COMPSCI4062/COMPSCI5063 Cyber Security Fundamentals (CSF)

Lecture 9

Digital Forensics

Digital Forensics

- is a digital investigation focuses on a digital device
  - Computer
  - Router
  - Switch
  - Cell-phone
  - SIM-card
  - ….

- Focuses on a digital device involved in an incident or crime
  - Computer intrusion
  - Generic criminal activity
    - Perpetrator uses internet to gather information used in the perpetration of a crime
  - Digital device is an instrument of a crime
    - Perpetrator uses cell-phone to set-off a bomb
    - Email scams
    - Internet auction fraud
    - Computer is used for intrusion of another system

Digital Forensics

- Digital Investigation has different goals
  - Prevention of further intrusions
    - ❖Goal is to reconstruct modus operandi of intruder to predict and prevent further intrusions
  - Assessment of damage
    - ❖Goal is to certify system for safe use
  - Reconstruction of an incident
    - ❖For criminal proceeding
    - ❖For organization-internal proceedings

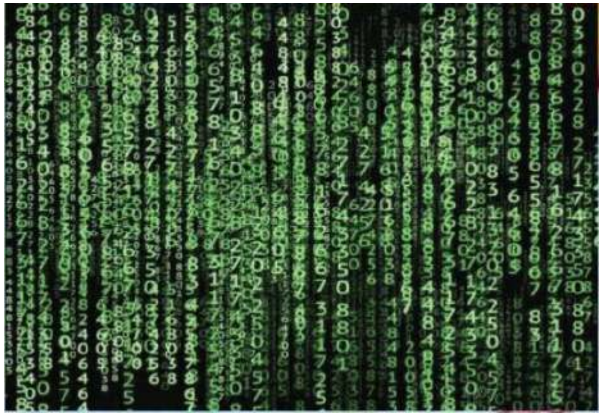
- Process where we develop and test hypotheses that answer questions about digital events
  - We can use an adaptation of the scientific method where we establish hypotheses based on findings and then (if possible) test our hypotheses **against** findings resulting from additional investigations

- Evidence
- Procedural notion
- That on what our findings are based
- Legal notion
- Defined by the “rules of evidence”
- Differ by legislation
- “hear-say” is procedurally evidence, but excluded (under many circumstances) as legal evidence

Types of digital forensics

Computer Forensics

Network Forensics



Mobile Forensics

Forensic Data Analysis (FDA)

- **Digital Forensics** is a procedure of acquiring and processing data found in digital devices. Digital Forensics was used as a synonym of computer forensics in early years but now there are different categories depending on the type of the digital evidence and procedures.
- **Computer Forensics** is the procedure of acquiring a snapshot of **the internal state of a computer system** (cloning the **hard drive/memory**) and moving on in analysing the acquired copy.

- **Network forensics** is focusing on the **communication aspect** of the device and it captures **the traffic** as data for further analysis; helps in intrusion detection.
- **Mobile Forensics** is representing practices employed for **recovering data from a mobile device.**
- **Forensic data analysis** is another branch which focuses on structured data analysis relevant to **financial crimes.**
- Most of the time these practices are used in **digital crime investigations** and the goal is to lead into **successful prosecution**

Who should know about digital forensics

- Those involved in legal proceedings that might use digital evidence
  - Judges, prosecutors, attorneys, law enforcement, expert witnesses
- Those involve in systems administration
  - Systems administrators, network administrators, security officers
  - Those writing procedures
  - Managers

Is computer Forensics Important?

- Need to know how to recover data
- What if you work as an investigator in the Law enforcement?
- Be able to discover malicious activities

Computer Forensics Steps

1. Seizure
2. Acquisition
3. Analysis: Physical searching + whitelist + registry examination + Browser Analysis + Timeline Reconstruction

4. Reporting

Note

- Upon arriving at a crime scene a forensic investigator should be cautious. The forensic investigator must search the crime scene extensively, label and register in a formal form all the hardware equipment found and place them safely in antistatic bags. The hard drive must be removed if a desktop is discovered powered off and placed in a safe box. If a desktop is powered on an investigator needs to decide if he/she will proceed with a live forensics procedure.

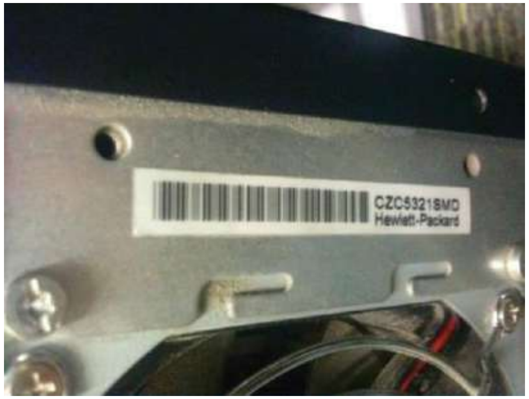
- All these steps will be analysed in the following slides.
- Taking pictures and screenshots for supporting evidence is essential in the investigation.

Step 1: Seizure (1/2)

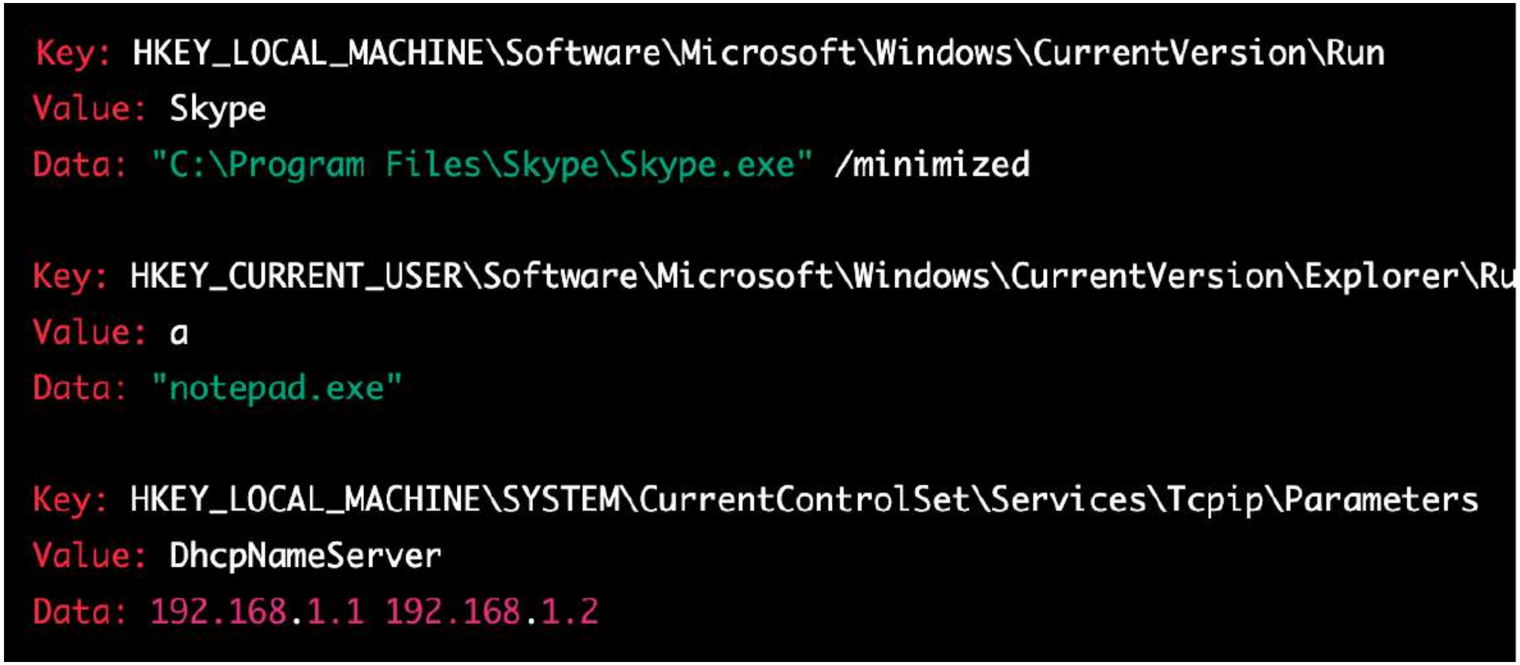
- Purpose: prevent digital devices being used and data getting changed
- Inspection of equipment – labelling – **Registry** – Bagging – Bios Time (F10) & Hard Drive details
- Be prepared for a tower bomb or even USBs hidden inside a plug
- Equipment is on; What now?

Should the investigator turn off the found computer in the scene?

Step 1: Seizure (2/2)



- Note
  - Getting the time from BIOS is important as if this is set wrongly some evidence might be pointing us in the wrong direction.
  - A registry table example



```
Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Value: Skype
Data: "C:\Program Files\Skype\Skype.exe" /minimized

Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Ru
Value: a
Data: "notepad.exe"

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value: DhcpNameServer
Data: 192.168.1.1 192.168.1.2
```

Step 2: Acquisition

- Creating a digital forensic copy! A forensic copy can have different types of format but we will just concentrate on the **raw format**. Use of **write blockers** is important!
- Bit-by-bit copy of the data using a tool like **Data Duplication** or **FKT imager** to create a forensic image of the device

Step 2: Acquisition

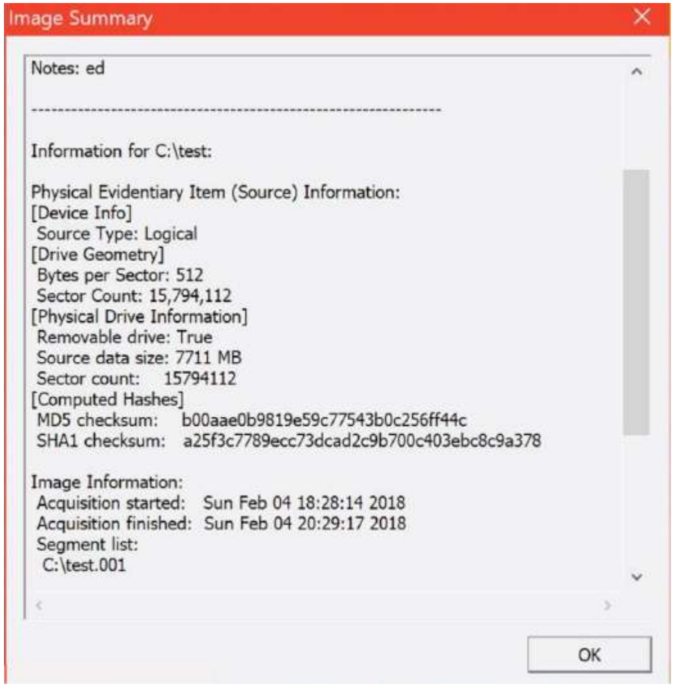


Image Summary

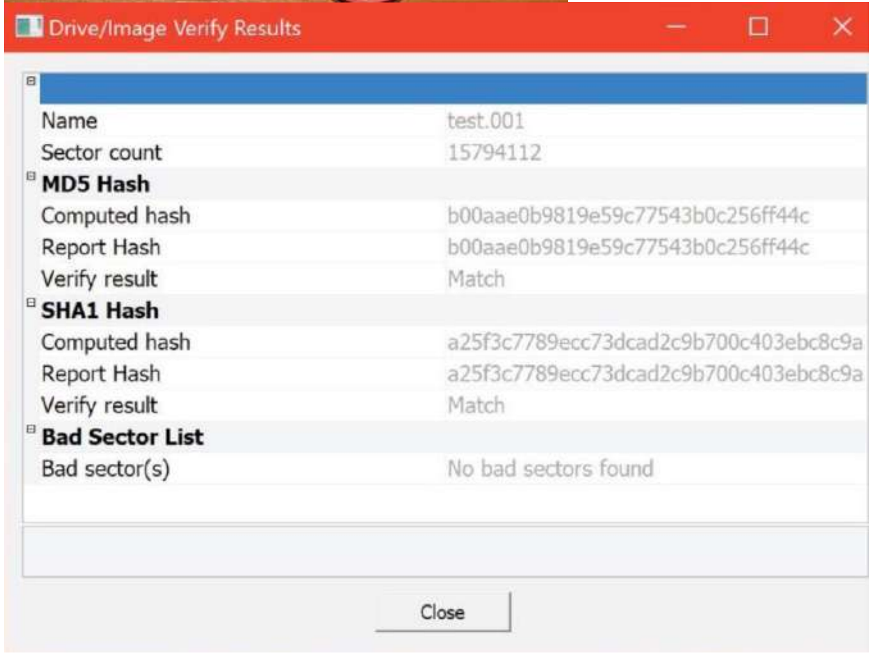
```
Notes: ed

--------------------------------------------------------------

Information for C:\test:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 15,794,112
[Physical Drive Information]
 Removable drive: True
 Source data size: 7711 MB
 Sector count:    15794112
[Computed Hashes]
 MD5 checksum:    b00aae0b9819e59c77543b0c256ff44c
 SHA1 checksum:   a25f3c7789ecc73dcad2c9b700c403ebc8c9a378

Image Information:
 Acquisition started:  Sun Feb 04 18:28:14 2018
 Acquisition finished:  Sun Feb 04 20:29:17 2018
 Segment list:
  C:\test.001
```



Drive/Image Verify Results

Name	test.001
Sector count	15794112
MD5 Hash	
Computed hash	b00aae0b9819e59c77543b0c256ff44c
Report Hash	b00aae0b9819e59c77543b0c256ff44c
Verify result	Match
SHA1 Hash	
Computed hash	a25f3c7789ecc73dcad2c9b700c403ebc8c9a
Report Hash	a25f3c7789ecc73dcad2c9b700c403ebc8c9a
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

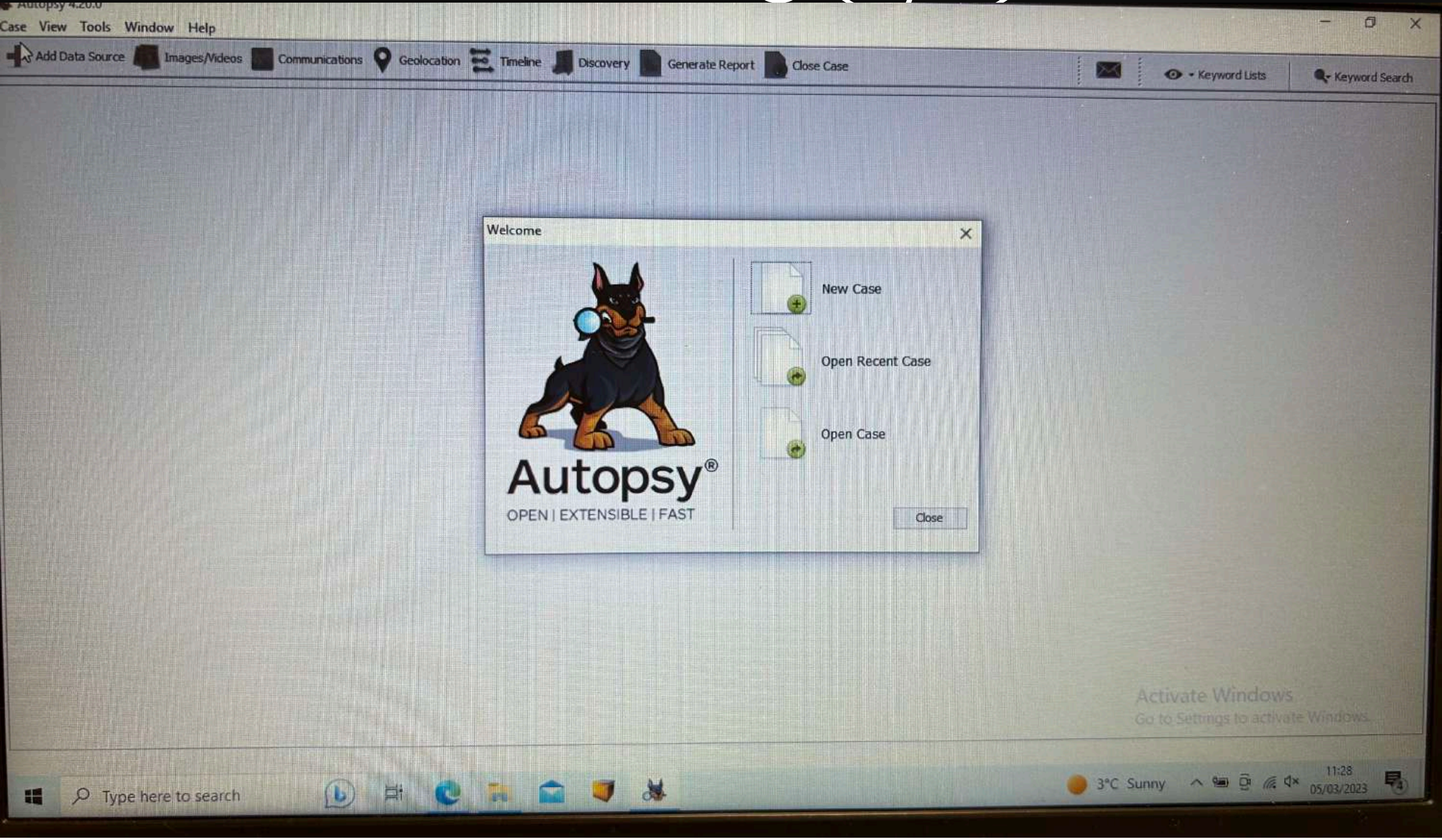
- After the seizure has taken place the forensic investigator will take the hard drive or laptop and generate a clone copy of its content.
- For this clone a specific **hash value** will be generated and kept safely; in this way the forensic examiner will ensure that while analysing the data he\she will not make any changes in the copy and use it as a proof that can be presented in court.
- It is a good practice for an investigator to work on a second copy; so if anything goes wrong he/she does not have to re-do this step.

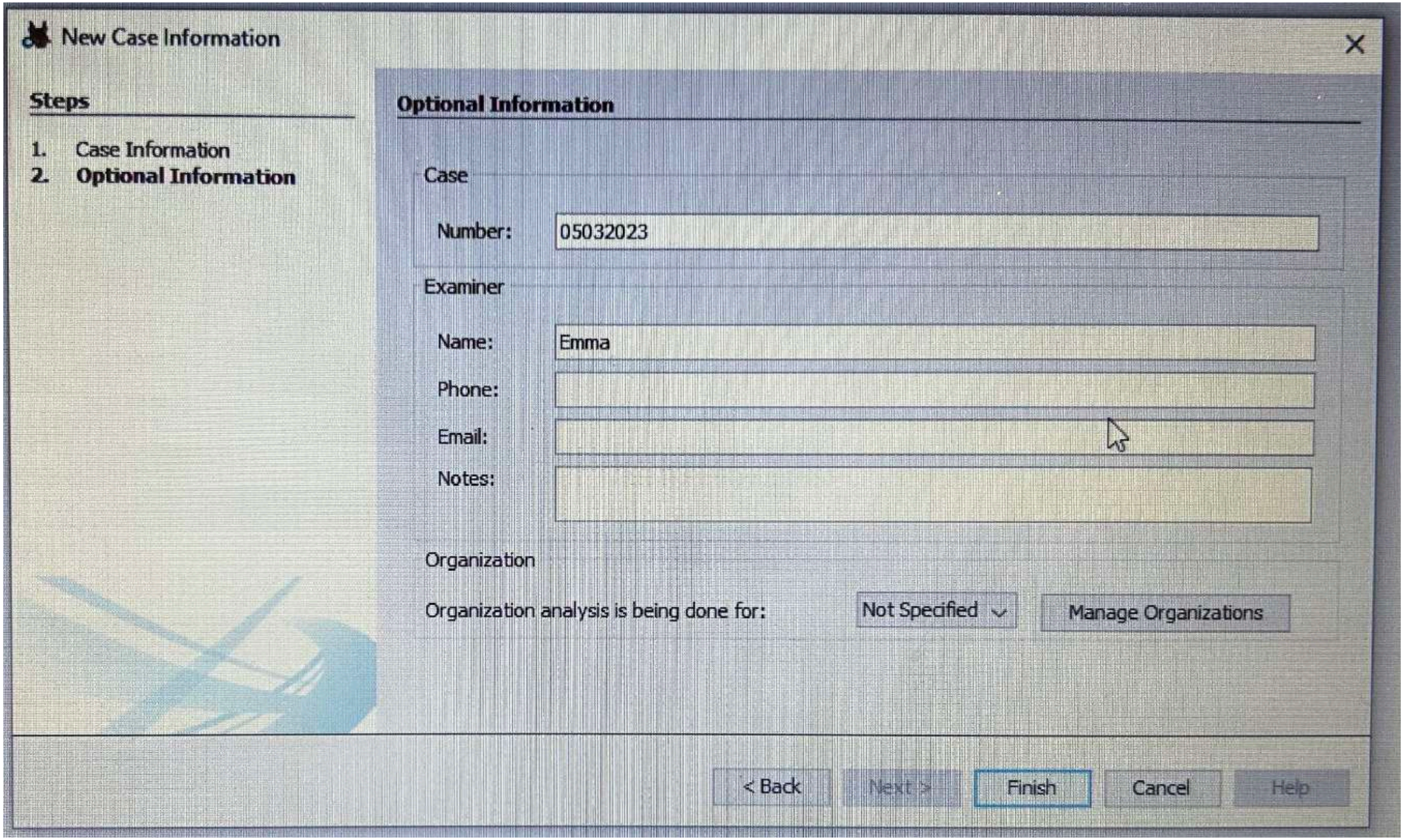
- Tools can be used (e.g., **FTK Imager)** to acquire a copy of a forensic image.
- There're the different types of format that exist; raw format is a bit by bit copy often accompanied with metadata of the suspect drive.
- **Write blockers** ensure that nothing can be written on the suspect drive which helps in eliminating the possibility of contaminating evidence

Step 3: Analysis – Physical Searching (1/3)

- Creating a case using **Autopsy**
  - ✓First thing is to make a **hash check**
  - ✓String commands, indexing, **grep search** via index & foremost, file carving
  - ✓Use of **foremost** for extracting all the files
    - ✓Foremost is command-line tool to recover deleted files from disk images

Step 3: Analysis – Physical Searching (2/3)





Optional Information

Case

Number: 05032023

Examiner

Name: Emma

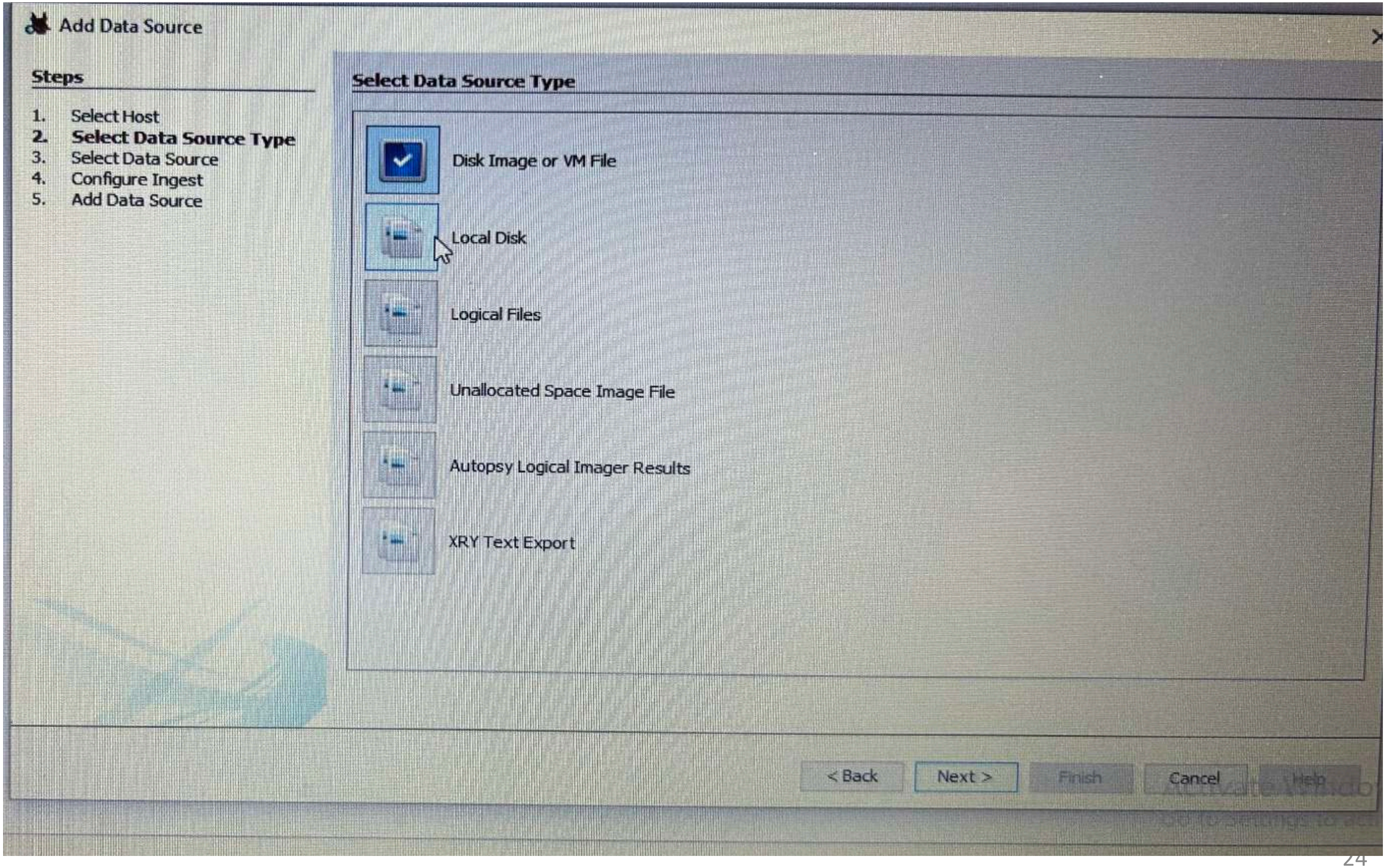
Phone:

Email:

Notes:

Organization

Organization analysis is being done for: Not Specified



Add Data Source

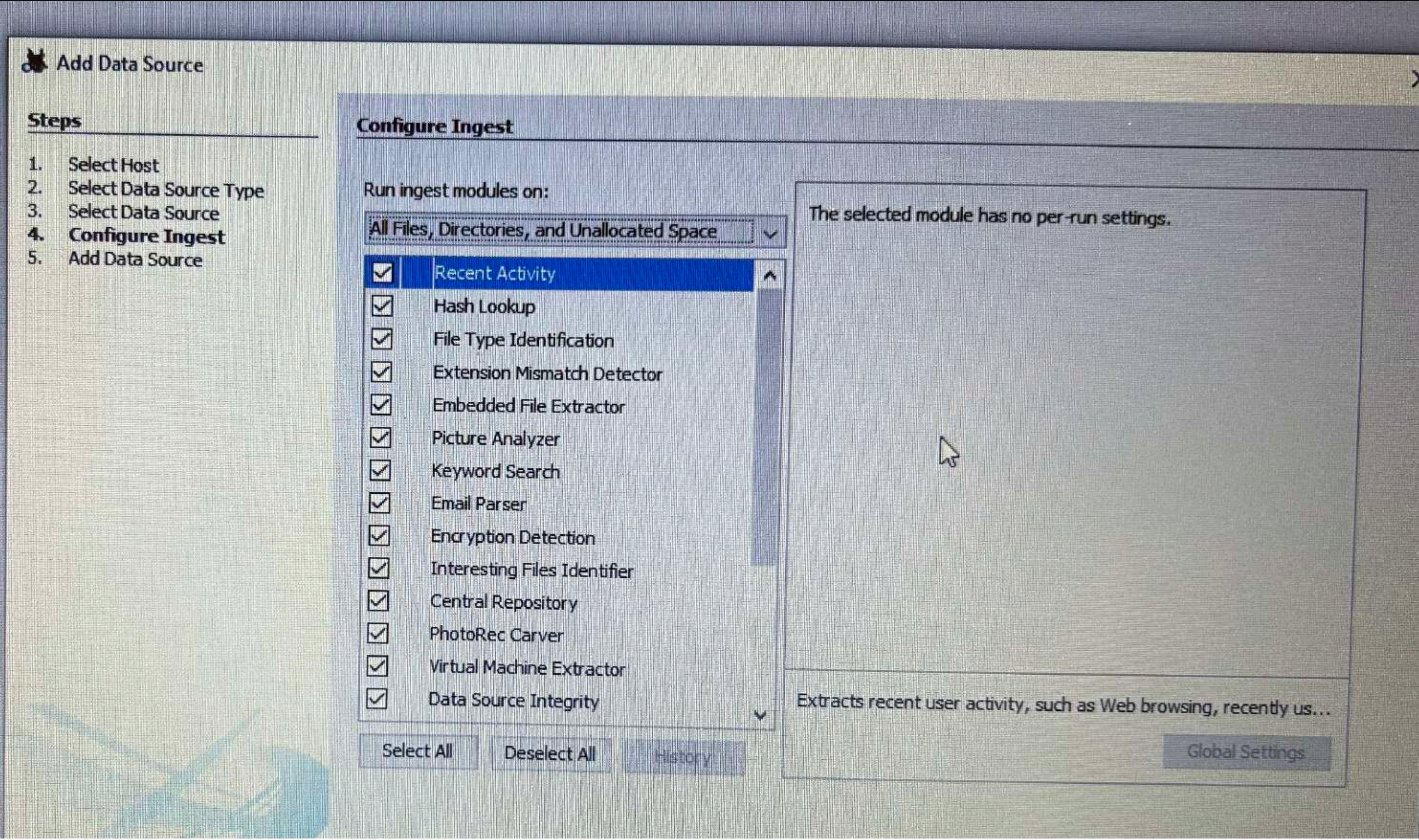
Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

Activate Windo
Go to Settings to act



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

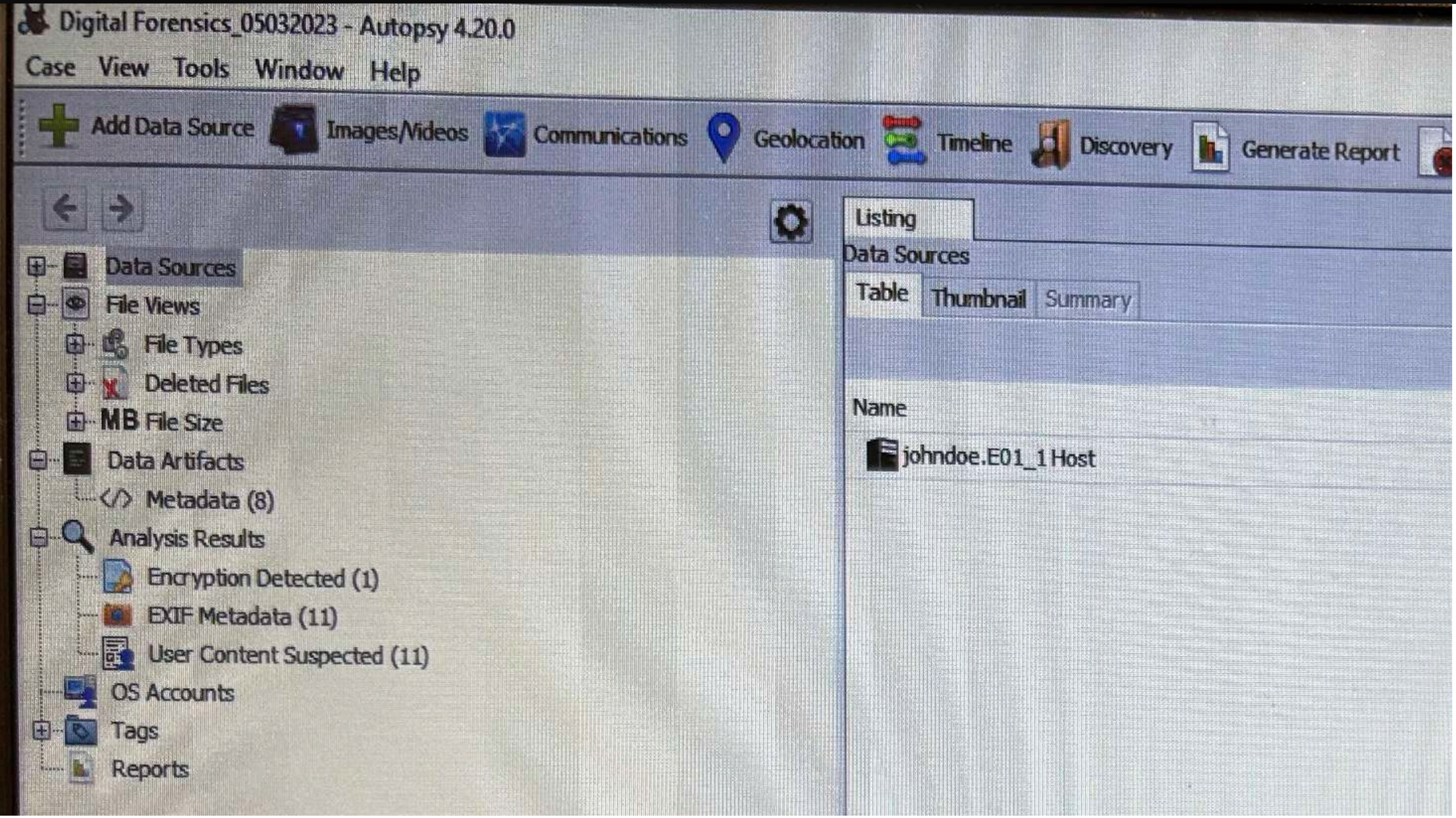
Run ingest modules on:

All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...



johndoe.E01_1 Host

Notes

- In the analysis step the forensics investigator searches for evidence in the acquired copy. There are multiple searching techniques that can be employed that will result in different types of information.
- List of **users, emails, documents, and pictures** are some of the files that can be fully recovered and examined.
- Always make a **hash comparison** to ensure your copy has not been compromised in any way. A good tool that can be used for loading an image and moving into the analysis is called **Autopsy**.

Notes

- There are different commands that can be used upon searching for evidence in a forensic copy. **Keyword searching** reminds a bit of google searching. Depending on what type of investigation you have different relevant words that can be "good" candidates.
- The **grep command** is used for specific files that you want to be extracted. Foremost is one of the most useful ones as it can extract from our copy all the recovered data and separate them in different folders depending on their file type; one for .doc, .pdf etc.
- Metacam is specifically used for getting into the .jpeg directory. As you dig deeper you might find information also about the type of the camera that was used to take these photos

Step 3: Analysis – Whitelist Production

- Creation of Windows XP image (qemu) containing known “good” hashes for filtering
  - Use of **md5deep** for creating lists
  - Use of cut and grep commands for comparing the lists

Notes

- Depending on the suspect’s operating system in this case Windows XP you will have to load and create a good hashing list (whitelist) and then compare it with the list that you can extract from your forensic copy

Step 3: Analysis - Registry Examination (1/2)

- Identifying the users and all the installed applications and devices on the suspect OS
  - ✓Copy the registry files from the suspect image file
  - ✓Use of **regviewer** for the registry examination

Step 3: Analysis - Registry Examination (2/2)

- User Activity Tracking
- Malware Analysis
- Network Activity Analysis
- Recovery of Deleted Data
- User Authentication Analysis

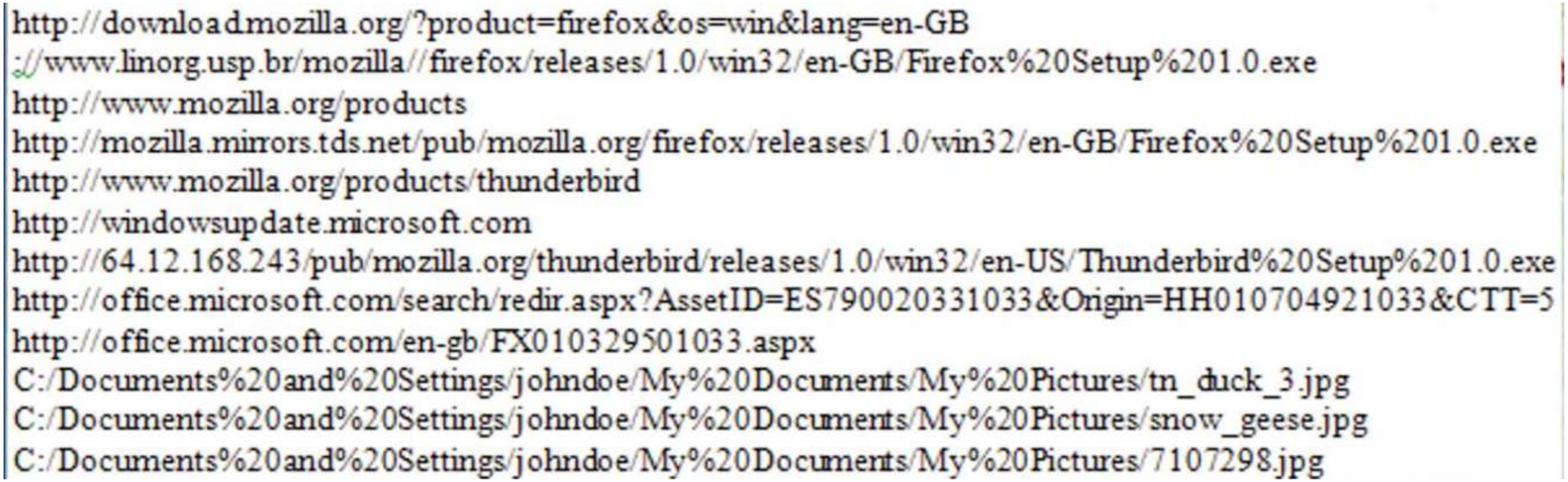
Note

- You have to examine all the registry files in order to identify all the users and the applications which were part of the system. **RegViewer** is a tool that will help you examine registry files and it gives the data in a structured

Step 3: Analysis - Browser Analysis (1/2)

- Analysis of Browser activities
  - Use of **Autopsy** for discovering the browser files and also the history index.dat file from the browser
  - Analysis of bookmarks and recent items

Step 3: Analysis - Browser Analysis (2/2)

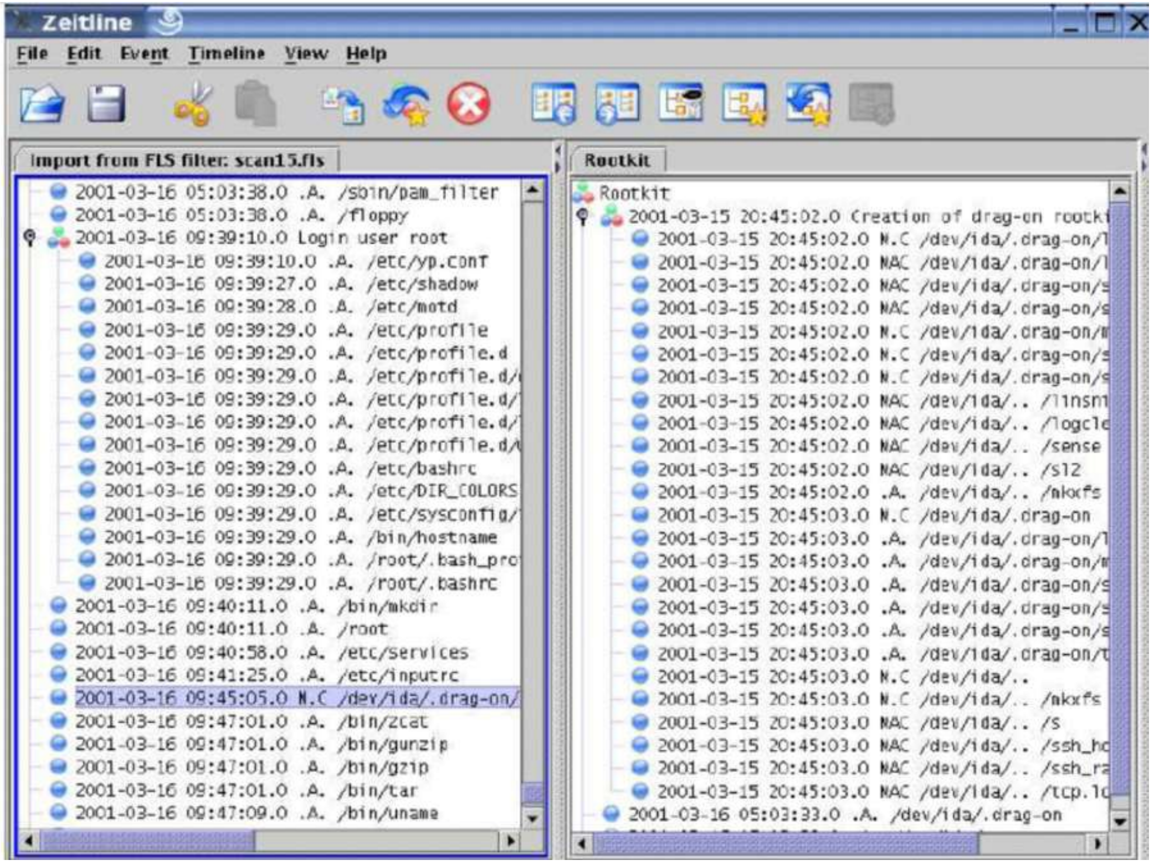


```
http://download.mozilla.org/?product=firefox&os=win&lang=en-GB
://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe
http://www.mozilla.org/products
http://mozilla.mirrors.tds.net/pub/mozilla.org/firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe
http://www.mozilla.org/products/thunderbird
http://windowsupdate.microsoft.com
http://64.12.168.243/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe
http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&Origin=HH010704921033&CTT=5
http://office.microsoft.com/en-gb/FX010329501033.aspx
C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg
C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg
C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg
```

- Notice that the suspect has installed a windows update and has been accessing some photos saved on their device

Step 3: Analysis & Reconstruction

- Creation of .fls file and use of Zeitline for examining all the events
- Creation of events' timeline by using Zeitline;
- Filtering and dig further


Zeitline
File Edit Event Timeline View Help
Import from FLS filter: scan15.fls
Rootkit

```
  2001-03-16 05:03:38.0 .A. /sbin/pam_filter
  2001-03-16 05:03:38.0 .A. /floppy
  2001-03-16 09:39:10.0 Login user root
    2001-03-16 09:39:10.0 .A. /etc/yp.conf
    2001-03-16 09:39:27.0 .A. /etc/shadow
    2001-03-16 09:39:28.0 .A. /etc/motd
    2001-03-16 09:39:29.0 .A. /etc/profile
    2001-03-16 09:39:29.0 .A. /etc/profile.d
    2001-03-16 09:39:29.0 .A. /etc/profile.d/
    2001-03-16 09:39:29.0 .A. /etc/profile.d/
    2001-03-16 09:39:29.0 .A. /etc/profile.d/
    2001-03-16 09:39:29.0 .A. /etc/profile.d/
    2001-03-16 09:39:29.0 .A. /etc/bashrc
    2001-03-16 09:39:29.0 .A. /etc/DIR_COLORS
    2001-03-16 09:39:29.0 .A. /etc/sysconfig/
    2001-03-16 09:39:29.0 .A. /bin/hostname
    2001-03-16 09:39:29.0 .A. /root/.bash_pro
    2001-03-16 09:39:29.0 .A. /root/.bashrc
  2001-03-16 09:40:11.0 .A. /bin/mkdir
  2001-03-16 09:40:11.0 .A. /root
  2001-03-16 09:40:58.0 .A. /etc/services
  2001-03-16 09:41:25.0 .A. /etc/inputrc
  2001-03-16 09:45:05.0 M.C /dev/ida/.drag-on/
  2001-03-16 09:47:01.0 .A. /bin/zcat
  2001-03-16 09:47:01.0 .A. /bin/gunzip
  2001-03-16 09:47:01.0 .A. /bin/gzip
  2001-03-16 09:47:01.0 .A. /bin/tar
  2001-03-16 09:47:09.0 .A. /bin/uname
```

```
Rootkit
  2001-03-15 20:45:02.0 Creation of drag-on rootk
    2001-03-15 20:45:02.0 M.C /dev/ida/.drag-on/l
    2001-03-15 20:45:02.0 MAC /dev/ida/.drag-on/l
    2001-03-15 20:45:02.0 MAC /dev/ida/.drag-on/s
    2001-03-15 20:45:02.0 MAC /dev/ida/.drag-on/s
    2001-03-15 20:45:02.0 M.C /dev/ida/.drag-on/m
    2001-03-15 20:45:02.0 M.C /dev/ida/.drag-on/s
    2001-03-15 20:45:02.0 M.C /dev/ida/.drag-on/s
    2001-03-15 20:45:02.0 MAC /dev/ida/.. /linsn
    2001-03-15 20:45:02.0 MAC /dev/ida/.. /logcl
    2001-03-15 20:45:02.0 MAC /dev/ida/.. /sense
    2001-03-15 20:45:02.0 MAC /dev/ida/.. /sl2
    2001-03-15 20:45:02.0 .A. /dev/ida/.. /mkxfs
    2001-03-15 20:45:03.0 M.C /dev/ida/.drag-on
    2001-03-15 20:45:03.0 .A. /dev/ida/.drag-on/l
    2001-03-15 20:45:03.0 .A. /dev/ida/.drag-on/m
    2001-03-15 20:45:03.0 .A. /dev/ida/.drag-on/s
    2001-03-15 20:45:03.0 .A. /dev/ida/.drag-on/s
    2001-03-15 20:45:03.0 .A. /dev/ida/.drag-on/s
    2001-03-15 20:45:03.0 .A. /dev/ida/.drag-on/t
    2001-03-15 20:45:03.0 M.C /dev/ida/..
    2001-03-15 20:45:03.0 M.C /dev/ida/.. /mkxfs
    2001-03-15 20:45:03.0 MAC /dev/ida/.. /s
    2001-03-15 20:45:03.0 MAC /dev/ida/.. /ssh_h
    2001-03-15 20:45:03.0 MAC /dev/ida/.. /ssh_r
    2001-03-15 20:45:03.0 MAC /dev/ida/.. /tcp.l
  2001-03-16 05:03:33.0 .A. /dev/ida/.drag-on
```

Notes

- Identification of current user at a certain time is really important as this can be used as evidence.
- So establishing a timeline is one of the most crucial parts of the investigation

Step 4: Report

- Job Description and Instructions
- Description of recovered/examined items
- Analysis of methodology
- Production list and associated description

Note

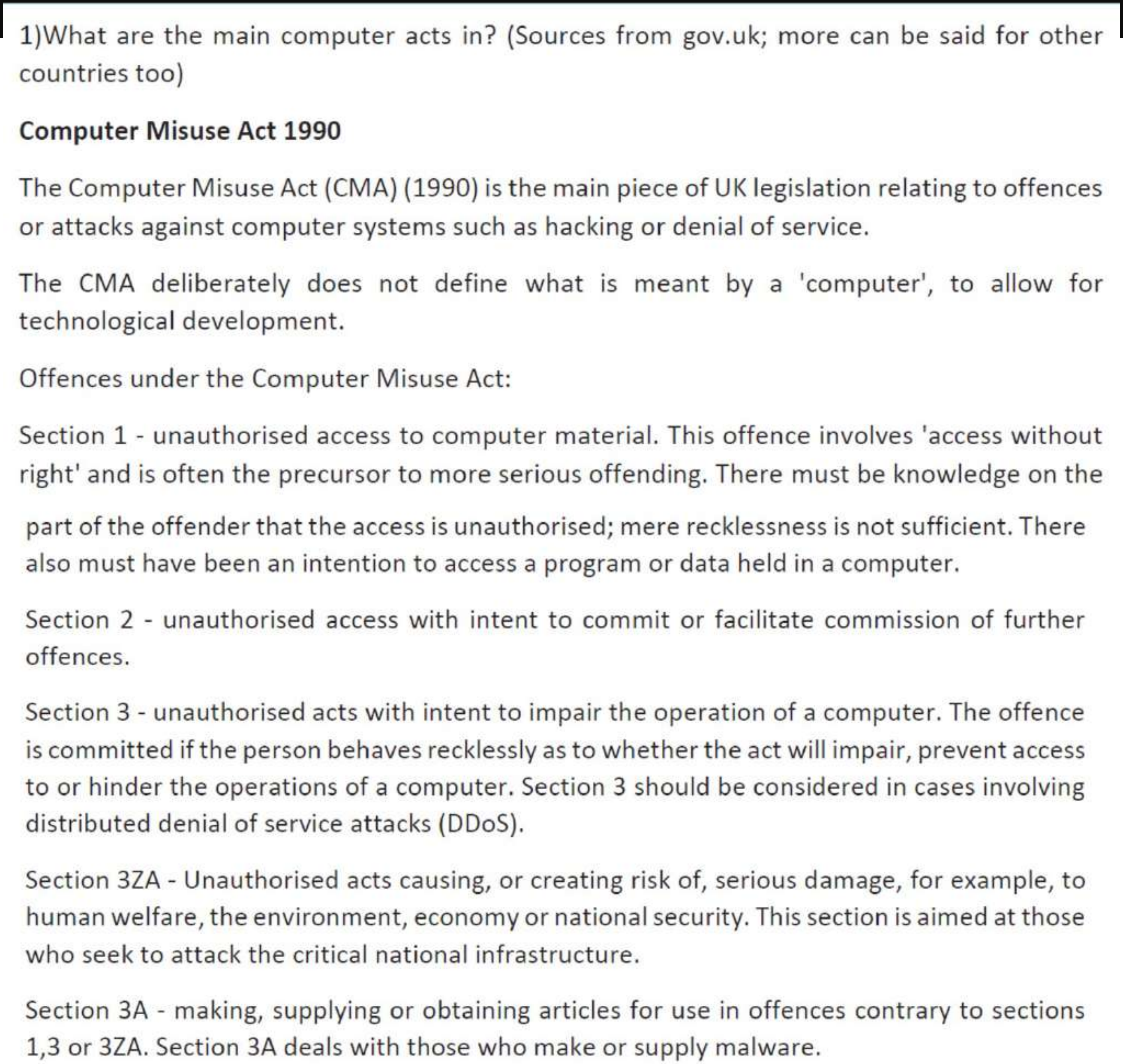
- Once the analysis is complete the forensic investigator will need to prepare a report with all the findings and prepare to testify if needed in court. The report should be extensive containing a register of evidence not biased by any personal opinions.
- In the report a specific structure should be followed and all evidence should be referenced and presenting with not any personal opinions emerging

Interesting hot topics

- Main “Computer crime” acts?
- Is there any difference between England’s and Scotland’s legislation?
- What is a Trojan defense?
- What if someone used your wireless broadband for illegal activities?

Summary

Note 1/4



1)What are the main computer acts in? (Sources from gov.uk; more can be said for other countries too)

Computer Misuse Act 1990

The Computer Misuse Act (CMA) (1990) is the main piece of UK legislation relating to offences or attacks against computer systems such as hacking or denial of service.

The CMA deliberately does not define what is meant by a 'computer', to allow for technological development.

Offences under the Computer Misuse Act:

Section 1 - unauthorised access to computer material. This offence involves 'access without right' and is often the precursor to more serious offending. There must be knowledge on the part of the offender that the access is unauthorised; mere recklessness is not sufficient. There also must have been an intention to access a program or data held in a computer.

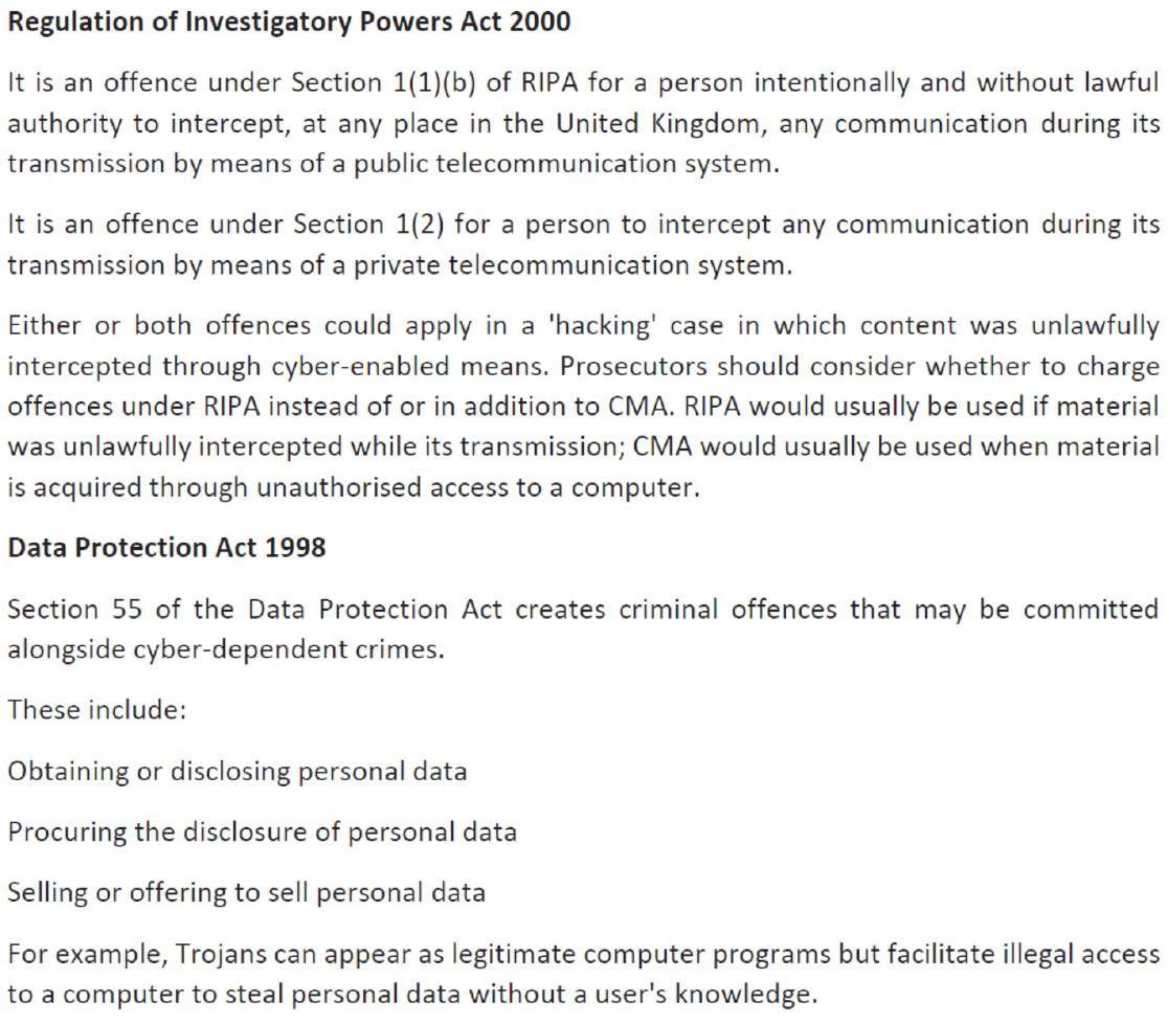
Section 2 - unauthorised access with intent to commit or facilitate commission of further offences.

Section 3 - unauthorised acts with intent to impair the operation of a computer. The offence is committed if the person behaves recklessly as to whether the act will impair, prevent access to or hinder the operations of a computer. Section 3 should be considered in cases involving distributed denial of service attacks (DDoS).

Section 3ZA - Unauthorised acts causing, or creating risk of, serious damage, for example, to human welfare, the environment, economy or national security. This section is aimed at those who seek to attack the critical national infrastructure.

Section 3A - making, supplying or obtaining articles for use in offences contrary to sections 1,3 or 3ZA. Section 3A deals with those who make or supply malware.

Note 2/4



Regulation of Investigatory Powers Act 2000

It is an offence under Section 1(1)(b) of RIPA for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication during its transmission by means of a public telecommunication system.

It is an offence under Section 1(2) for a person to intercept any communication during its transmission by means of a private telecommunication system.

Either or both offences could apply in a 'hacking' case in which content was unlawfully intercepted through cyber-enabled means. Prosecutors should consider whether to charge offences under RIPA instead of or in addition to CMA. RIPA would usually be used if material was unlawfully intercepted while its transmission; CMA would usually be used when material is acquired through unauthorised access to a computer.

Data Protection Act 1998

Section 55 of the Data Protection Act creates criminal offences that may be committed alongside cyber-dependent crimes.

These include:

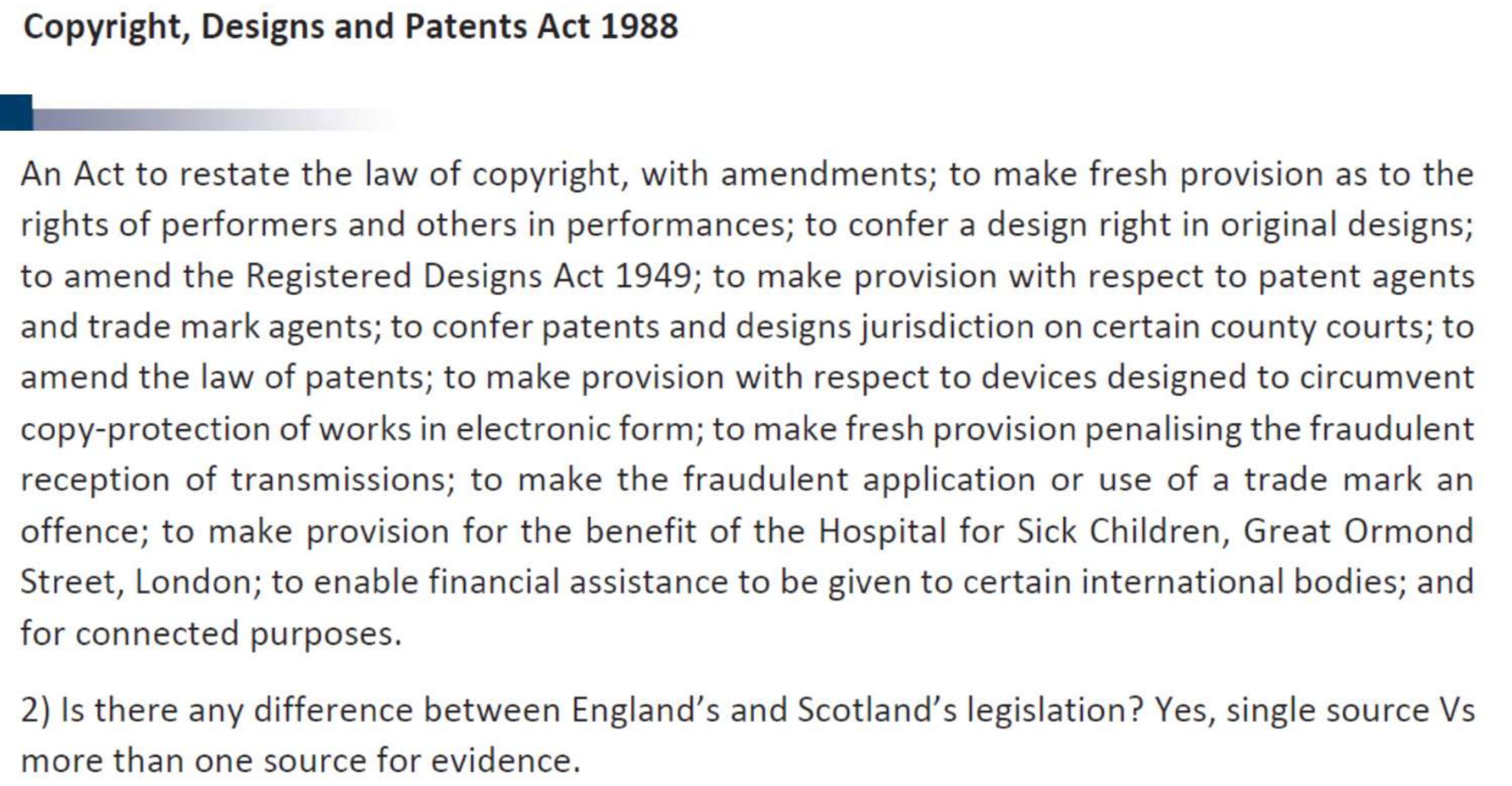
Obtaining or disclosing personal data

Procuring the disclosure of personal data

Selling or offering to sell personal data

For example, Trojans can appear as legitimate computer programs but facilitate illegal access to a computer to steal personal data without a user's knowledge.

Note 3/4



Copyright, Designs and Patents Act 1988

An Act to restate the law of copyright, with amendments; to make fresh provision as to the rights of performers and others in performances; to confer a design right in original designs; to amend the Registered Designs Act 1949; to make provision with respect to patent agents and trade mark agents; to confer patents and designs jurisdiction on certain county courts; to amend the law of patents; to make provision with respect to devices designed to circumvent copy-protection of works in electronic form; to make fresh provision penalising the fraudulent reception of transmissions; to make the fraudulent application or use of a trade mark an offence; to make provision for the benefit of the Hospital for Sick Children, Great Ormond Street, London; to enable financial assistance to be given to certain international bodies; and for connected purposes.

2) Is there any difference between England’s and Scotland’s legislation? Yes, single source Vs more than one source for evidence.

Note 4/4

3) What is a Trojan Defence? Can you guess?

The defence typically involves defendant denial of responsibility for (i) the presence of cyber contraband on the defendant's computer system; or (ii) commission of a cybercrime via the defendant's computer, on the basis that a malware (such as a Trojan horse, virus, worm, Internet bot or other program) or on some other perpetrator using such malware, was responsible for the commission of the offence in question.

A modified use of the defence involves a defendant charged with a non-cybercrime admitting that whilst technically speaking the defendant may be responsible for the commission of the offence, he or she lacked the necessary criminal intent or knowledge because of malware involvement.

4) What if someone used your wireless broadband for illegal activities? Can you prove you are innocent?

Imagine the police knocking on your door and you are innocent. In this case you can express your concerns and a strategy will be discussed for testing your WIFI coverage and investigate other possible suspects.

Summary

- Discussed different types of Digital Forensics

- Demonstrated the different steps in Computer Forensics

- Explained different techniques and tools for recovering evidence