

Evidence

- Oral
 - All Statements which the Court permits or requires to be made by witnesses
 - in relation to matters of fact under inquiry
- Documentary
 - all documents including electronic records produced for the inspection of the Court;

Evidence (Contd..)

- Document

- any matter expressed or described upon any substance by means of
- letters, figures or marks, or by more than one of those means
- to be used or intended to be used
- for recording that matter
- includes the document generated or prepared by electronic machine or technology (ICT Act, 2006)

Evidence (Contd..)

- Electronic Record
 - data, record or data generated, image or sound stored, received or sent
 - in an electronic form or micro film or computer generated micro fiche

Nature of Computer Crimes

- Illegal Act
- Computer is used as tool or target or both
- Electronic Evidence
 - Computer crimes
 - Physical crimes

Collection of digital evidence

- Any action during investigation should not compromise evidence
- If accessing original media is necessary, the IO responsible must be competent to do so
- All procedures should be documented and preserved in a manner verifiable by an independent third party

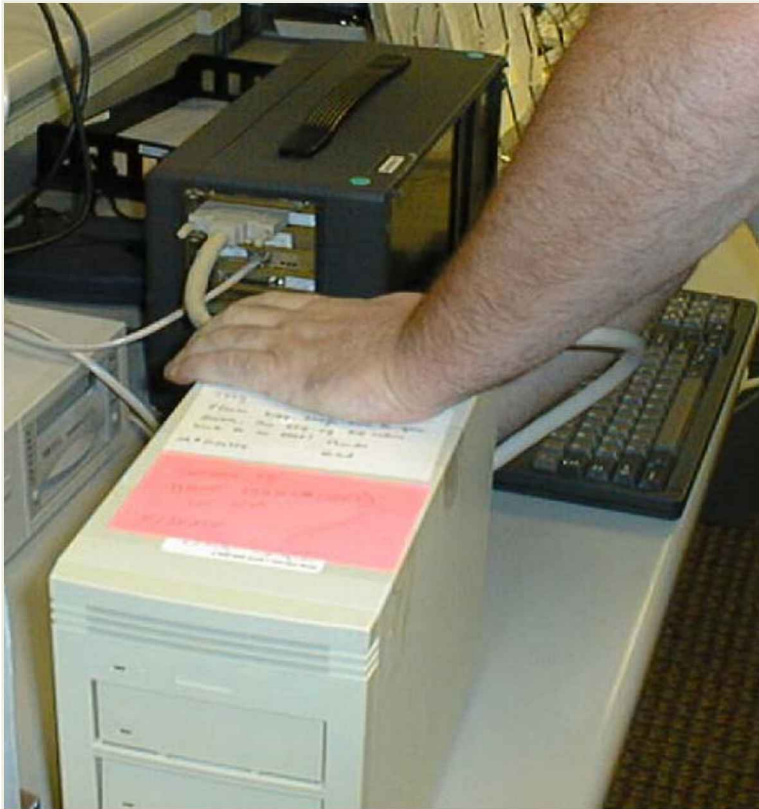
Compromising Evidence

- U.S. Doorframe Case
- Logic Bombs
 - Not switching a suspect computer on or off
- Admissibility

Collection of Computer Evidence

- From volatile memory – RAM
- From the browser
- From secondary memory – HDDs
- Mobile devices



The computer forensics process





- Acquire
- Authenticate
- Analyze
- Document

Select source medium

Clone Disk (Copy Sectors) [X]

Source: medium  

Drive C:

Destination: raw image file  

☒ Copy entire medium

Start sector (source):

Start sector (destination):

Number of sectors to copy:

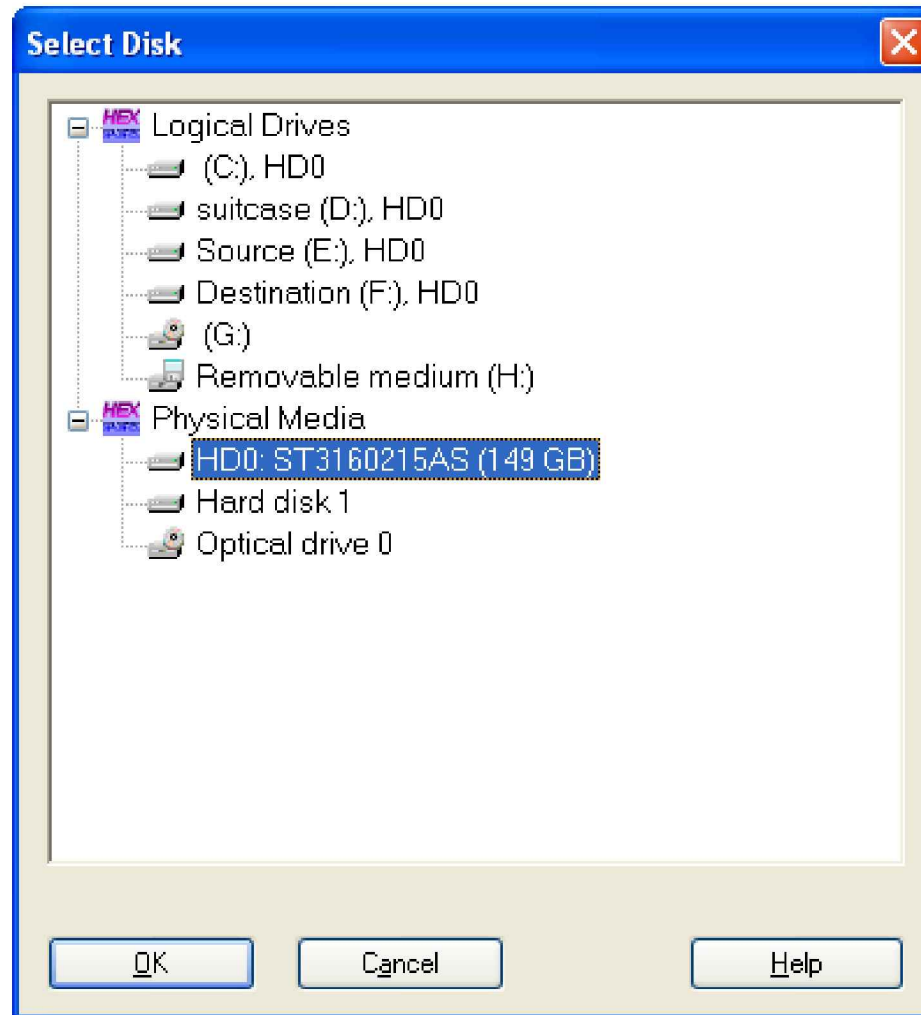
☒ Log procedure silently (no error messages)

☐ Avoid damaged areas. Skip range:

☐ Write pattern for damaged source sectors:

☐ Simultaneous I/O (faster, if source and destination are different physical media)


Select source medium



Select destination for the image file

Clone Disk (Copy Sectors)

Source: medium
Hard disk 0, ST3160215AS (149 GB)

Destination: raw image file


☒ Copy entire medium
Start sector (source): 0
Start sector (destination): 0
Number of sectors to copy: 312581808

☒ Log procedure silently (no error messages)
☐ Avoid damaged areas. Skip range: 32

☒ Write pattern for damaged source sectors: ? BAD SECTOR ?

☐ Simultaneous I/O (faster, if source and destination are different physical media)

OK Cancel Help

Authenticate

- Using hash functions to ensure authenticity of image
- If acquisition hash equals verification hash, image is authentic



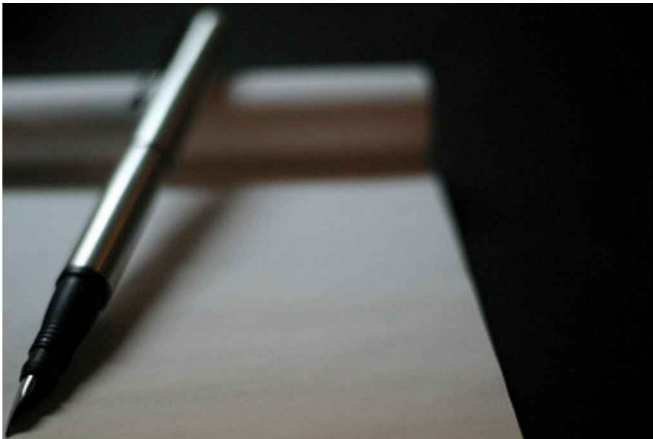
MD5 (128 bit)

...for Drive E:

B4AAE398F81383E43E30A2D5B371400D

Close

Document



- A forensic examination report must
 - List softwares used & their versions
 - be in simple language
 - list the hash results
 - list all storage media numbers, model, make

Document

- Chain-of-custody log
 - ACL of people having access to collected evidence
 - Tracks evidence from source to courtroom
 - Unbroken chain-of-custody authenticates electronic evidence

Document

- The five “Ws” of chain-of-custody log
 - Who – took possession of the evidence
 - What – description of evidence
 - Where – did they take it to
 - When – time and date
 - Why – purpose for taking evidence

The Omega Case

- July 31, 1996
- The Servers of CNC department in Omega Corporation are booted
- Message flash saying file server is being fixed
- Subsequent system crash
- All programs deleted, manufacturing halts

The Omega Case

- No backup tapes found
- All programs and code generators destroyed
- 25, 000 products to customize 500, 000 designs affected
- 34 years of growth lost in 1 year
- Disgruntled network administrator
- Fired because of non – cooperation

The Omega Case

- Network Administrator's house searched
 - Computers, CDs, motherboards, 500 disks, 12 hard drives, 2 formatted backup tapes
 - Backup tapes were labeled 14/5/96 and 1/7/96
- The cause of deletion, a six line program

The Omega Case

- 30/7/96 (Trigger Date)
- F: (Accessing the server)
- F:\LOGIN\LOGIN 12345 (first user logs in with supervisory rights and no password)
- CD\PUBLIC (gives access to the PUBLIC directory, a file system area)
- FIX.EXE /Y F:*.* (Run code, A=Yes, All files)
- PURGE F:\ /ALL

Electronic Evidence

- All items seized from the suspect's house: CDs, HDD, formatted Back up tapes, etc.
- But what is needed to establish guilt beyond reasonable doubt?
 - Correct procedure having been followed by IO
 - The function of the 6 line program (Expert Opinion)
 - The fact that it could only have been installed by the suspect

Collection of digital evidence

- Earlier
 - Optical (CDs, DVDs, etc.)
 - Electro-magnetic (HDDs)
 - SSDs (ROMs, Pen drives, Routers)
 - Networks
- Now
 - Cell phone internal memories
 - Cloud (FB, Insta, GDrive, iCloud, Drop Box, AWS, Azure etc., etc.)
 - IOTs (Cars, TVs, Watches, Speakers, Robo Vacuum cleaners, Aibo, etc., etc., etc.,)

Collection of digital evidence



UFED CelleBrite



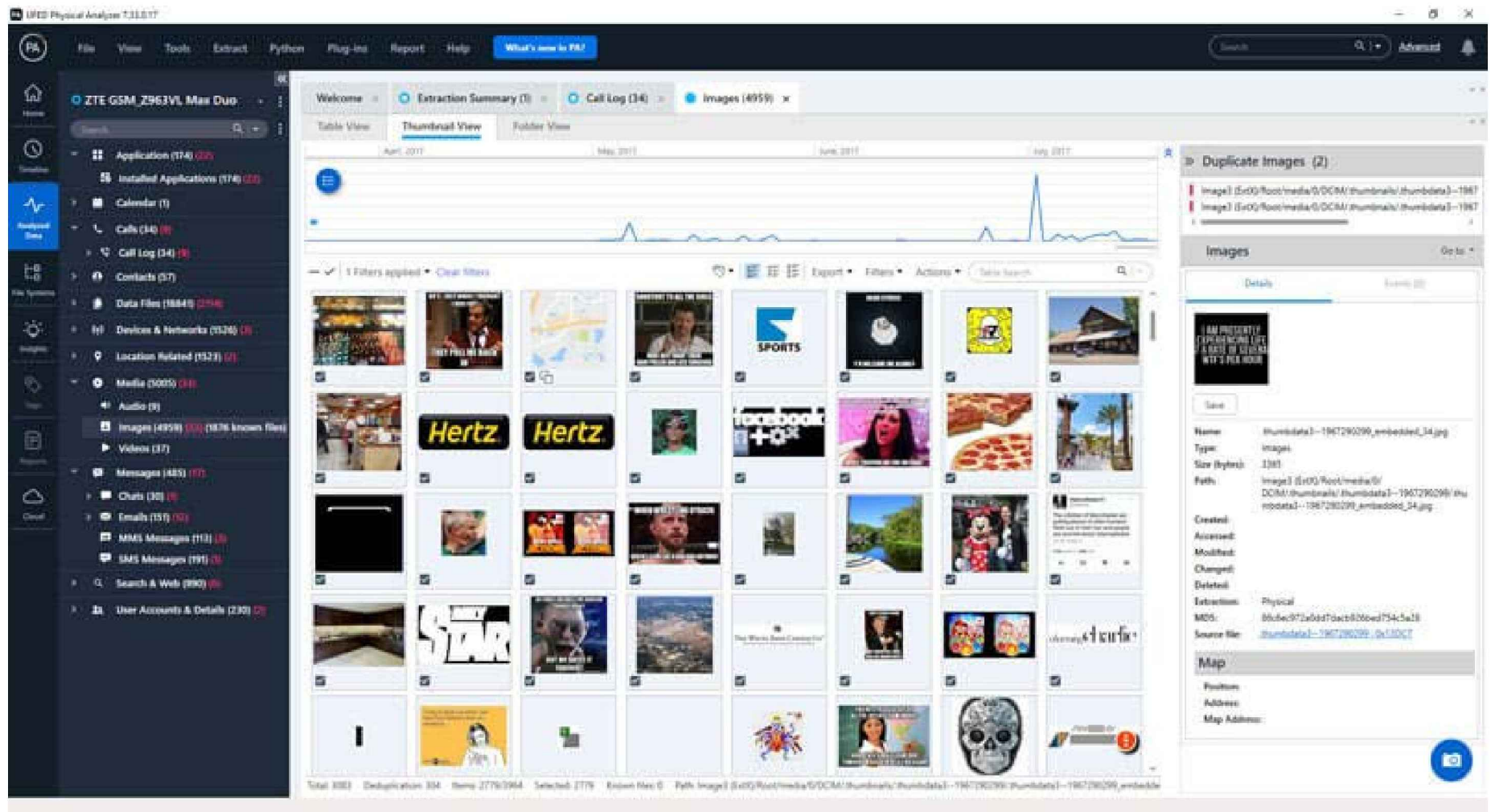
Paraben Cell Phone
Inv. Kit

Collection of digital evidence - Challenge

- Multiple iterations of Operating Systems compel frequent knowledge updates
 - Android 4.0, 4.1, 4.4.....11, 12
 - iOS 1, 2, 3.....15, Ipad OS 13, 14, 15
 - Windows 7, 8, 10, 11 and those before and in between!!
 - MacOS 10, 10.0, 10.1....10.15, 11, 12
 - Domain specific knowledge

Collection of digital evidence - Challenges

- Bugs or Errors in devices used for digital evidence collection, Cellebrite bug (Late 2020)
 - specially formatted file (e.g., a photo) with computer program put in a cell phone app
 - cell phone data acquired by Cellebrite and goes into Cellebrite memory

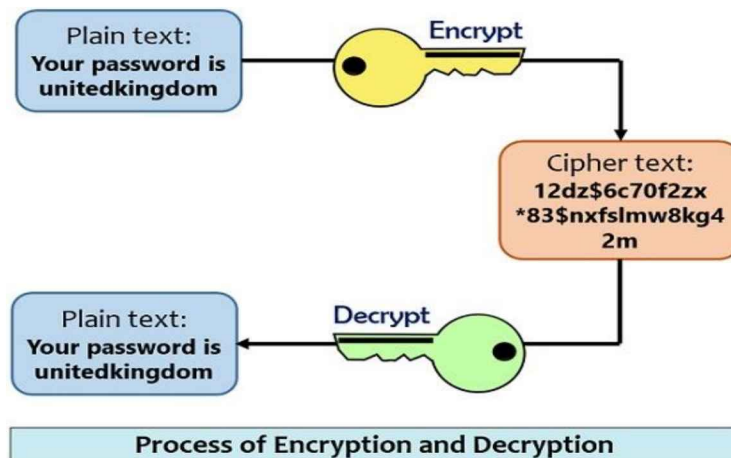


Collection of digital evidence – Challenges (Cellebrite bug)

- Once in memory, the program starts executing and can
 - Modify the current Cellebrite report
 - Modify all previous and future generated Cellebrite reports from all previously scanned cell phone arbitrarily by
 - inserting or removing text, email, photos, contacts, files, etc.
 - with no detectable timestamp changes or checksum failures

Collection of digital evidence – Challenges (Encryption)

- WhatsApp End-to-End encryption
- iOS encryption
- Windows bitlocker drive encryption



Circuit Globe

Preservation of digital evidence

- Electronic storage media not as robust as paper or parchment
- Has to be protected from
 - Shock, deterioration of the media itself
 - Moisture
 - Electro-magnetic fields
 - Temperature

Preservation of digital evidence

- Section 44 – Digital Security Act, 2018
 - *The Director General of Digital Security Agency, on application of IO or suo motu, require preservation of computer information*
 - *Upto 90 days that can be extended upto 180 days*
 - *Essential for ISPs in Internet based crimes*

Internet based crimes

- DNS spoofing
- Web defacement
- FTP attacks
- Bogus Websites
- Web spoofing
- Website based launch of malicious code, cheating and fraud

Fundamentals of investigation

- The KEY to almost all web based crimes
 - **IP Address**
 - Figures in server logs
 - Figures in email headers
- Identify the correct IP address
 - Time zones
 - Shivaji Maharaj (Airtel case)

Fundamentals of investigation

- Track physical location of the IP Address
- Identify the suspect computer to which the IP address was allotted
- Collect corroborative evidence from suspect computer

Whois Search

Whois search for 208.113.199.97 using www.whois.net

OrgName: New Dream Network, LLC
OrgID: [NDN](#)
Address: 417 Associated Rd
Address: PMB #257
City: Brea
StateProv: CA
PostalCode: 92821
Country: US

NetRange: [208.113.128.0](#) - [208.113.255.255](#)
CIDR: [208.113.128.0/17](#)
NetName: [DREAMHOST-BLK6](#)
NetHandle: [NET-208-113-128-0-1](#)
Parent: [NET-208-0-0-0-0](#)
NetType: Direct Allocation
NameServer: NS1.DREAMHOST.COM
NameServer: NS2.DREAMHOST.COM
NameServer: NS3.DREAMHOST.COM
Comment:
RegDate: 2006-04-12
Updated: 2007-11-01

Extended Info

IP Address: [208.113.199.97](#)

IP Location:  United States

Website Status: [active](#)

Server Type: Apache/2.0.61 (Unix) PHP/4.4.7

mod_ssl/2.0.61 OpenSSL/0.9.7e mod_fastcgi/2.4.2

DAV/2 SVN/1.4.2

Cache Date: 2008-04-29 03:21:29 MST

Server Logs

#Software: Microsoft Internet Information
Services 6.0

#Version: 1.0

#Date: 2007-10-13 06:45:10

2007-10-13 00:45:26 172.224.24.114 -67.19.217.53 80
GET /index.htm - 200 7930 248 31
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+200
0+Server)

Relevant Provisions

- Digital Security Act, 2018 (Notified Sep 30, 2019)
 - S/51. Taking opinion of experts, training, etc.
 - *The Tribunal or the Appellate Tribunal may, during trial, take independent opinion from any person expert in computer science, cyber forensic.....*
 - S/58 Evidentiary value
 - *Notwithstanding anything contained contrary in the Evidence Act, 1872any forensic evidence obtained or collected under this Act shall be admitted as an evidence in the trial.*

Appreciation

- Relevancy of facts – What is relevant will be admissible
 - Cyber forensic expert opinion under section 45
 - File meta data to recreate chain of events
 - Traffic data and log extracts for internet based offences
 - Email headers where supporting evidence is to be collected from suspect communication

Questions?