



Mobile forensic analysis for smartphones



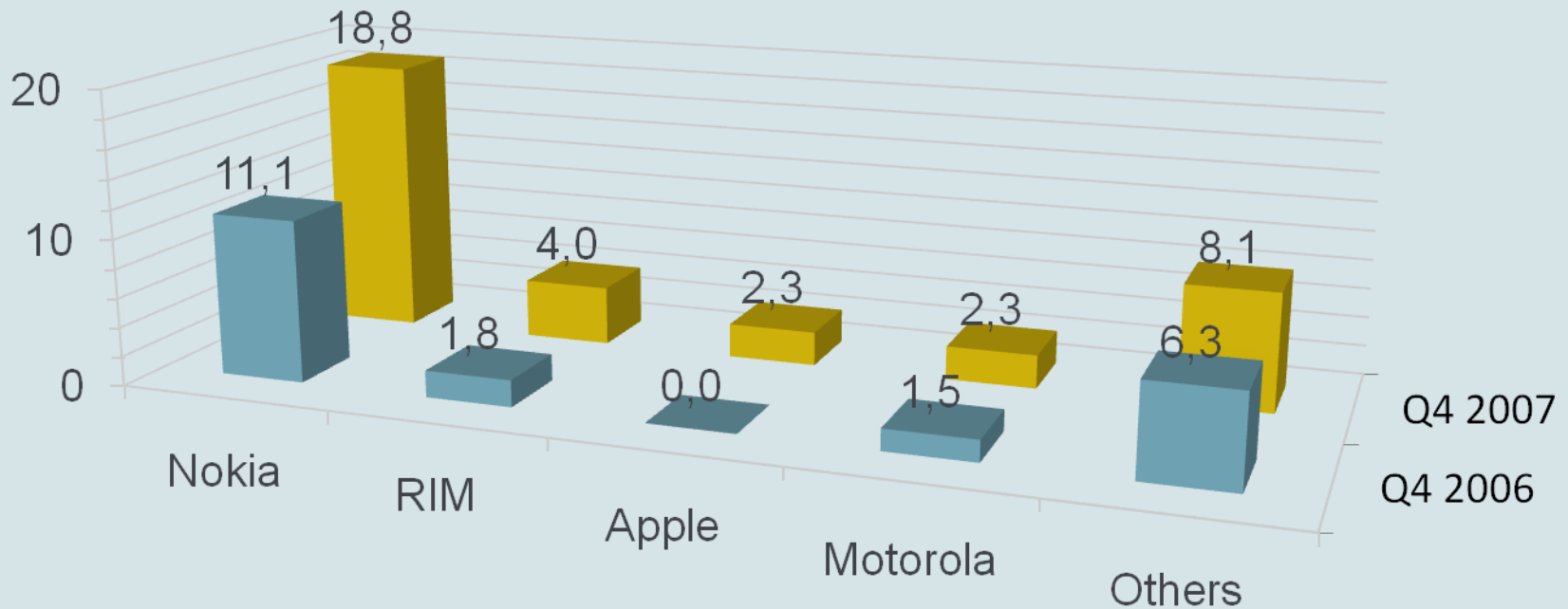
ISS World Europe 2008

Purposes of phone forensics

- ⦿ Extracting complete and unaltered information from cell phones, smartphones, PDA etc.
- ⦿ Analyzing extracted information and finding evidences.
- ⦿ Preparing forensic reports that can be presented in a court.
- ⦿ Proving data authenticity.

Smartphones market growth

Devices shipped, M
Total growth Q4 2006/2007 is 71.9%



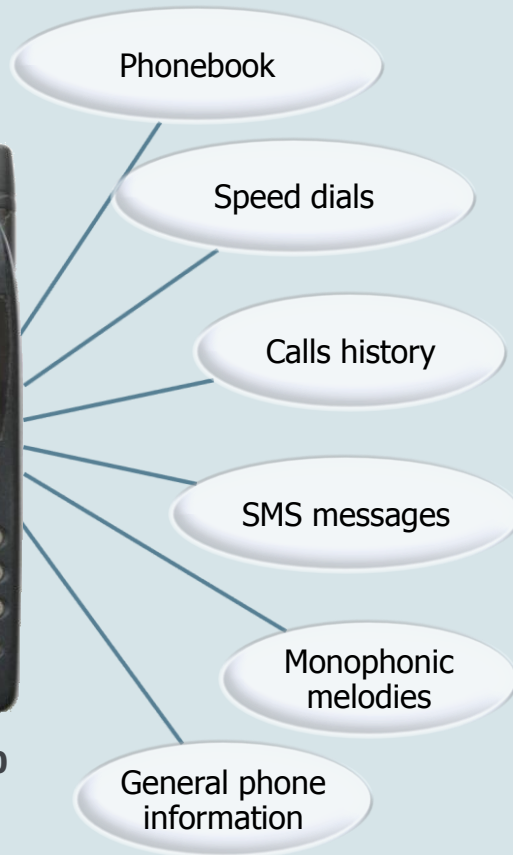
Source: Canals estimates , © canals.com ltd, 2008

Cell phones evolution

8 years ago



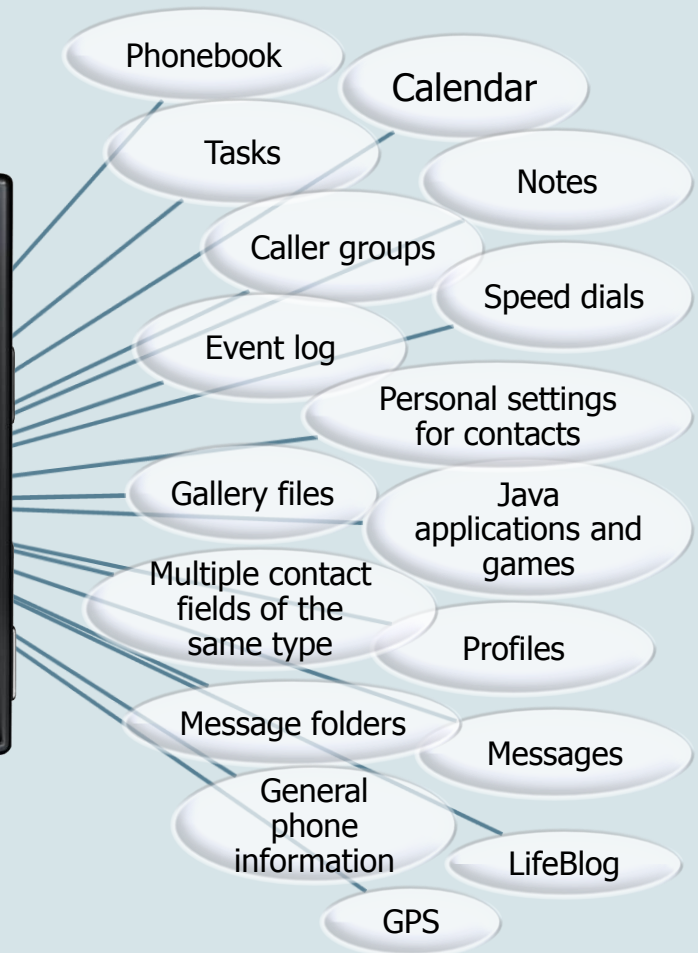
Nokia 5110



Nowadays



Modern smartphone



Communication protocols evolution



2000

AT+

- Contacts (simple), calls, SMS, files*, settings*
- Very slow
- Depends on implementation
- Developed for synchronization

Nokia FBUS

- Almost all information
- Undocumented
- Not for smartphones
- Depends on implementation
- Developed for synchronization

OBEX

- Contacts, calendar, files
- Depends on implementation
- Developed for files and objects exchange

SyncML

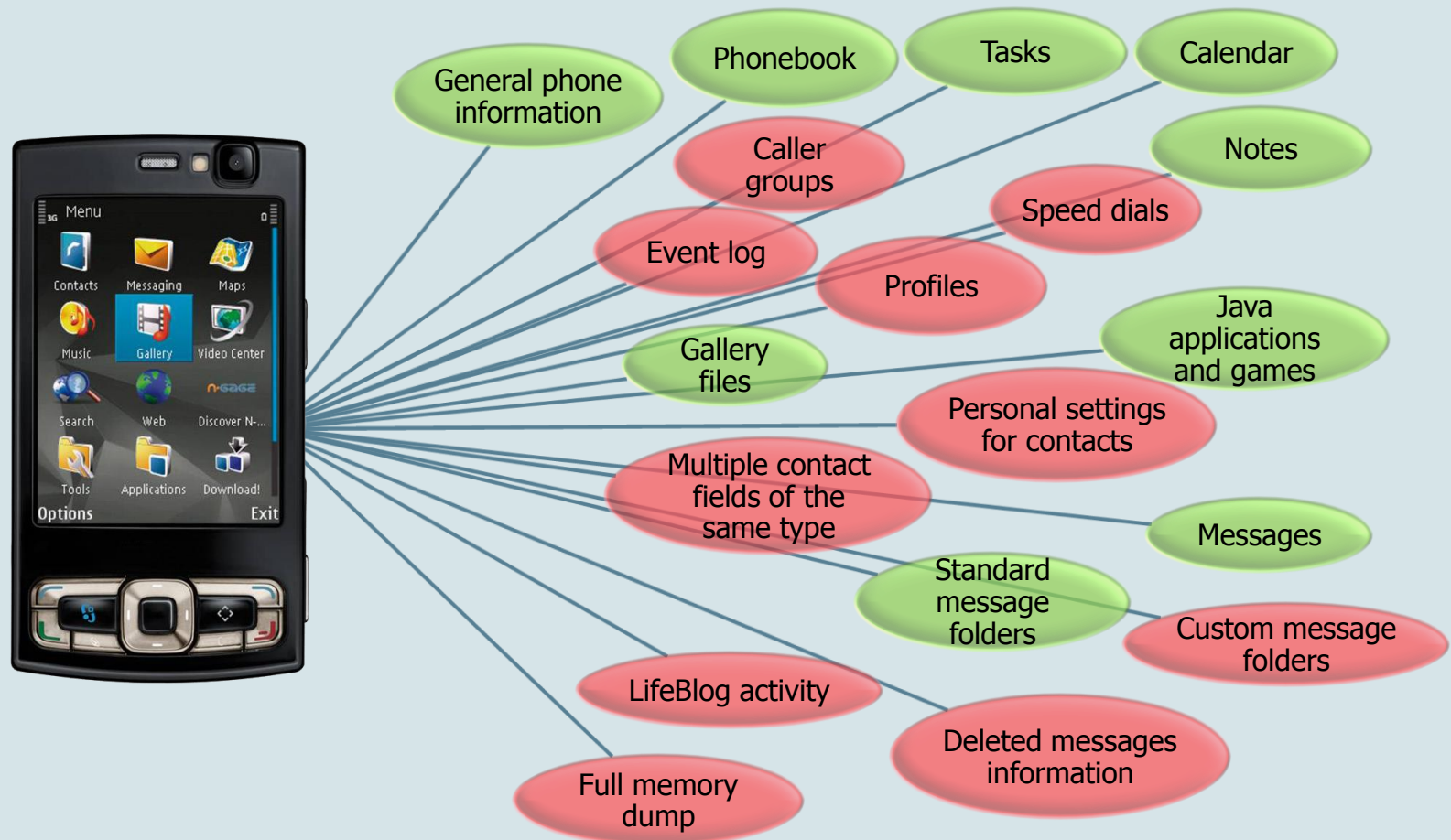
- Contacts, organizer, settings, messages*
- Developed for synchronization



2008

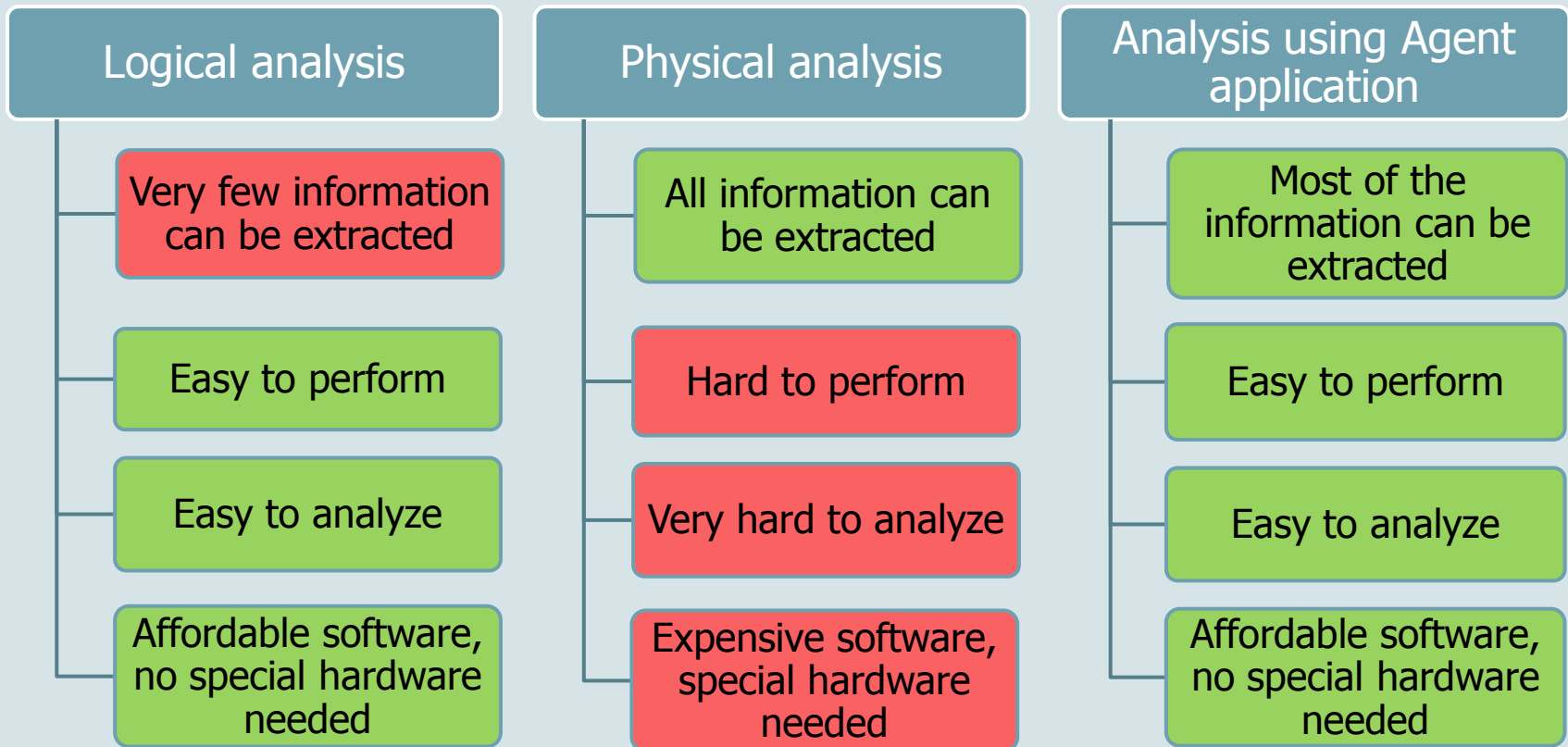
Smartphones and standard protocols

The striking discrepancy between data extracted by standard logical forensic tools and protocols and data which is stored in the devices and can be used for forensic investigations is quite obvious.



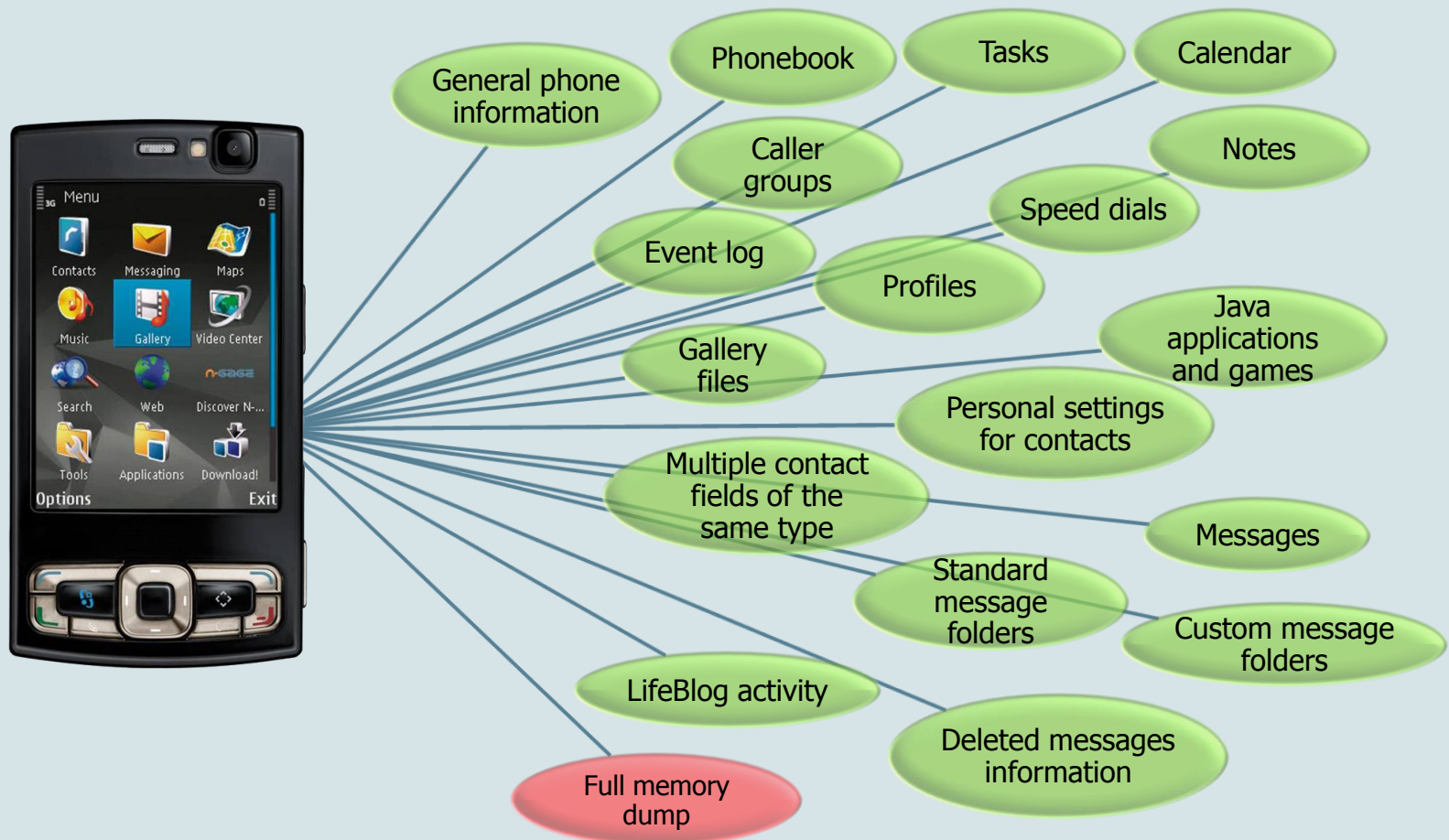
How to extract information?

There are 3 ways to get forensic information from smartphones: logical analysis, physical analysis and using a special agent application working inside smartphone OS



Agent application usage

We at Oxygen Software use an agent application approach. The Agent works inside a smartphone, has access to all device API's and implements custom communication protocol to extract almost all forensic information needed



Data authenticity and other concerns

Does putting agent into smartphone change its information?

No. Smartphones have different memory areas for data and applications.

Are there another way to extract full information from smartphones?

Yes, with restrictions – physical analysis.

What information can be extracted by agent application?

All the information available for native OS applications.

What information cannot be extracted by agent application?

Memory dumps and protected system files – usually this information scarcely useful for forensic analysis.

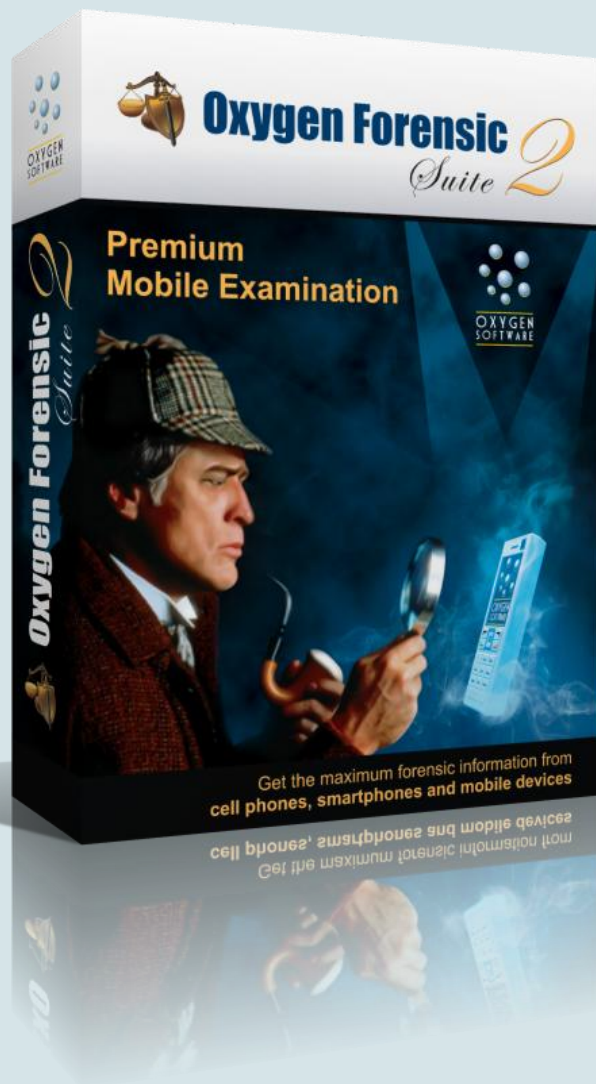
What are the main advantages of using agent application approach?

Extracting complete information and presenting it in a structured and easy to analyze way.
All this – using standard cables/adapters and with affordable price.

Is agent application able to read deleted information?

If this information is stored by operating system – yes. For example, Oxygen Forensic Suite reads information about SMS messages recently deleted from phone memory.

Interested in more details?



Oxygen Software
Feodosiyskaya st. 1, Moscow,
117216, Russia

Phones:

+1 (877) 9-OXYGEN (USA)

+44 020 8133 8450 (UK)

+7-495-222-9278 (Russia)

www.oxygensoftware.com

www.oxygen-forensic.com