



# Essential Online Tools for Phone Examiners

*Kevin Mansell, Control-F Ltd.  
Mobile Forensics World 2008, Chicago*



## Resources

# Essential ~~Online Tools~~ for Phone Examiners

*Kevin Mansell, Control-F Ltd.  
Mobile Forensics World 2008, Chicago*

# Overview

- About me and Control-F
- Essential websites
- Essential free software tools
- Wrap up



# Kevin Mansell & Control-F

- Kevin Mansell
  - 9 years experience in telecoms industry
  - 3 years as a high tech crime trainer at UK police training facility
    - Interpol
    - ACPO Good Practice Guide for Computer-Based Electronic Evidence
  - Founded Control-F in Jan 2007
  - Focussing on training and consultancy in digital forensics
  - Trained over 300 phone forensic examiners



# Before We Begin

- If you have:

1. A laptop with wireless Internet
2. A insatiable appetite for trying stuff out

then please join in

- If you don't, just feel free to watch me!

- The resources I mention are personal recommendations. Yours may differ - I'd love to hear about them!



# Essential Websites

# Scenario 1

*“I’ve never seen this handset before. I have no idea what it is, or what it’s capable of. I need to find out fast”*



[www.gsmarena.com](http://www.gsmarena.com)

[www.mobileforensicscentral.com](http://www.mobileforensicscentral.com)

# Scenario 2

*“I’ve retrieved an IMEI (handset serial #)  
and an ICCID (SIM serial #). I want to  
check them out”*

[www.numberingplans.com](http://www.numberingplans.com)

- Great for:
  - SIMs with no branding
  - Identifying obscure handsets



# Scenario 3

*“I’m going to be giving evidence in court tomorrow and I can’t remember what SIM stands for!”*

[www.wikipedia.org](http://www.wikipedia.org)

“define:” with [www.google.com](http://www.google.com)

also “site:” and “filetype:”

# Scenario 4

*“I’m banging my head  
against a brick wall  
trying to get anything  
from this Nokia 1112.  
What else can I try?”*



[www.phone-forensics.com](http://www.phone-forensics.com)

# Scenario 5

“My handset download has extracted a bunch of .IMY files. What the heck are they and how can I view/play them?”



<http://filext.com>

[www.download.com](http://www.download.com)

# Scenario 6

*“How on earth am I supposed to keep up to date with this insanely fast-paced industry?!”*

[www.theregister.com/comms/mobile](http://www.theregister.com/comms/mobile)

**The  Register®**

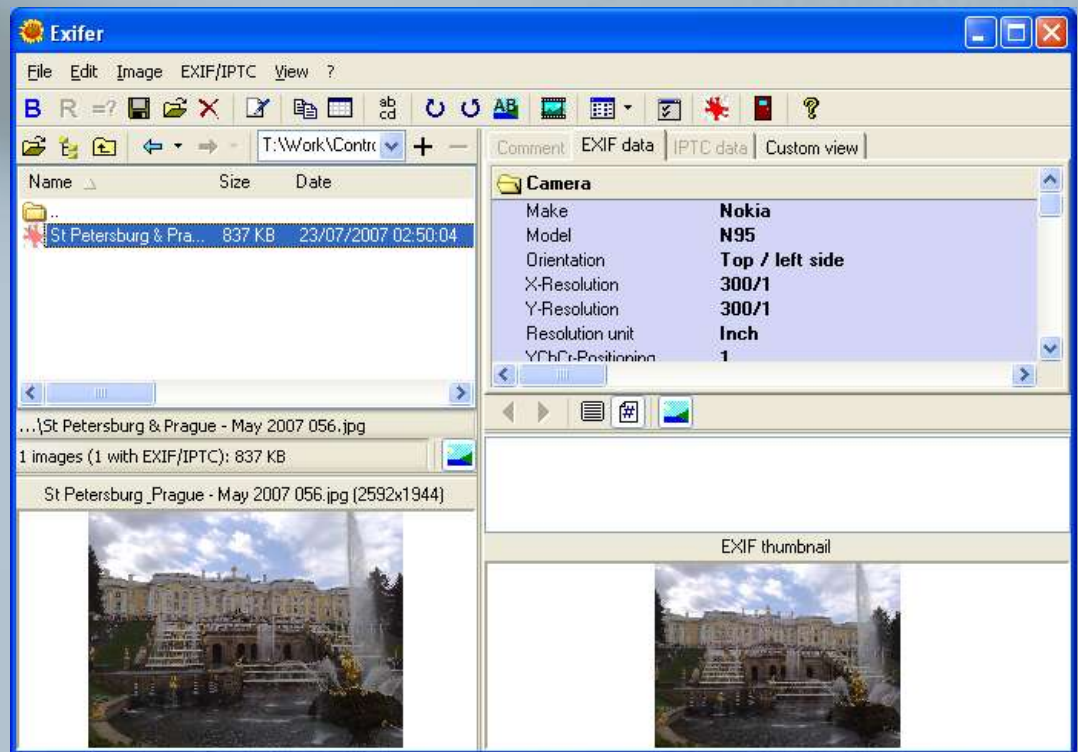


# Essential (Free!) Software Tools

# Scenario 7

*“I’ve extracted a pile JPG files from a handset and want to check if any of them have any EXIF metadata”*

*Exifer*



# Scenario 8

*“I’ve extracted a video file from this handset but I can’t seem to view it. Maybe it’s corrupted. What should I try?”*



*QuickTime Player*



*RealPlayer*



*VLC Media Player*

# Scenario 9

*“I’ve downloaded an SYN file from a handset. I can’t find anything to view/play it. Notepad doesn’t really work. How can I view the contents of the file?”*

PSPad

```
00000000 0000 001C 6674 7970 3367 7034 0000 0400 [...]...ftyp3gp4....
00000010 3367 7034 3367 3261 6973 6F6D 0001 2D78 3gp43g2aisom..-x
00000020 6D64 6174 0000 8002 080A 1CF3 F251 D060 mdat..€.....óòQÐ`
00000030 03C4 A5AC 4947 27EA 4181 102E 63EA E20A .Ã¥-IG'éA]..céá.
00000040 2E65 8F88 7BF8 4DE8 097C 9E0A 2847 COCO .e|^(øMè.|ž.(GÀÀ
00000050 06F8 7CA6 E8F6 E738 6ADC 218F A88D 3B4F .ø||èöç8jÛ![];O
00000060 2E7B AF8F 7BF5 9401 A4F8 5B1D AF3C 077C .([] (õ".æø[.~<.|
00000070 0E40 153C 0600 3681 CDBD 87A8 8181 0D1D .@.<...6[] Í*#>[]..
00000080 CAAS A245 2521 94A9 D5E4 97C1 1818 7FD5 Ê¥øE*!"@õä-Á..[]õ
00000090 60E5 FF64 5831 97A0 1C8C CDE0 FD52 B55C `ãÿdX1- .@íàÿR\
```

# Wrap Up

- There are some great websites and free software tools out there
- They will save you time and make you a more effective examiner
- Tell me about ones you love!

# Thank you

Kevin Mansell

[kevin.mansell@controlf.net](mailto:kevin.mansell@controlf.net)

+44 (0)7749 886450

[www.controlf.net](http://www.controlf.net)