OXYGEN FORENSICS

DOWNRANGE WITH OXYGEN FORENSIC® DETECTIVE

A problem-solving study with OFD in a conflict zone

TABLE OF CONTENTS

INTRODUCTION

To set the scene for this conversation:

In 2001, over 86 million cellphones existed in the United States. Today, there are over 300 million. In total, there are over five billion cell phone users in the world today. Americans use their mobile devices for nearly everything – serving as an extension of their person, often holding their most valuable information. This is no different for nefarious actors. Devices recovered from the battlefields of low intensity conflicts contain large quantities of targetable, actionable information.

The geography of this conversation is Afghanistan, and it provides its own unique challenges.

Early in the war on terror, technology was scarce. The path of least resistance to that problem was cell towers popping up and small villages becoming linked by cell phones. Afghanistan's population began using mobile phones heavily. Today in Afghanistan, almost all internet activity is conducted using cellular networks with very few, if any, internet service providers. This lack of infrastructure helped shape how Afghanistan became almost wholly dependent on mobile networks, mobile devices, and mobile applications. This translated to nefarious actors as well, who were forced to use mobile devices in all their activities.

This document discusses the pairing of a DoD digital forensic examiner and Oxygen Forensic® Detective, deployed in a forward operating location. This pairing successfully navigated the most common battlefield mobile forensic problems as a technology suite while other pairings required multiple procurements, additional workflows, more equipment, and several technologies.

BATTLEFIELD PROBLEMS

Small resources | Big problems:

The DOD is in a transition phase from the last 20 years of small wars to diverting resources to near peer competitors. Resources directed to the "small wars" and counter-insurgency efforts will continue but on tighter budgets and with less personnel.

With less resources to feed the targeting cycle, a technology is needed that does more with less overhead. Gone are the days of having teams of analysts who would enhance your digital forensics reports and review images, documents, messages, locations, and call data. Having one tool that can perform the work that once took 20 analysts is *key*.

Alternate device dominance:

No two objectives | targets bring the same device through the door.

For instance, any given objective may contain any combination of smartphones, feature phones, sim cards, drones, cameras, or even laptop or desktop computers. When items are recovered from the battlefield, you need a Swiss army knife not a hammer. Having a tool that can parse all these disparate devices and place them into one consolidated reviewing platform is key – especially when it comes to analytics.

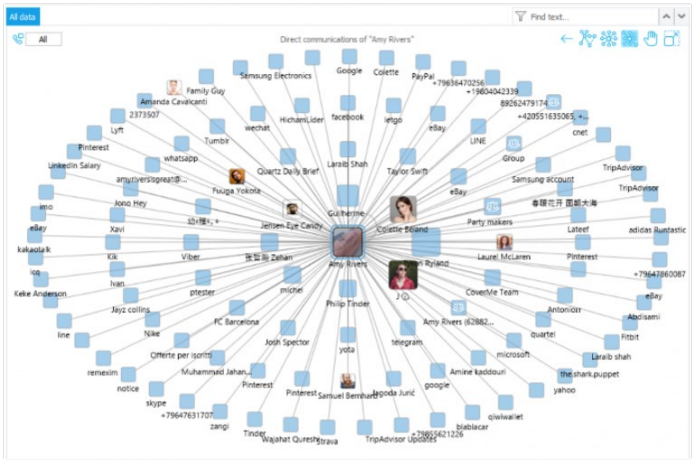
"Rolling comms"

Unlike traditional computer forensics where evidence may sit in a queue for weeks or months at a time and still prove valuable, battlefield forensics live and die in a matter of days or sometimes hours. Having the ability to get a strike force or platform to quickly target new objectives after they are identified during forensic analysis is critical. When nefarious actors are captured or taken off the battlefield, **there is no faster network** and associates will "roll comms" or get rid of mobile devices which had been used to communicate. Devices (phones and sim cards) are replaced, and often times quickly put back into alternate use to throw off pursuers.

OXYGEN FORENSIC® DETECTIVE SOLUTIONS

Oxygen Forensic® Detective is an all-in-one forensic software platform built to extract, decode, and analyze data from multiple digital sources: mobile and IoT devices, device backups, UICC and media cards, drones, and cloud services. Oxygen Forensic® Detective can also find and extract a vast range of artifacts, system files as well as credentials from Windows, macOS, and Linux machines.

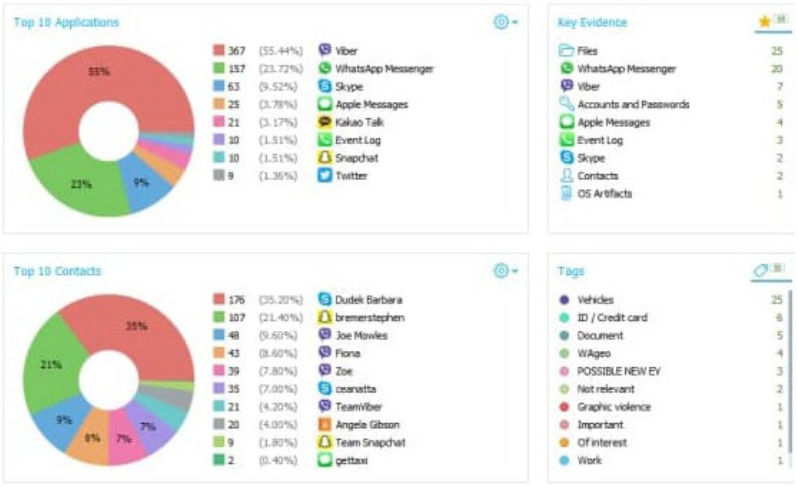
Furthermore, multiple extractions can be investigated in a single interface to gain a complete picture of the data. By using our integrated, industry-leading analytical tools to find social connections, build timelines, and categorize images, investigators from all over can help us in our mission to make this world a safer place.



Oxygen Forensic® Detective provided solutions in the following fashions:

Streamlining F3EAD to Analyze and Dissemination with Analytics:

When the small resource is tackling the big problem, Oxygen Forensic® Detective provides an all-inclusive package at an accessible price. It completes many of the tasks required in the F3EAD cycle with limited resources and analysts previously needed to bring objectives to conclusion. Additionally, as the one examiner for the investigation, when jumping from mobile devices to computers, including KeyScout technologies and review platforms for host-nation agencies allows quicker and more complete target analysis, preventing other time-sensitive problems.



Casting a wider net with one extraction technology

Devices recovered from the battlefield vary widely. Android devices are most common, but it is not unusual to be provided a variety of devices in addition to phones (drones/computers). With Oxygen Forensic® Detective, you can exploit multiple devices concurrently with ease. While the extraction of alternate devices is a key function of Oxygen Forensic® Detective, the commonality between their artifacts is where the technology and investigator combine forces to provide uniform data collection and easily understood data deliverables to the ultimate end customers.

Decreasing turnaround time

One of the most time sensitive problems occurs when actionable data is not acted upon in a timely fashion. When evidence becomes separated and disparate among investigators and tools, the clear picture can lose focus, or even be lost, allowing the enemy to throw curve balls by “rolling comms”.

Oxygen Forensic® Detective allows the investigator to apply laser focus to relationships, communications, applications used, time and geography involved including accounts and aliases to prove points faster than the bad actors can recognize and change.

Commanders now have faster, more accurate options with which to make decisions.

CONCLUSION

Exploiting data collected from the battlefield in a timely, forensically sound manner provides critical intelligence to commanders and stakeholders. Whether it be supporting precision fires, re-allocating Intelligence Surveillance Reconnaissance (ISR), or providing evidentiary data to host-nation forces to prosecute and adjudicate terrorist-related activity, it is essential that technology and examiners work quickly and accurately to circumvent some of those most common obstacles.

The technology is a commercial, off the shelf, all-in-one package, capable of exploiting mobile devices, drones, and when used in conjunction with KeyScout, personal computers. The power and ability of Oxygen Forensic® Detective force-multiplied with an experienced DoD digital forensic examiner is crucial to supporting ever-scaling mission parameters (personnel, funding, objectives).