

Commercial Fraud Lawyers Association – 14 September 2017

Search Orders-from 3 perspectives

⋮ Dipti Hunter-PwC

⋮ Jane Colston-Brown Rudnick

Phil Beckett-Alvarez & Marsal

BROWNRUDNICK.COM

The Speakers



Dipti Hunter
Senior Manager



Jane Colston
Partner



Phil Beckett
Managing Director



Search orders: recap

1. What premises may be searched?
2. When do I apply?
3. What do I need to apply?

Search orders: recap

1. Does the Claimant have a substantive strong prima facie case?
2. Has there been serious damage caused to the Claimant?
3. Is there clear evidence that the Defendant has relevant material?
4. Is there a real risk that the Defendant will destroy that material?

YES = Sufficient grounds to obtain a Search Order

Search orders: recap

What do I need to apply?

1. Application Notice
2. Draft (standard) Search Order
3. Draft/issued Claim Form
4. Draft/Sworn Affidavit
5. Skeleton argument

The hearing

1. Full and Frank e.g. Claimant's financial standing
2. Take a full note of what is said and promptly serve on the Defendant (*Interoute Telecommunications (UK) Ltd v Fashion Gossip Ltd (1999)*
 - Consider using a court shorthand writer to do the note

Drafting a Search Order



NOTE: The Order should be drafted by somebody with extensive experience of Search Orders

1

- Penal Notice

2

- Comprehensive list of items and hard copy documents that you are expecting to find

3

- Balance should be struck between a list that is:
 - Too broad (and creates a “fishing expedition” impression) OR
 - Too narrow (and does not give the Claimant access to all the evidence it requires)

4

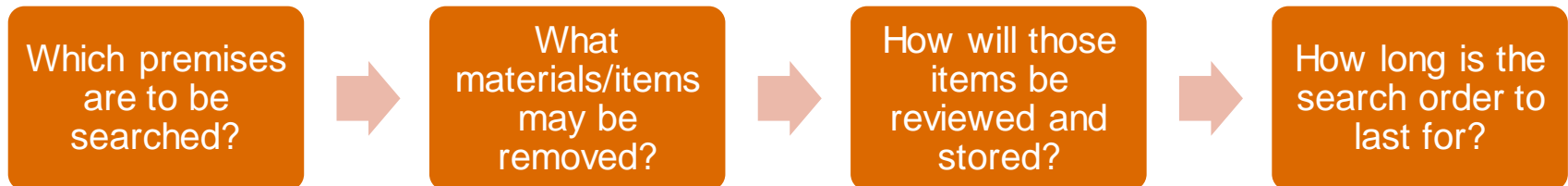
- Practical and easy for third parties to understand

Drafting a Search Order



Be pragmatic, not dogmatic AND utilise your resource wisely

The execution of the Order should be described in detail to assure the Court that the Defendant will not suffer any undue oppression and to show that it is correctly targeted




Don't forget: Privilege against self-incrimination

Instructing third parties and logistics

- Instruct barristers, corporate intelligence experts, and IT experts with appropriate civil litigation experience
- Ensure that Defendant's data or IT hardware is not damaged or destroyed
- Urgency of application leaves little time to brief the wider search team, but important you do take time to have a call and take on board their perspectives
- Choose experienced third parties
- Undertakings will have to be provided to the Court




Benefit of hindsight – preparing for the search day

- 
- Get location(s) right (and in the Sealed Order) and know where your Respondents' movements are on the chosen day
 - Have a team at the office to deal with logistics as well as at the search sites
 - Make sure Defendant is going to be at one of the sites when you intend to serve
 - Be prepared for what is behind the door e.g. children, animals, guns etc.
 - Take copies of all the bundles to be served and have scans ready to email, back at the office
 - Have copies of the practicing certificates of the solicitor members of the search party
 - Prepare extracts of the Law Society's or SRA's website proving the independence of the Supervising Solicitor

Benefit of hindsight – preparing for the search day

When preparing for the search day, you also want to consider taking with you:

- 
- A list of contact details of local solicitors with relevant experience for the Defendant
 - A prepared letter to the Defendant explaining the Search Order, which can then be annexed to the Supervising Solicitor's report to the Court
 - Carbon paper, evidence boxes/bags, digital voice recorder, Wi-Fi, camera, USB memory sticks, post-it notes, marker pens, mobile chargers, folders etc.
 - A skeleton of the Supervising Solicitor's report to the Court in soft copy, which the Supervising Solicitor can update or progress during the course of the search
 - Food, drink, protective clothing and rubber gloves

Post Settlement/Final Court Order

- Destruction of data or retention of data
- Be mindful of the hazards of data retention
- Criminal Production Order...



On the day

1. Be vigilant
2. Don't let the Defendant touch his/her computer
3. Expect the unexpected
4. Sometimes you need luck but also you make your own luck
 - The careful listening
 - The chance remarks
 - People under pressure doing foolish things or wanting to explain or unburden themselves

The Defendant's first response

1. The Defendant has a right to apply immediately to vary or discharge the Order
2. This is difficult to do
3. If the Defendant decides not to make an immediate application he/she can wait until the return date

Defendant's solicitor's first response

1. Seek Order, hearing note, affidavit & skeleton
2. With the client, assess whether there are any clear grounds to discharge the Order
3. In most cases seeking a discharge of the Order is unrealistic & the Order must be complied with
4. Identify privileged data (both in regard to incriminating and legal professional privilege) and segregate
5. Take full notes - perhaps photographs - of the search

Defendant's solicitor during execution

1. Ensure Order is executed professionally & doesn't stray beyond the terms of the Order
2. Seized items may include:
 - i. Documents
 - ii. Computer records and files
 - iii. Chattels specified in the Order
3. But not:
 - i. Privileged material
 - ii. Materials and stock-in-trade used in lawful business
 - iii. Clothes, bedding, and usually, furnishings

- 1. No material may be removed from the Defendant's premises:**
 - Unless it is "clearly" covered by the terms of the Order
 - Except in the presence of the Defendant
 - Before it is listed and the list checked by the Defendant. A copy of the list should be given to the Defendant
- 2. Material the Supervising Solicitor decides is not covered by the Order or is privileged, will be excluded, listed & returned**

If doubt, the Supervising Solicitor will retain

Defendant's solicitor during execution

- Be present when your client is being questioned by the Claimants e.g. in regard to the disclosure sought by the Order
- Take a careful record of what is said
- Ensure questions do not stray beyond the terms of the Order and into, in essence, a deposition

Defendant's solicitors

1. Stress the need for truthful answers in responding to search orders
 - i. If the Defendant wilfully disobeys the Order, this will constitute contempt of court
 - ii. The court will imprison and strike out defences
2. But don't volunteer what is not ordered
 - i. Time pressure leads to mistakes

Defendant's solicitors-Post execution

- Laser focus in choosing battles
- Practically, it is difficult to discharge Search Orders
 - The Risk is high - almost inevitable - of losing given the low thresholds and the Courts' reluctance to prejudice the action early on
- Resist being bullied into providing, in effect, early witness statements when giving the ordered disclosure or to support an application to set aside the injunction

Defendant's solicitors

1. Primary counter attack-failure to be full and frank
2. General rule, unlawfully obtained evidence admissible
3. *St Merryn Meat*
 - evidence of the Defendant's fraud was obtained through bugging home telephone. The injunction was discharged
4. *Dubai Aluminium Limited v Al Alawi*
 - breach of the DPA and Swiss Banking Law. Court ordered disclosure of the investigation reports

Defendant's solicitors

1. Seeking to utilize unlawfully sourced material brings risks outside the civil courtroom, including criminal, reputational and disciplinary risks for the lawyers
2. Even if a Search Order has been fully executed, it can still be worth seeking its discharge if it is established that the Order should not have been made:
 - Damages can be awarded
 - Indemnity costs
 - Return of the seized material
 - Discharge of those parts of the Order that still require compliance e.g. the provision of information on Affidavit

Range of devices



Some of which need some consideration...

...on how to locate them and what to do with them



Network attached storage: small, WIFI only connection, can be located anywhere

Memory cards: small, versatile and can “hide” in a variety of places and devices



Smartphones: unlike laptops and computers, not every smartphone is made equal in terms of components and connectivity. Therefore, there is always a “battle” to gain forensic access to new devices, so be aware that workarounds may be needed

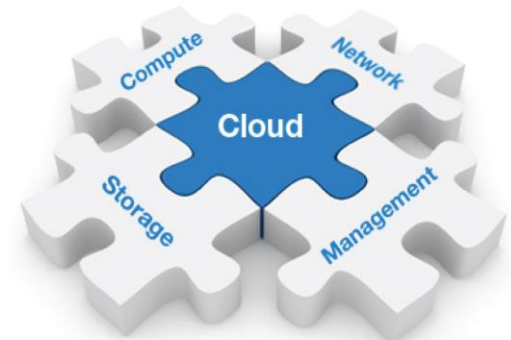
Not just about devices...

...”services” are just as important



Webmail: used prolifically by individuals, especially when behaving ‘badly’, what can be salvaged?

Cloud services for a business: how do they use technology, where is the data, how accessible is it, is there an impact for the Order?



Cloud services for individuals: can be used to transfer large amounts of data that can be accessed from anywhere

Social media accounts: can provide details of contacts, activities and communications



Before the execution of the Order

Key pointers from a technology perspective

- **Wording of the order:** ensuring it covers the appropriate devices and services, as well as means of access (including account names, log-on details and authorisations to third parties).
- **Forewarned is forearmed:** knowing as much detail as possible enables us to be fully prepared, having the right people, equipment and back-up to execute effectively.
- **Imaging takes time:** capturing the data is not a quick process and as devices contain more and more storage they take longer to capture...therefore plan ahead, ensuring that “truly personal” and “priority” devices are started asap, whereas others can be done overnight etc.
- **Taking equipment away:** ensuring that the order allows for certain devices to be removed, imaged over-night/next day and returned, rather than everything being done there and then.
- **What can be done off-site:** allow for the possibility of anything that can be remotely accessed to be done so from the office as opposed to the physical site.
- **Limitations:** ensure that there are none, or appropriate limitations on what can and can't be done with the data subsequent to the execution – do not restrict to certain keywords for example.

During the execution of the Order

Key pointers from a technology perspective

- **Things are never as you think:** no matter how well planned a project is, you will always hit the unexpected, so be prepared to adapt and make sure that all parties are aware.
- **Forensic principles:** ensure that appropriate forensic principles are followed throughout to ensure admissibility and the ability to extract, process and review data going forward.
- **People lie:** they will try and hide things or lie by omission, so be on the lookout and be aware. Have the technology person present when going round the premises and not stuck in a backroom.
- **People get upset:** when dealing with their data, people can get very “touchy” about what we have access to, therefore it is important to be able to explain the safeguards upfront and explain exactly what will happen.
- **Passwords:** ensure that any passwords that are provided are verified and changed as soon as possible to (a) avoid any remote actions being taken on the data; and (b) respondents often have a habit of making ‘mistakes’ when providing passwords initially.

After the execution of the Order

Key pointers from a technology perspective

- **Immediate actions:** include the preparation of witness statements, backups, return of any equipment and provision of all data to supervising solicitor
- **It doesn't work anymore:** be prepared for the false accusations of damaged or broken equipment, ensuring that machines are verified as being operational before being returned and that photos are taken
- **So what now?**



Reviewing the evidence

From a practical and not legal perspective

Dual track approach because although the “files” are interesting, they are not **everything!**



Document review

- Requirement for a document review system
- Review process
- Consideration of filters and keywords
- Use of Technology Assisted Review

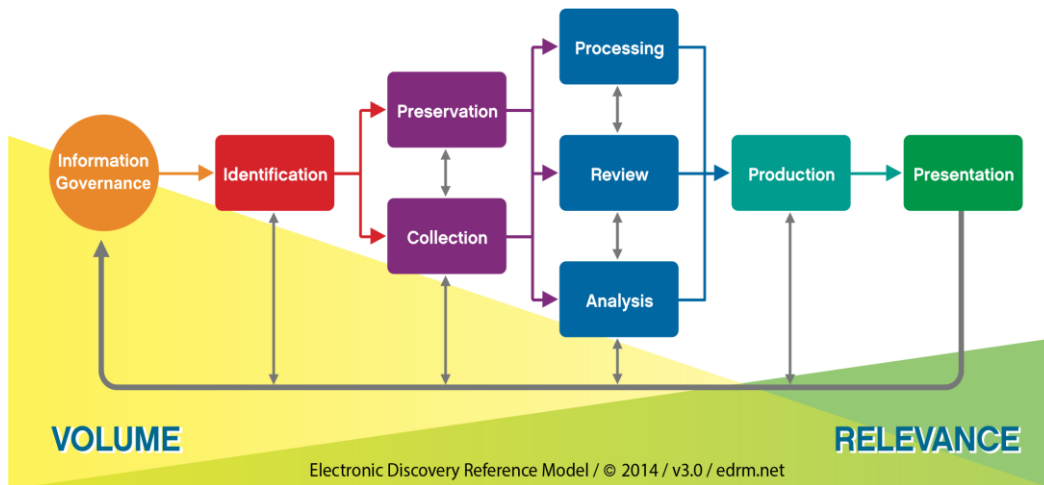
Forensic review

- Deleted data
- Web-based data
- USB activity
- Smartphone related data

Document review

How do you review millions of documents efficiently and effectively?

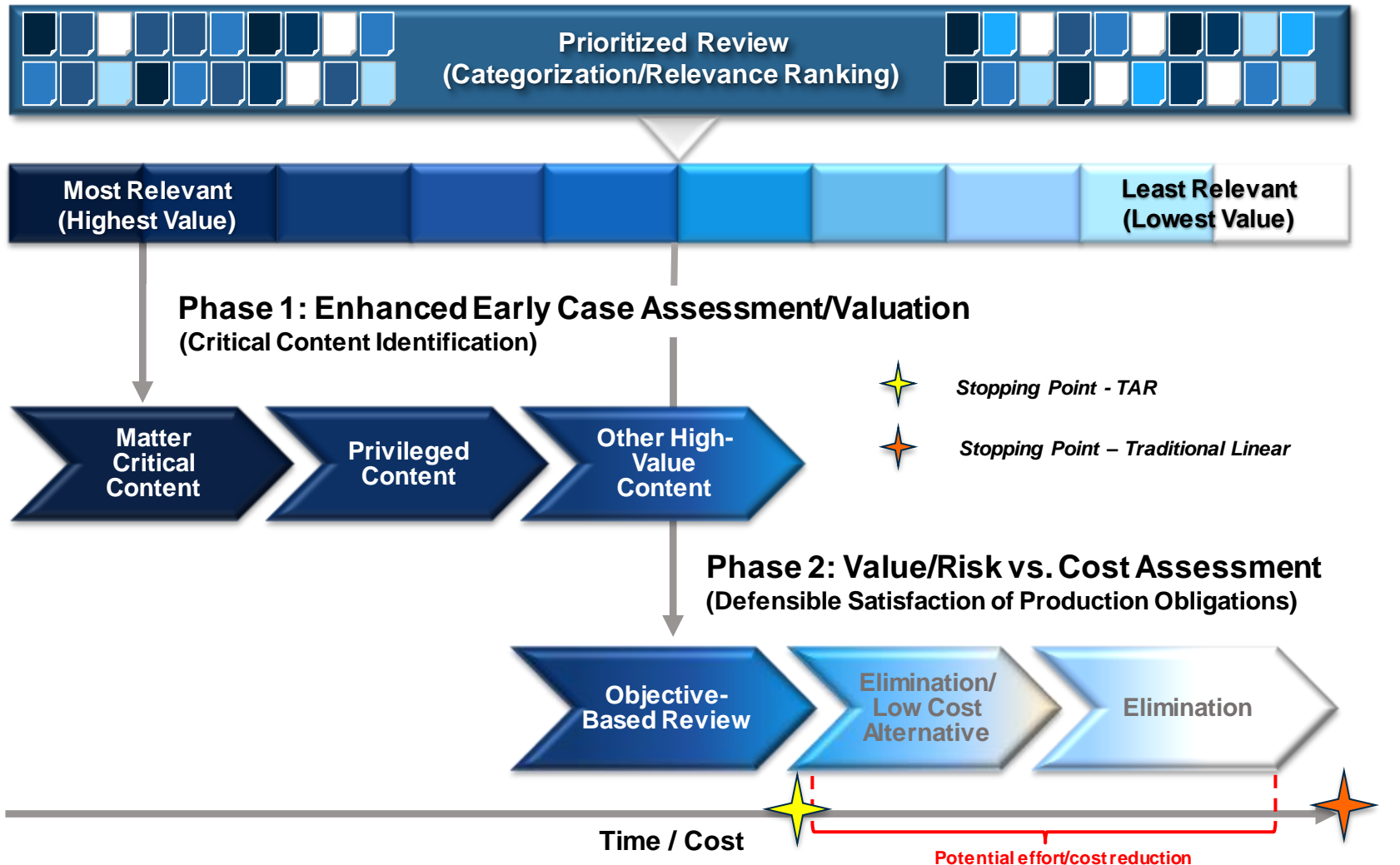
Electronic Discovery Reference Model



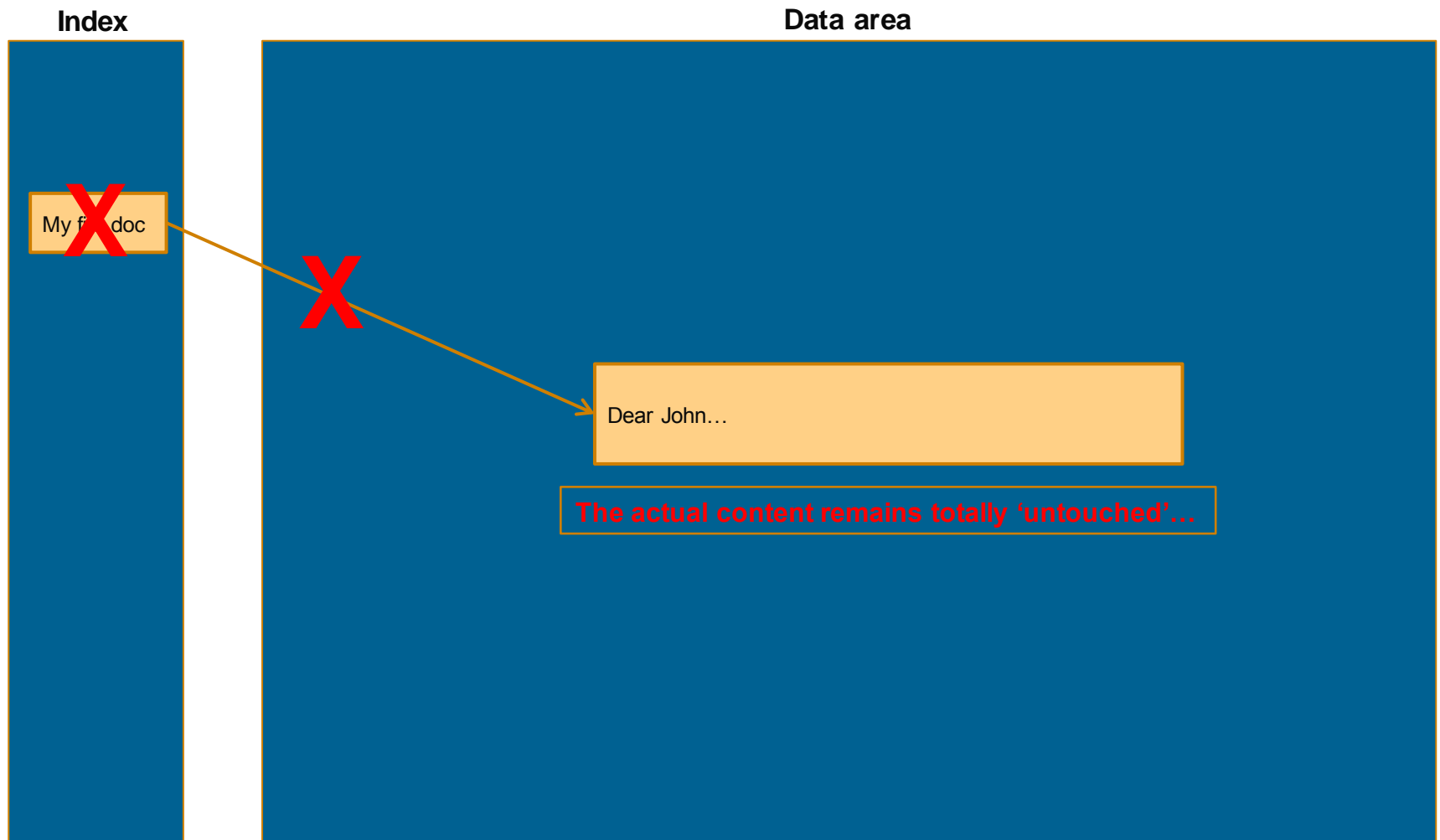
Some indicative pointers on timing and costs:

- It will generally take 1-3 days to get all data extracted from the images, processed and loaded into a review tool (depending on volume) although priority data can be loaded within a day
- Generally we see 10-20GB of data being extracted from a typical PC/laptop: 50-150,000 documents
- Costs will vary greatly especially if economies of scale can be achieved, one recent case we worked on where there were >30 devices and >450GB of data, cost in the region of £15-20k

Document Review: Technology Assisted Review



Forensic review: recovery of deleted data & wiping tools



Forensic review: analysing Internet activity

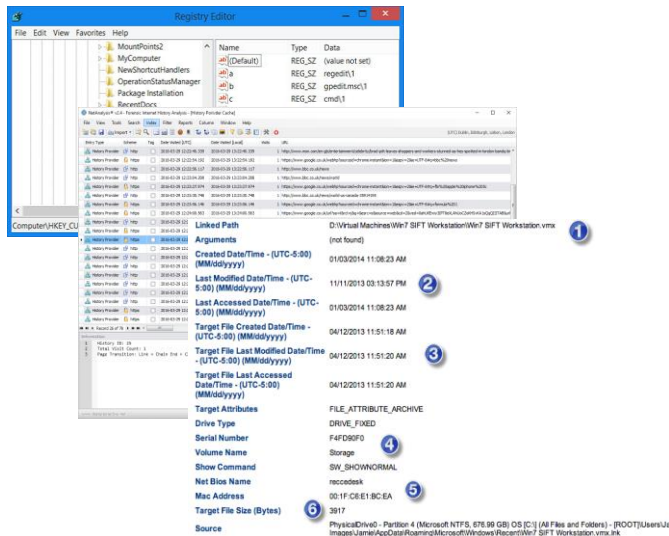


Forensic review: USB activity

Often easy to establish what devices were attached and when, less easy to identify what happened on them!



When a device is attached to a computer, there is an initial “handshake” whereby the computer recognises the device...leading to various pieces of information being stored – including make, model, serial number



Various system artefacts can trace activity on the USB devices, for example: MRU lists, Shellbags, Internet History and LNK files

Forensic review: smartphone related data

Access to more than you think...

- Normal office and email-related data...
- ...but with potentially personal accounts?



- Phone-related evidence (call logs, contacts etc)
- Application databases
- Chat applications
- Backups
- The Cloud...



The Speakers



Dipti Hunter
Senior Manager



Jane Colston
Partner



Phil Beckett
Managing Director

