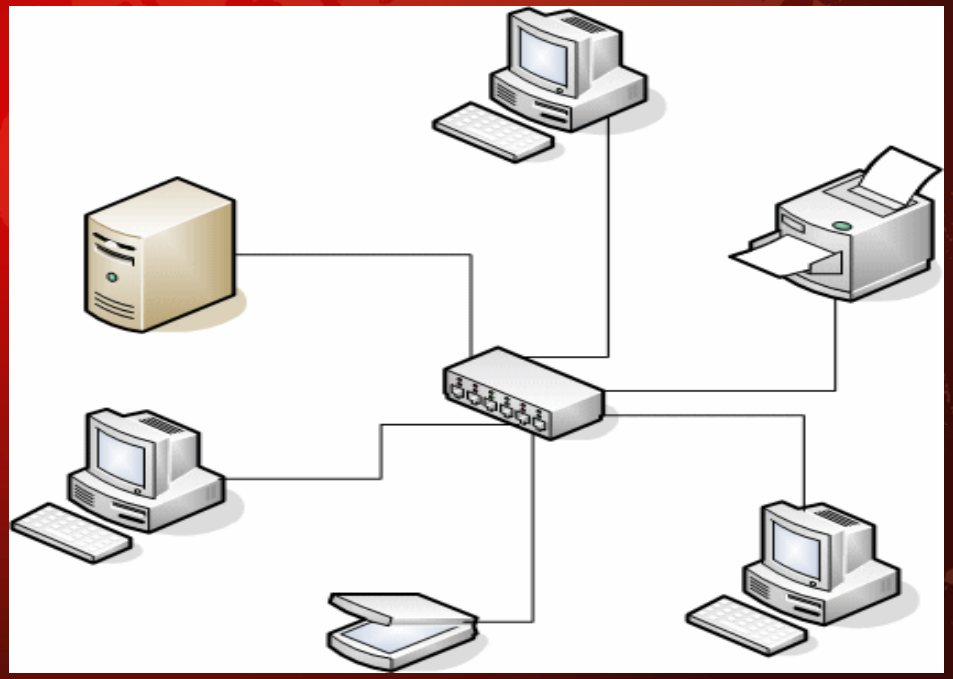


ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Sometimes you expect this:



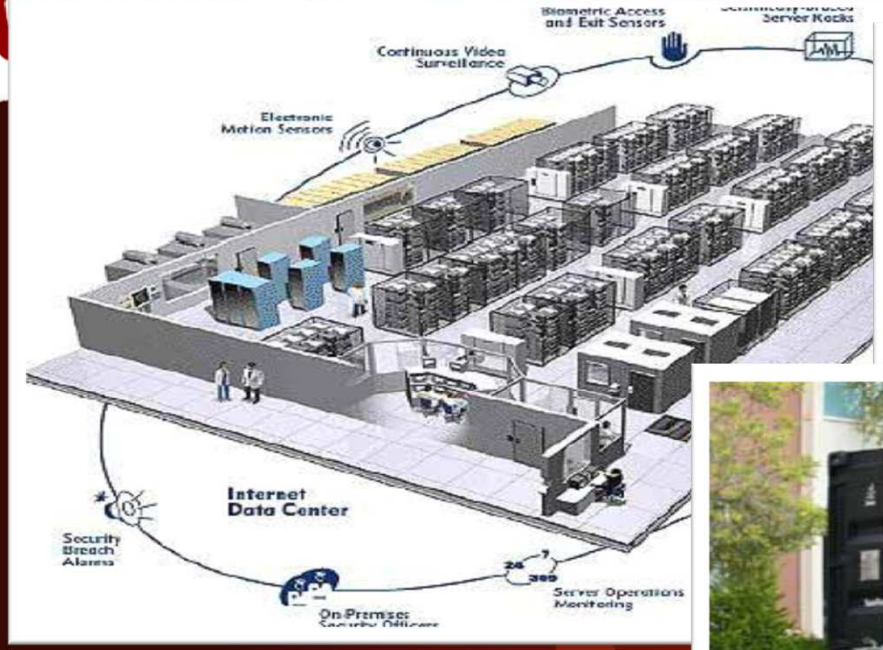
Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS •
DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# But you get this:





Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Sometimes you expect this:

Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# ...But you get this..

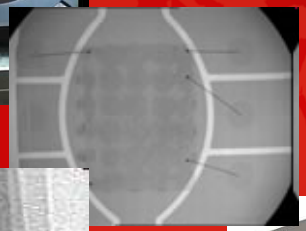
Web Site www.asoto.com  Email: info@asoto.com

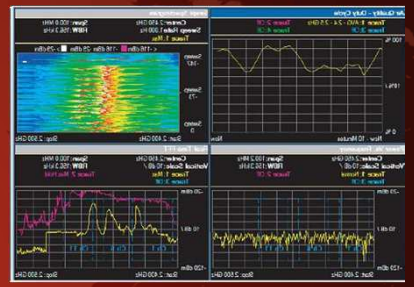
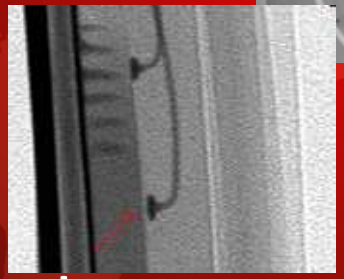
ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

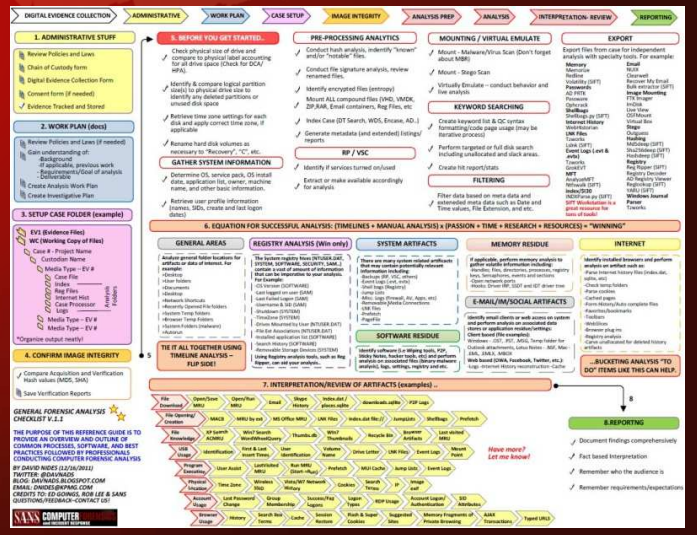




Lab TOOLS…

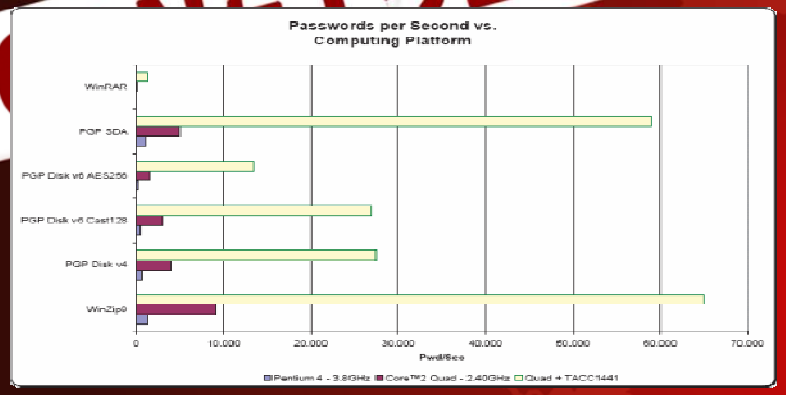
- Software
- Hardware
- Specialized tools

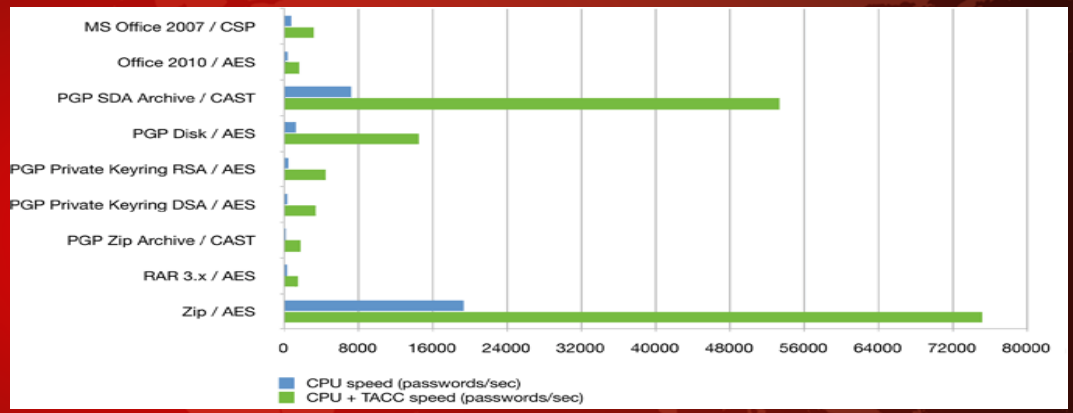


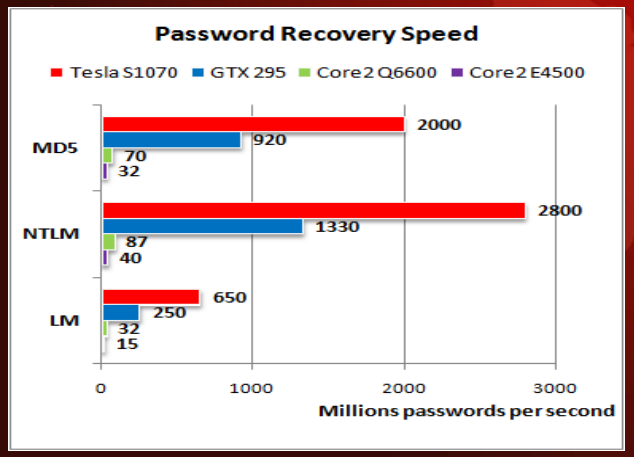
ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

WWW.ASOTO.COM

# Password Protection…




http://www.freerainbowtables.com/ ….

http://www.freerainbowtables.com/en/tables2/

Others…

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

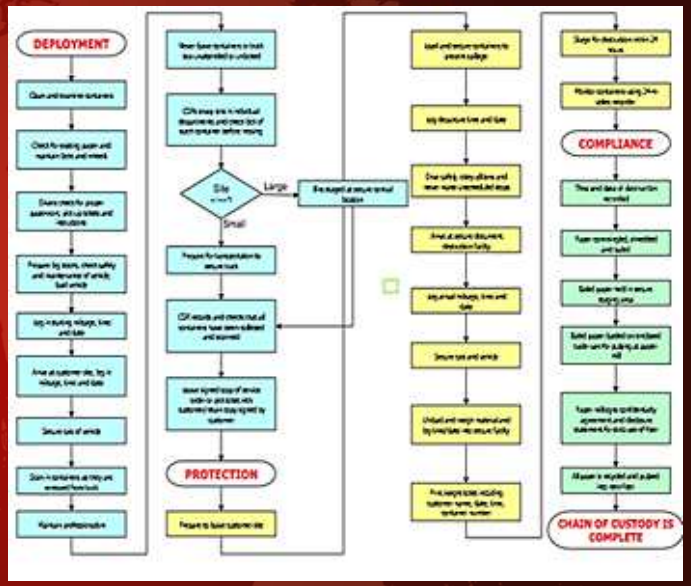
WWW.ASOTO.COM

# Manual Password Recovery

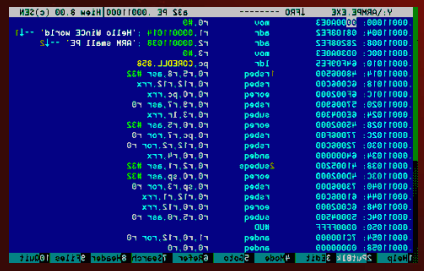

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS •
DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM




# Really Standard process??



## EVIDENCE

Submitting Agency _____

Date Collected _____ Time _____

Item # _____ Case # _____

Collected By _____

Description of Evidence _____

_____

Location Where Collected _____

Type of Offense _____

### CHAIN OF CUSTODY

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

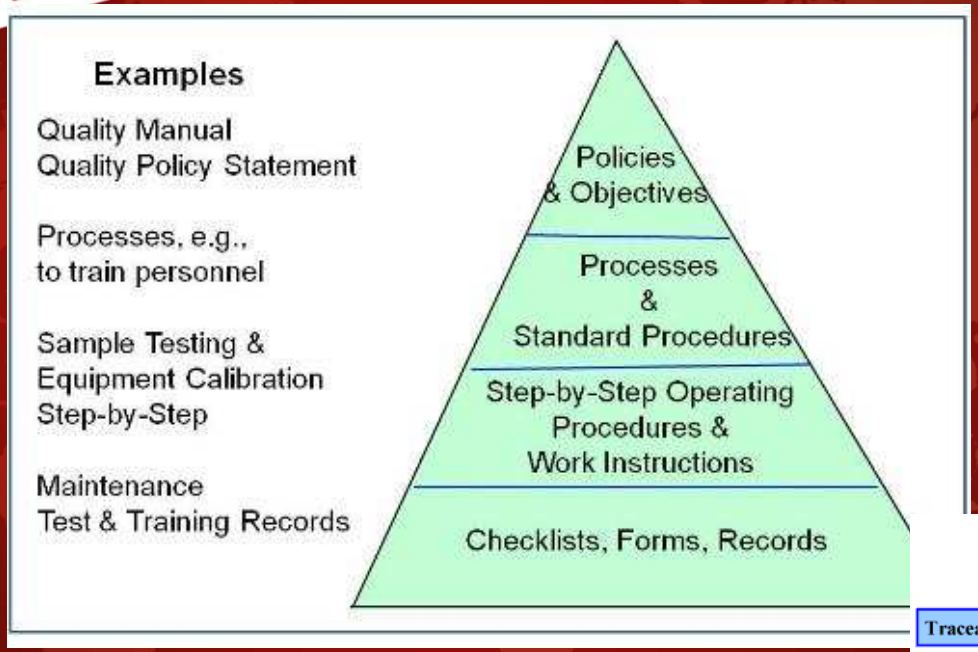
Date _____ Time _____

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

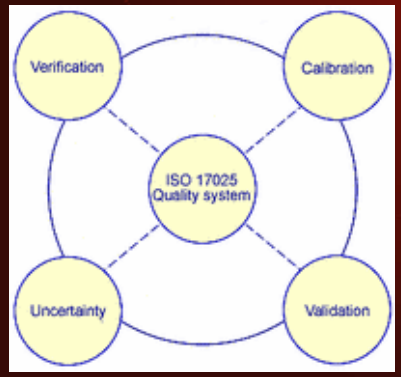
CONFIDENTIAL

WWW.ASOTO.COM

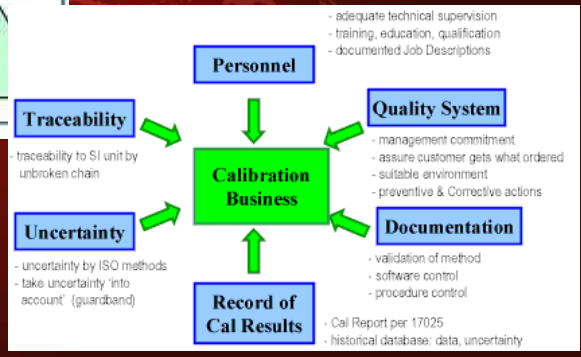
- ISO 17025..








And remember the LIMS…..




ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS •
DATA RECOVERY • SPECIAL PROJECTS
CONFIDENTIAL
WWW.ASOTO.COM
• Technical Process..
• Administrative Process..
• Legal process…
• Integration…

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# Actual/Future paths for specializations in digital forensics

- OS + internals
- NOS + internals
- Mobile phones/smart phones
- Digital devices / appliances
- Reverse engineering / malware analy
- App Servers / web 2.0, 3.0 …..

Web Site www.asoto.com  Email: info@asoto.com

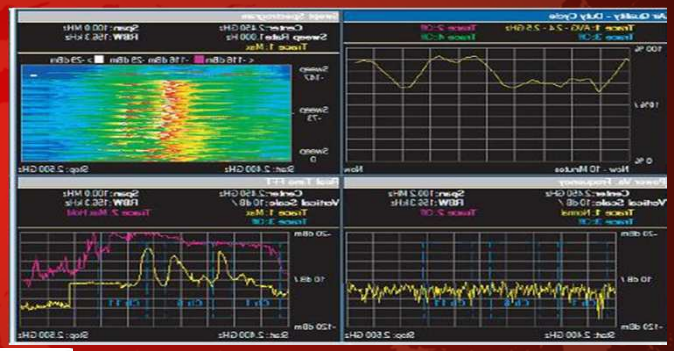
ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# New trends/challenges.. new tools required...

- Firmware analysis and repair
- Mechanical tools for media
- Faraday cages
- EEPROM / NAND readers
- Spectrum analyzers
- Mobile multiplexers
- Sand boxes
- Reverse engineering
- Strong SSO auth.
- Data mining…. Terabytes waiting for..




ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# ACE / SD / Others..

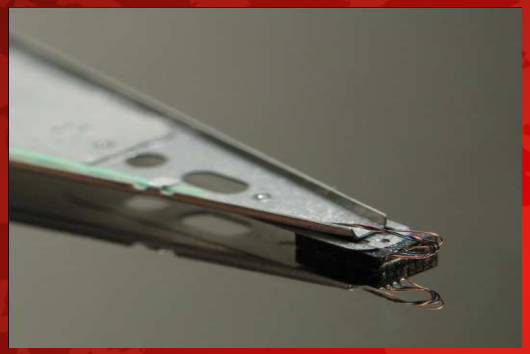
Web Site www.asoto.com ✉ Email: info@asoto.com

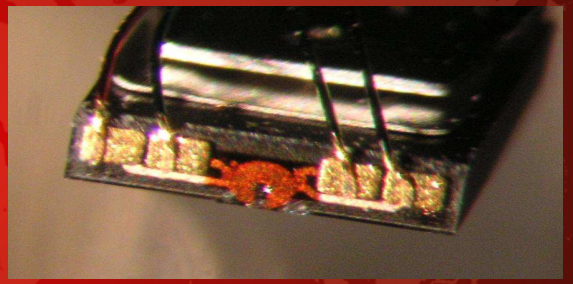
ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

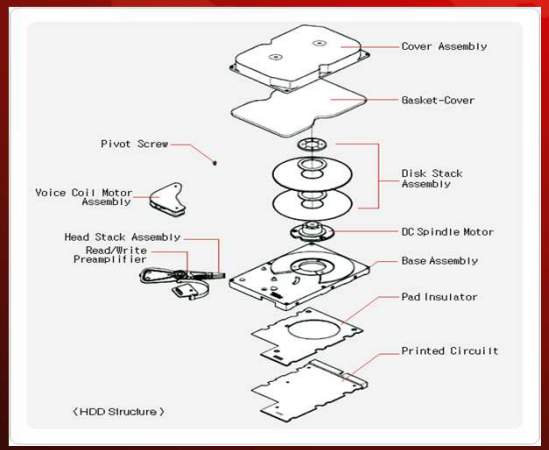
CONFIDENTIAL

WWW.ASOTO.COM

# Nude HDD…








Web Site www.asoto.com  Email: info@asoto.com


ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

WWW.ASOTO.COM

# Example of eXtreme Digital Forensics, beyond the logical level…

The dark side of storage

- ATA Commands
- ATA Factory commands
- What is the SA?
- Firmware
- Flash ROM
- Heads/Platters
- Security Erase, HDD Self destruction?
- ATA password

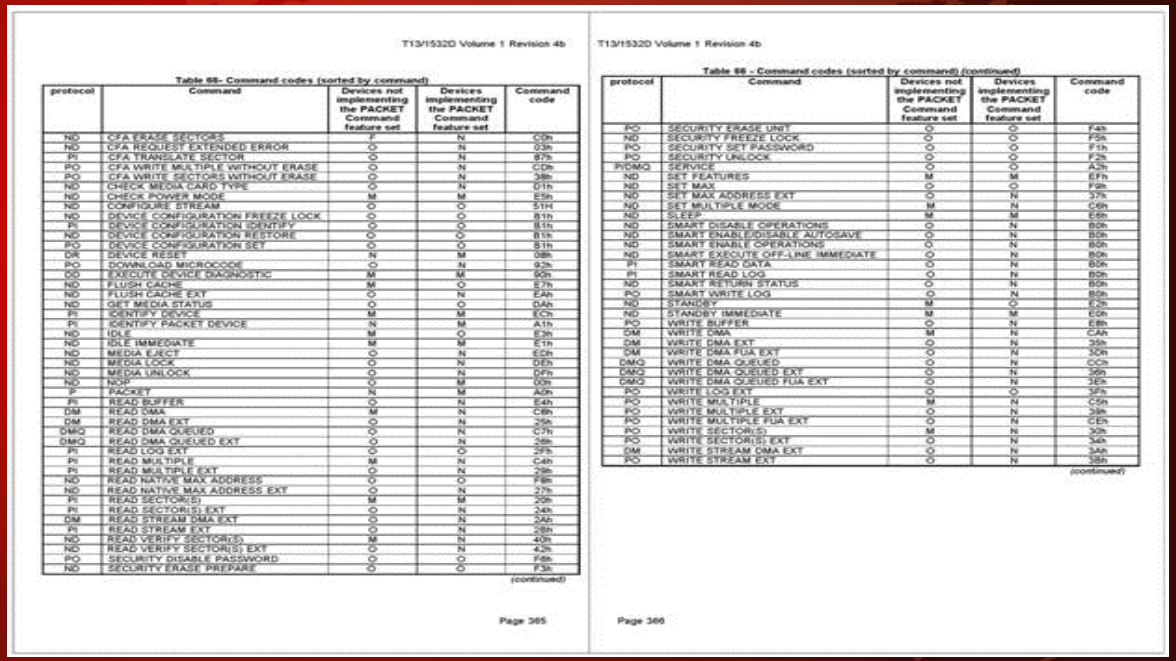
Web Site www.asoto.com Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# ATA commands..



T13/1532D Volume 1 Revision 4b

Table 66- Command codes (sorted by command)

| protocol | Command | Devices not implementing the PACKET Command feature set | Devices implementing the PACKET Command feature set | Command code |
|---|---|---|---|---|
| ND | CFA ERASE SECTORS | F | N | C0h |
| ND | CFA REQUEST EXTENDED ERROR | O | N | 03h |
| PI | CFA TRANSLATE SECTOR | O | N | 87h |
| PO | CFA WRITE MULTIPLE WITHOUT ERASE | O | N | CDh |
| PO | CFA WRITE SECTORS WITHOUT ERASE | O | N | 38h |
| ND | CHECK MEDIA CARD TYPE | O | N | D1h |
| ND | CHECK POWER MODE | M | M | E5h |
| ND | CONFIGURE STREAM | O | O | 51H |
| ND | DEVICE CONFIGURATION FREEZE LOCK | O | O | B1h |
| PI | DEVICE CONFIGURATION IDENTIFY | O | O | B1h |
| ND | DEVICE CONFIGURATION RESTORE | O | O | B1h |
| PO | DEVICE CONFIGURATION SET | O | O | B1h |
| DR | DEVICE RESET | N | M | 08h |
| PO | DOWNLOAD MICROCODE | O | N | 92h |
| OD | EXECUTE DEVICE DIAGNOSTIC | M | M | 90h |
| ND | FLUSH CACHE | M | O | E7h |
| ND | FLUSH CACHE EXT | O | N | EAh |
| ND | GET MEDIA STATUS | O | O | DAh |
| PI | IDENTIFY DEVICE | M | M | ECh |
| PI | IDENTIFY PACKET DEVICE | N | M | A1h |
| ND | IDLE | M | O | E3h |
| ND | IDLE IMMEDIATE | M | M | E1h |
| ND | MEDIA EJECT | O | N | EDh |
| ND | MEDIA LOCK | O | N | DEh |
| ND | MEDIA UNLOCK | O | N | DFh |
| ND | NOP | O | M | 00h |
| P | PACKET | N | M | A0h |
| PI | READ BUFFER | O | N | E4h |
| DM | READ DMA | M | N | C8h |
| DM | READ DMA EXT | O | N | 25h |
| DMQ | READ DMA QUEUED | O | N | C7h |
| DMQ | READ DMA QUEUED EXT | O | N | 26h |
| PI | READ LOG EXT | O | O | 2Fh |
| PI | READ MULTIPLE | M | N | C4h |
| PI | READ MULTIPLE EXT | O | N | 29h |
| ND | READ NATIVE MAX ADDRESS | O | O | F8h |
| ND | READ NATIVE MAX ADDRESS EXT | O | N | 27h |
| PI | READ SECTOR(S) | M | M | 20h |
| PI | READ SECTOR(S) EXT | O | N | 24h |
| DM | READ STREAM DMA EXT | O | N | 2Ah |
| PI | READ STREAM EXT | O | N | 2Bh |
| ND | READ VERIFY SECTOR(S) | M | N | 40h |
| ND | READ VERIFY SECTOR(S) EXT | O | N | 42h |
| PO | SECURITY DISABLE PASSWORD | O | O | F6h |
| ND | SECURITY ERASE PREPARE | O | O | F3h |

(continued)

Page 365

T13/1532D Volume 1 Revision 4b

Table 66 - Command codes (sorted by command) (continued)

| protocol | Command | Devices not implementing the PACKET Command feature set | Devices implementing the PACKET Command feature set | Command code |
|---|---|---|---|---|
| PO | SECURITY ERASE UNIT | O | O | F4h |
| ND | SECURITY FREEZE LOCK | O | O | F5h |
| PO | SECURITY SET PASSWORD | O | O | F1h |
| PO | SECURITY UNLOCK | O | O | F2h |
| P/DMQ | SERVICE | O | O | A2h |
| ND | SET FEATURES | M | M | EFh |
| ND | SET MAX | O | O | F9h |
| ND | SET MAX ADDRESS EXT | O | N | 37h |
| ND | SET MULTIPLE MODE | M | N | C6h |
| ND | SLEEP | M | M | E6h |
| ND | SMART DISABLE OPERATIONS | O | N | B0h |
| ND | SMART ENABLE/DISABLE AUTOSAVE | O | N | B0h |
| ND | SMART ENABLE OPERATIONS | O | N | B0h |
| ND | SMART EXECUTE OFF-LINE IMMEDIATE | O | N | B0h |
| PI | SMART READ DATA | O | N | B0h |
| PI | SMART READ LOG | O | N | B0h |
| ND | SMART RETURN STATUS | O | N | B0h |
| PO | SMART WRITE LOG | O | N | B0h |
| ND | STANDBY | M | O | E2h |
| ND | STANDBY IMMEDIATE | M | M | E0h |
| PO | WRITE BUFFER | O | N | E8h |
| DM | WRITE DMA | M | N | CAh |
| DM | WRITE DMA EXT | O | N | 35h |
| DM | WRITE DMA FUA EXT | O | N | 3Dh |
| DMQ | WRITE DMA QUEUED | O | N | CCh |
| DMQ | WRITE DMA QUEUED EXT | O | N | 36h |
| DMQ | WRITE DMA QUEUED FUA EXT | O | N | 3Eh |
| PO | WRITE LOG EXT | O | O | 3Fh |
| PO | WRITE MULTIPLE | M | N | C5h |
| PO | WRITE MULTIPLE EXT | O | N | 39h |
| PO | WRITE MULTIPLE FUA EXT | O | N | CEh |
| PO | WRITE SECTOR(S) | M | N | 30h |
| PO | WRITE SECTOR(S) EXT | O | N | 34h |
| DM | WRITE STREAM DMA EXT | O | N | 3Ah |
| PO | WRITE STREAM EXT | O | N | 3Bh |

(continued)

Page 366

PC3k… SD… Etc…

Web Site www.asoto.com  Email: info@asoto.com


ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

WWW.ASOTO.COM

# OSINT

- Open-source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or classified sources); it is not related to open-source software or public intelligence.

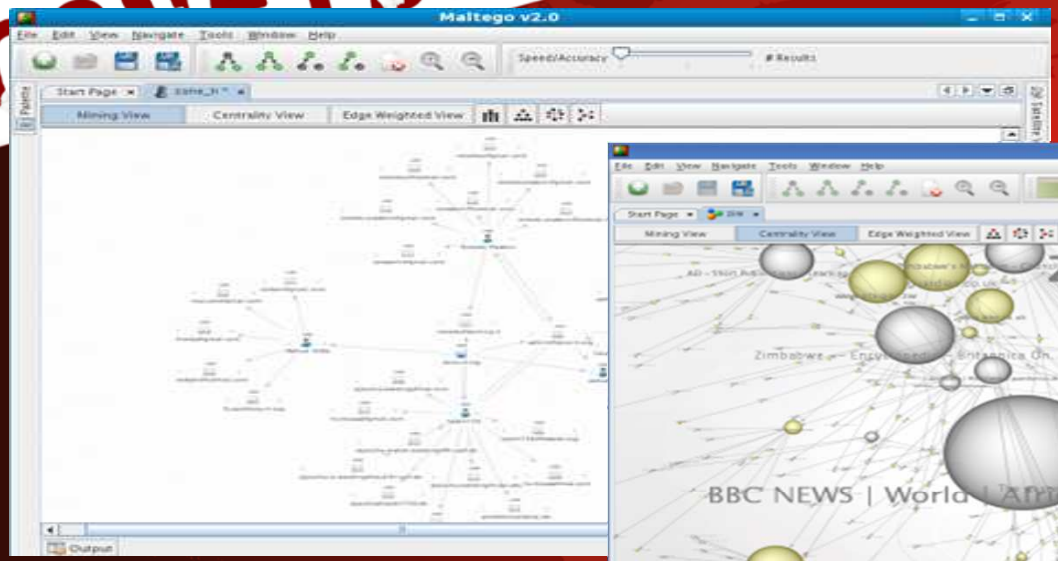
Web Site www.asoto.com  Email: info@asoto.com

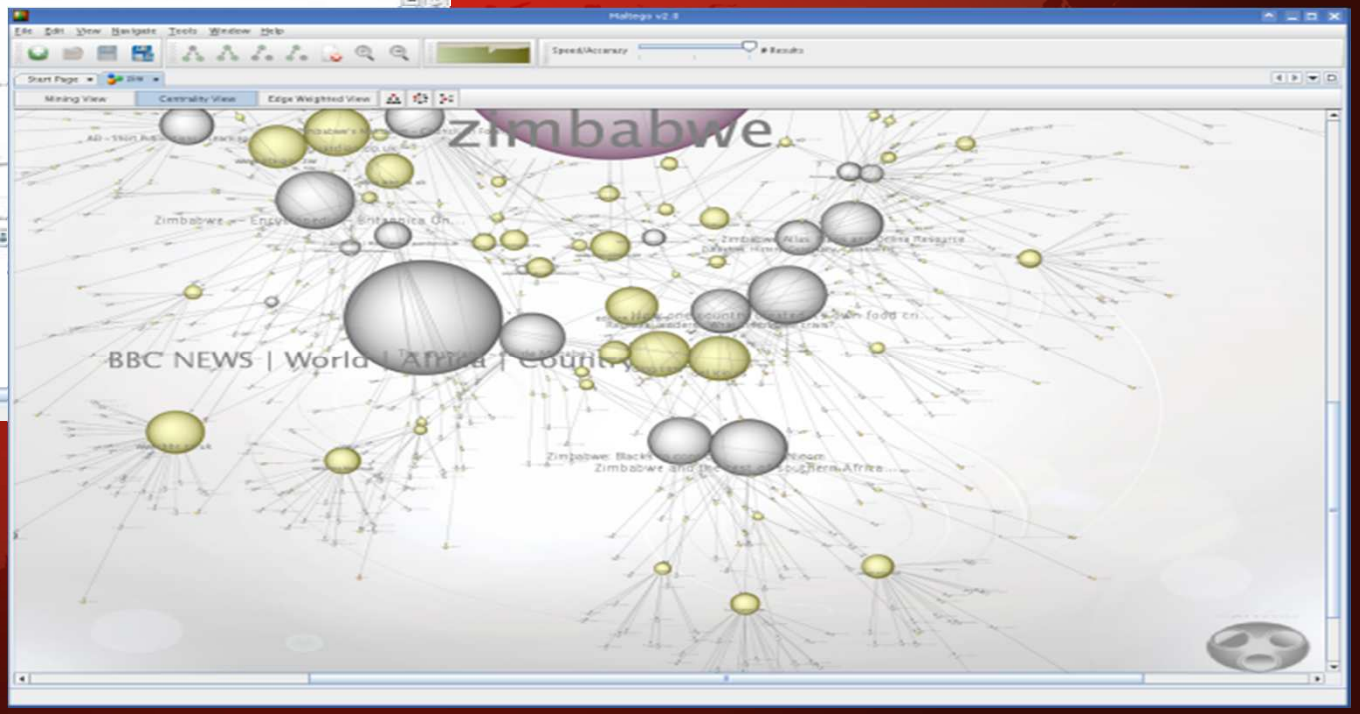
ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# OSINT Free...




Web Site www.asoto.com  Email: info@asoto.com


# More boy toys…

- http://labs.adobe.com/technologies/swfinvestigator/
- IDA+Olly+Syser+Python+.
- http://sourceforge.net/projects/malclassifier.adobe/
- http://aws.amazon.com/free/
- http://corelan.be/


ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS •
DATA RECOVERY • SPECIAL PROJECTS
CONFIDENTIAL
WWW.ASOTO.COM
Conlusions
• teamwork, teamwork, teamwork
• research beyond the standard channels
• reverse engineering
• binary analysis
• VM and isolation
• avoiding self destruction techniques (Media/Mobile)
• hardware hacking…
• reaserch, reaserch, reaserch
• legal - technical integration local, regional and beyond the borders
• concept unification, committee, academy and industry
• welcome ideas, research join efforts
Web Site www.asoto.com  Email: info@asoto.com

ASOTO TECHNOLOGY GROUP
INFORMATION GUARDIANS
IT SECURITY • DIGITAL FORENSICS • DATA RECOVERY • SPECIAL PROJECTS

CONFIDENTIAL

WWW.ASOTO.COM

# QUESTIONS ?

☺