Legal & Regulatory Requirements

Dr Syed Naqvi

syed.naqvi@bcu.ac.uk

Outline

- Introduction
- Legal framework
- National, European & International laws
- Privacy concerns
- Best practices
- Exercise: Example case

Introduction

- Jurisdiction of case
  - Legal boundaries
  - Non-disclosure agreement
- Search and seizure of digital evidence
  - Search warrants
  - Chain of custody
- Protection of digital evidence
  - Data protection
  - Contents/equipment protection

BIRMINGHAM CITY University

Introduction

- Processing of digital evidence
  - Integrity of the evidence
  - Interpretation of the findings
- Privacy assurances
  - Traces of different aspects of custodian's life
  - Protection from non-intended use of data
- Ethics and civil liberties
  - Principle of Innocence
  - Fundamental freedoms

Legal framework

- UK Legal jurisdictions
  - England & Wales
  - Scotland
  - Northern Ireland
- The basic principles are very similar but the actual law and nomenclature varies.
- Court procedure is **adversarial** as opposed to **inquisitorial**

Legal framework

- CPS (Crown Prosecution Service) formulate the precise charges
  - Investigations by law enforcement officers
- Crown Court
  - Judge: To chair the proceedings & rule on points of law
  - Jury: To decide matters of fact
  - Counsels: Both prosecution and the defendant(s) have their own counsels/barristers
- Magistrates' Court: Less serious cases; no jury

European Regulations

- Directives
  - Legislations by each member state
- Coordination of member states
  - No enforcement power
  - Referral service
  - Information sharing protocols
- Europol EC3 (European Cyber Crime Centre)
- Eurojust: Judicial cooperation in criminal matters

International conventions

- UNO charter & its agencies
  - Facilitate the functioning of public bodies & NGOs
  - Gathers political support for joint actions
- Interpol
  - Intergovernmental organization facilitating international police cooperation
- The International Court of Justice (ICJ)
  - Peaceful settlement of inter-State disputes

Privacy concerns

- European Directives
  - 95/46/EC
  - 2002/58/EC
- UK Data Protection Act 1998
  - Covers: Ethnic background, political opinions, religious beliefs, health, sexual health, criminal records
- US HIPPA (Health Insurance Portability and Accountability Act) Act 1996

Privacy concerns

- Personal privacy
  - Unrelated data to the investigations
  - Exceptions: E.g. Child pornography
- Organisational privacy
  - Commercial secrets
  - Reputation
  - Non-disclosure agreement (NDA)
  - Exceptions: E.g. Public safety

Best practices

- Legal and practical guidelines for digital forensics practitioners
  - Need to be adapted for changes in legislation, technology, practices, etc.
- ACPO Good Practice Guide for Digital Evidence
- Organisational guidelines for Digital Investigations
  - Adapted to specific nature of investigations
  - Provided in the company's working language

Best practices

- In general
  - Work with the legal experts (joint teams)
  - Document all the events (**log book**)
  - Awareness of data ownership and protection clauses
  - Be organised and maintain an inventory of resources
  - Follow the principle of “least privilege”
  - Avoid piling up unnecessary material in your work area (clean desk policy)
  - Avoid work related discussions in public places, during socialising, etc.
  - Clarify grey areas with domain experts

BIRMINGHAM CITY University

Case Example: Print Spooler Files

Print spooler evidence was the only evidence in a counterfeiting case in Orange County, California.

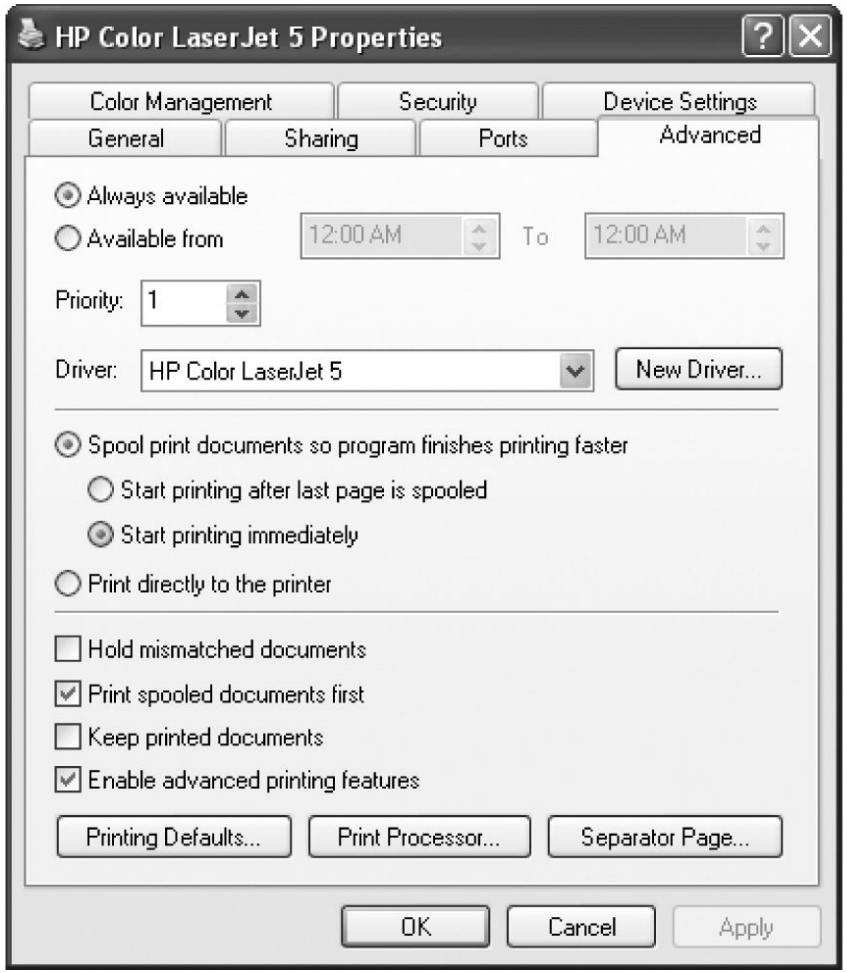
Department of Consumer Affairs examiners arrested a suspect for selling counterfeit state license certificates and seized his computer.

Although the examiner had seized some of the counterfeit certificates from victims, they were unable to locate evidence on the computer.

When the examiner requested a second view from the California Department of Insurance, Fraud Division, the Computer Forensic Team identified several deleted enhanced metafiles that exactly matched the paper copies that had been seized during the investigation.

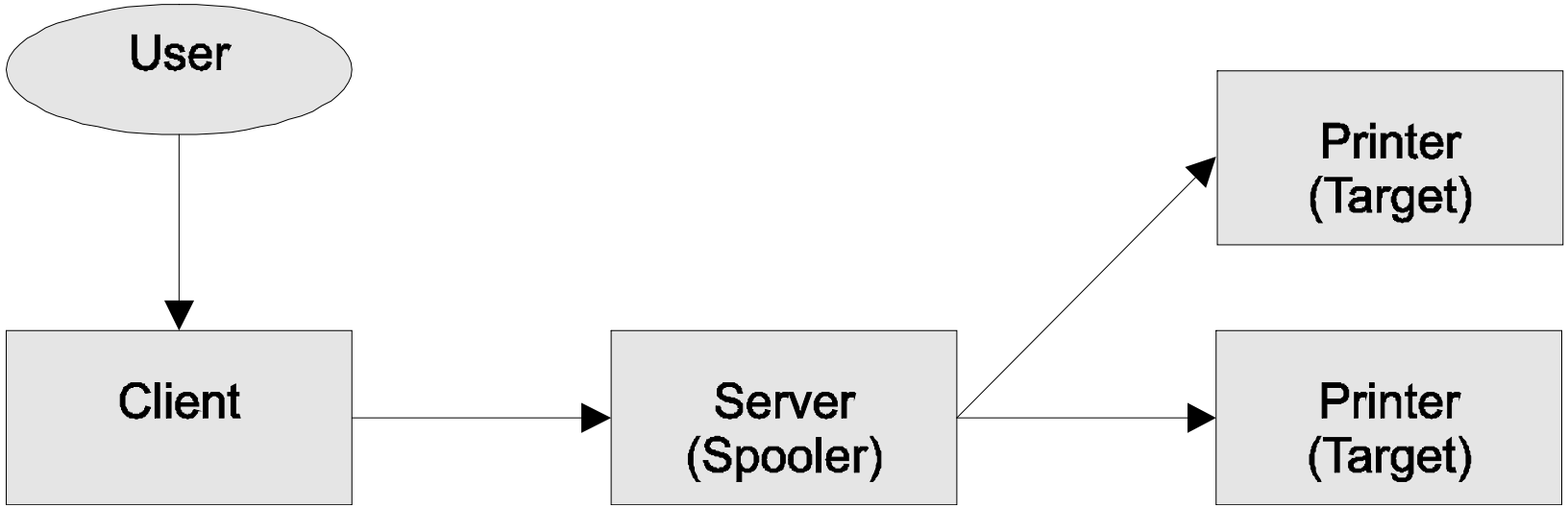
The only evidence present on the drive was the enhanced metafiles. The defendant was convicted at trial.

Printer Properties



BIRMINGHAM CITY University

Print Spooler Basics



BIRMINGHAM CITY University

Printing

- Printing involves a spooling process whereby the sending of data to a printer is delayed
  - The delay allows the application program to continue to be responsive to the user
  - The printing takes place in the background
- Print spooling is accomplished by creating temporary files that contain both the data to be printed and sufficient information to complete the print job

BIRMINGHAM CITY University

Print Spooler Files

- Files with extensions .SPL and .SHD are created for each job
  - .SHD file is a ‘shadow’ file that contains information about the print job including owner, the printer, the name of the file printed and the printing method (EMF or RAW)
    - EMF: Enhanced Meta File
    - RAW: Simple text based printing
  - In RAW format, the .SPL file contains the data to be printed
  - In EMF format, the .SPL file contains the name of the file printed, the method and a list of files that contain the data to be printed
  - .SHD, .SPL files are deleted after the print job completes

Print Spooler Files

- In Windows, the spool files are kept in

  C:\Windows\System32\spool\Printers

- The .SPL and .SHD files contain the name of the file to be printed including its fully qualified path
  - The path may suggest that other media containing evidence exist
  - .SPL - The print job's spooled data is contained in a spool file.
  - .SHD - The shadow file contains the job settings

Print Spooler Files – Forensics

- If the original file that the user printed does not exist on the seized evidence, the file may be found in enhanced metafile format

- While in Hex view, locate the letters “EMF” in the right part of view pane
  - Starting from the byte just prior to “E” select 41 bytes backwards
  - Right-click on the highlighted area and view it as a picture