

CS 798: Digital Forensics and Incident Response

Lecture 2 - Legal Framework

Diogo Barradas

Winter 2025

University of Waterloo

- **Digital Forensics:**
 - Branch of forensic science concerned with the proper acquisition, preservation and analysis of digital evidence, typically **after** an unauthorized access or use has taken place.

Ensuring evidence admissibility

- Ideally, digital investigators wish that the evidence they handle can help unfolding a case in court.
- However, the courts can reject evidence! We're going to find out why.

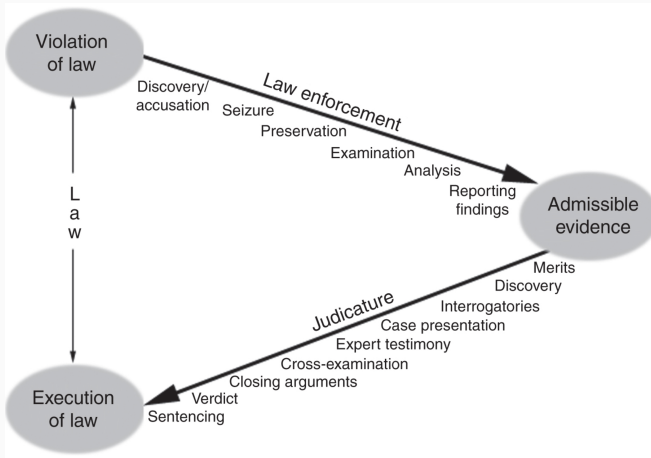


1. Digital Evidence and Law
2. Cybercrime Law
3. Digital Crime Scene
4. Admissibility of digital evidence
5. The Case of the Stolen Exams¹

¹The Open University: <https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3>

Digital Evidence and Law

Investigators operate within a legal framework



from: Digital Evidence and Computer Crime, Eoghan Casey

Ontario Superior Court of Justice – Court File No. 116/16



- **Court File No.:** 116/16
- **Citation:** R. v. J.B., 2018 ONSC 4726
- **Date:** 2018-08-03
- **Descriptors:** Criminal law; Sexual offences; Publishing intimate images; Sentencing; Conditional sentence

- **Link to Court File:**
<https://www.canlii.org/en/on/onsc/doc/2018/2018onsc4726/2018onsc4726.html>
- **Link to Abridged Description from the eQuality Project (Technologically-Facilitated Violence):**
<http://www.equalityproject.ca/wp-content/uploads/2019/01/TFVAW-Non-Consensual-Distribution-of-Intimate-Images-6-March-2018.pdf>

Circumstances of offense

Abridged description:

- Mr. B, a 30-year-old man, pleaded guilty to **publishing images of Ms. T without her consent** following the breakdown of their intimate relationship.
- Mr. B **created a fake Facebook page using Ms. T's full name** and **posted five intimate images of her** on the page that he had taken during their relationship.
- **Ms. T had not given him permission** to share those images with anyone. **96 people, including her employer, co-worker, family and friends were invited to "friend" her on Facebook and viewed the images.**

What does the Criminal Code say?

Offense

Before me for sentencing is J.C.B. who, on October 30, 2017, pled guilty to a charge of publishing an intimate image without consent, contrary to **s.162.1 of the Criminal Code of Canada**, (“the Code”).

Publication, etc., of an intimate image without consent

- **162.1 (1)** Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty
 - (a) of an indictable offence and liable to imprisonment for a term of not more than five years; or
 - (b) of an offence punishable on summary conviction.

Sentencing objectives

- As emphasized by s.718 of the Code, the fundamental purpose of sentencing is to contribute to respect for the law and the maintenance of a **just, peaceful and safe society** (...)
- Pursuant s.718.2 of the Code (...) **A sentence should be increased or reduced to account for any relevant aggravating or mitigating circumstances** relating to the offence or the offender

Sentencing Principles

Other considerations

- The court noted “It was only through a position of trusted intimacy that he was able to take and retain the intimate images in question”.
- This was considered an **aggravating factor** along with (...) the ongoing negative impact on Ms. T, the inability to control the images once they have been released online, and the deliberateness of creating the impersonation account.
- **Mitigating factors** included his new relationship and family.

Sentence

- Mr. B was sentenced to a 16 months’ conditional sentence and three years’ probation, additional orders included a \$200 victim surcharge fine, a no contact order with the victim, and a DNA order.

The court file mentions the existence of some pieces of digital evidence like photos and copies of online content:

- After the fake Facebook profile and posted intimate images had been brought to her attention on August 20, 2015, Ms T. attended London Police headquarters later that day to file a report, providing a detailed statement, as well as **copies of the fake Facebook profile and the relevant intimate images.**

Cybercrime Law

Definition of Crime

- A **crime** is an offensive act against society that violates a law and is punishable by the state
- Two important principles:
 - The act must violate at least one current criminal law
 - It is the state (not the victim) that punishes the violator
- Until a law addresses an action, there is no “crime” in performing it



The Criminal Code

- It **collects and restates** most of the criminal law in Canada.
- Defines the conduct that constitutes criminal offences.
- Establishes the kind and degree of punishment that may be imposed on someone convicted of an offence.
- The provinces and territories are primarily responsible for enforcing the criminal law.
 - Including the investigation and prosecution of most offences.



The Criminal Code of Canada: <https://www.justice.gc.ca/eng/csj-sjc/ccc/index.html>

Cybercrime

- The terms computer crime, cyber crime, information crime, and high-tech crime are generally used interchangeably.
- The RCMP defines **cybercrime** as any crime where a **cyber element** (that is, the internet and information technologies such as computers, tablets or smart phones) has a substantial role in the commission of a criminal offence.



Examples of Cybercrime - Technology-as-instrument

- **Identity Theft & Fraud**

- Acquire another person's identity information (with intent to use it to commit an offence).
- Defraud the public or any person of any property, service, money or valuable security

- **Extortion**

- By threats, accusations, menaces or violence induces or attempts to induce any person to do anything or cause anything to be done.

- **Cyber-stalking**

- **Child Sexual Abuse Material (CSAM)**

Examples of Cybercrime - Technology-as-target

- **Illegal access**
 - e.g., using malicious software (“malware”) to illegally access computer systems
 - Hacking to steal sensitive data such as personal identifiable information
 - Penetrate a network and change its internal configurations
- **Denial of service**
 - Aim at stopping legitimate requests to a network over the Internet by subjecting the network to illegitimate requests

Cybercrime categories

The RCMP splits up cybercrime in two main categories:

- **Technology-as-target**
 - computer or its data is the crime target
 - E.g., viruses and worms, trojan horses, theft of data, software piracy, defacing corporate web sites...
- **Technology-as-instrument**
 - computer is used to plan/commit the crime
 - E.g. stalking, gambling, child pornography, counterfeiting, forgery, identity theft, phishing, drug trafficking, burglary, ...
- In some cases, the computer can be the **target and the tool**

Cybercrime jurisdiction

- Cybercrime is often **international** (two or more jurisdictions)

Braintech v. Kostiuk

- Braintech decided to sue Kostiuk, a B.C. citizen, in Texas because of the allegedly defamatory comments that Kostiuk had posted on an investors' chat line that were read by (potential) shareholders residing in Texas.
- The B.C. Court of Appeal held that merely presenting information via the Internet which is accessible to users in foreign jurisdictions does not provide sufficient grounds to allow a court in another country to assert jurisdiction.

<https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf>

Cybercrime treaties

- Rules of evidence, police powers, etc. in one country don't usually carry over to another
- The Council of Europe cybercrime treaty (a.k.a., “Budapest Convention”), to which Canada and the US are also signatories, stipulates that member countries should pass laws making it easier for law enforcement to access telecommunications traffic



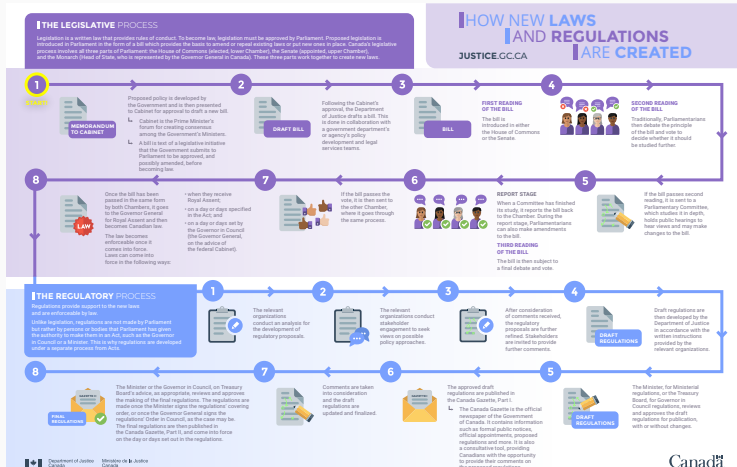
Investigative Powers for the 21st Century Initiative (IP21C)

- Horizontal initiative led by the Department of Justice Canada (Justice) in collaboration with the Public Prosecution Service of Canada (PPSC), the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada (GAC).
- **Goal:** To provide the means to (...) meet Canada's international obligations stemming from ratification of the Budapest Convention
- A report found that the **mutual legal assistance** provisions of the Budapest Convention are considered to be inefficient, "given the legal and procedural protections in place to protect privacy and other human rights".

<https://www.justice.gc.ca/eng/rp-pr/cp-pm/eval/rep-rap/2020/ip21c-pe21s/index.html>

Lengthy legislative process

- A “crime” requires an existing law
 - More often than not, the law lags behind the crimes



Digital Crime Scene

- **Digital evidence** is information that can be admitted to court for a case that is stored digitally or electronically. The courts call this type of evidence “**electronic document**” evidence.
- Section 31.8 of the Canada Evidence Act defines an “electronic document” as:
data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data.

- The electronic environment where digital evidence can potentially exist (Rogers, 2005)
- **Locard's Exchange Principle**
 - the perpetrator of a crime will bring something into the crime scene and leave with something from it, and both can be used as evidence.
 - Edmond Locard was a French criminologist (1877-1966), and pioneer in forensic science



The task of forensic investigators



- Recognize, document, and collect **evidence** from both the scene of a crime, and anything or anyone that may have come in contact with the crime scene
- Solving the crime is then dependent on the investigators ability to piece together the evidence to form a picture of events

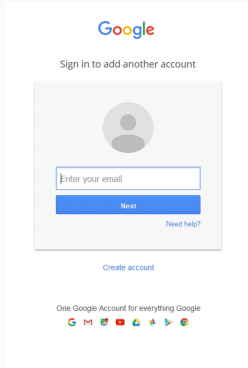
The task of forensic investigators



- Recognize, document, and collect **evidence** from both the scene of a crime, and anything or anyone that may have come in contact with the crime scene
- Solving the crime is then dependent on the investigators ability to piece together the evidence to form a picture of events

Q: What if computers are involved?

Locard's Exchange Principle in the Digital World



- Suppose a subject logs into google.com

Q: What evidence of this “visit” does she **leave** at the server?

Q: What evidence of this “visit” does she **take** with her?

Locard's Exchange Principle in the Digital World

Q: What evidence of this “visit” does she **leave** at the server?

- An entry in the web server log
- ...

Locard's Exchange Principle in the Digital World

Q: What evidence of this “visit” does she **leave** at the server?

- An entry in the web server log
- ...

Q: What evidence of this “visit” does she **take** with her?

- A cookie from the google.com server
- Your browser caches a copy of the web pages you visit
- Your browser keeps a history of all the pages you've visited
- ...

More examples of “things you leave”

- **Login attempts:** Every attempt to login to a system, successful or not, is logged in file `varlogauth.log`

```
Nov 1 08:38:05 rona sshd[3962]: pam_unix(sshd:auth): authentication failure;  
    logname= uid=0 euid=0 tty=ssh rhost=131.122.6.104 user=mxxxxxxx  
Nov 1 08:38:05 rona sshd[3962]: Accepted password for stahl from 131.122.6.104  
    port 49961 ssh2  
Nov 1 08:38:05 rona sshd[3962]: pam_unix(sshd:session): session opened for  
    user mxxxxxxx by (uid=0)
```

- **Commands executed:** Every command executed is logged.
The `lastcomm` tool lists every command executed by any user

```
md5sum      mxxxxxxx ??      0.00 secs Thu Nov 3 07:36  
bash       F      mxxxxxxx ??      0.00 secs Thu Nov 3 07:36  
ssh        mxxxxxxx ??      0.00 secs Thu Nov 3 07:36  
bash       F      mxxxxxxx ??      0.00 secs Thu Nov 3 07:36
```

More examples of “things you take”

- **Recently accessed files:** Files opened recently appear in the Windows registry

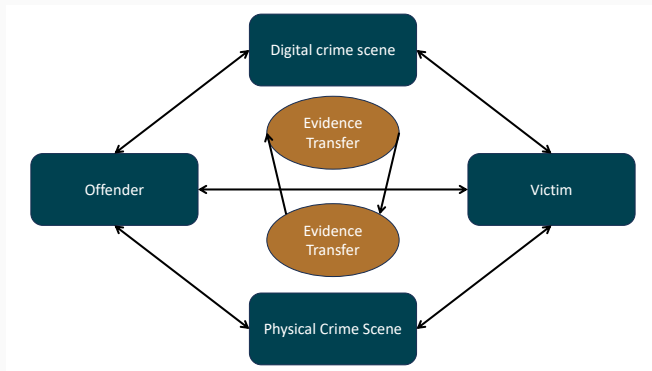
```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
```

- **Visited networks:** The MAC addresses of the routers for networks you've been connected to are recorded in the registry

```
KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\NetworkList\Signatures
```

Computers add a digital dimension to investigations

- Transfers occurs in both the physical and digital realms and can **provide links** between both realms
- Existence of such links between the offender and crime scene become **stronger and easier to demonstrate**



Admissibility of digital evidence

Only admissible evidence be accepted in court

- What makes evidence “admissible”?
 - Short answer – if a judge says it is, it is...
- Judges use guidelines for admissibility:
 - Is the evidence **relevant**?
 - Is the evidence **authentic**?
 - Is the evidence **credible**?
 - Was the evidence **legally obtained**?
- An overriding principle is the “**exclusionary rule**” which says it is not admissible if these criteria are not met

Is the evidence relevant?

- The question of relevance is usually the first considered by a judge: If it is not relevant, then it will not be admissible
- To be deemed relevant, evidence must satisfy 2 conditions:
 - It must be **material** – directly related to the case
 - It must be **probative** – proves something that will help get to the truth of the situation

Is the evidence relevant?

- The question of relevance is usually the first considered by a judge: If it is not relevant, then it will not be admissible
- To be deemed relevant, evidence must satisfy 2 conditions:
 - It must be **material** – directly related to the case
 - It must be **probative** – proves something that will help get to the truth of the situation

Example:

In US vs. Carey (1998), the investigator found child pornography on a machine while searching for evidence on drug-related activity but the images were inadmissible because they were outside the scope of the warrant

Is the evidence authentic?

- The question of authenticity is basically asking if the evidence is what it purports to be
- This requires asking:
 - Was it **collected correctly**?
 - Could it have been **altered** in any way?
- Must show that:
 - Evidence was acquired from a specific computer and / or location
 - A complete and accurate copy of digital evidence was acquired
 - Evidence remained unchanged since it was collected

Is the evidence credible?

- This requires asking a number of questions which include:
 - Is the material an **out-of-court statement** (hearsay)?
 - Is the evidence **sustained** by the testimony of a witness?
- Knowledge from secondary sources is “hearsay evidence” and is, in principle, inadmissible
 - i.e., not what the witness knows personally, but what someone else told her

Is the evidence credible?

- This requires asking a number of questions which include:
 - Is the material an **out-of-court statement** (hearsay)?
 - Is the evidence **sustained** by the testimony of a witness?
- Knowledge from secondary sources is “hearsay evidence” and is, in principle, inadmissible
 - i.e., not what the witness knows personally, but what someone else told her

Example:

- An e-mail message may be used to prove that an individual made certain statements, but cannot be used to prove the truth of the statements it contains
 - Larry Froistad sent a message to a mailing list saying he had killed his daughter, but a confession and other evidence were needed

Some exceptions to the “hearsay” rule

- Business records:
 - Documents compiled by the ordinary course of a business (e.g., emails, records, memoranda, etc.)
 - Were supplied by a person who had personal knowledge of the matters dealt with
- Automatically-generated data
 - When a person is not making an assertion
 - e.g., computer logs, network traces, etc.

Was the evidence legally obtained?

- Search warrants are required
- The most common mistake that prevents digital evidence from being admissible is that it is **obtained without authorization**
 - Privacy violations render evidence inadmissible
- Directives for **data privacy protection** defined by law
 - GDPR: General Data Protection Regulation
 - PIPEDA: The Personal Information Protection and Electronic Documents Act
 - HIPAA: Health Insurance Portability and Accountability Act

The limits of a warrant

- Forensic investigators must articulate a probable cause necessary to obtain a search warrant
- They must also recognize the limits of warrants for the search and seizure

Wisconsin v. Schroeder

- A search warrant for evidence of online harassment was issued and given to the detective to search and seize the defendant's computer and related items. During the initial search the computer lab examiner found some pornographic images of children.
- The search process was halted and a second warrant sought to provide authority to search for evidence of child pornographic pictures.

Some past loopholes...

- In the US, collection of electronic evidence via wiretaps has been controlled through statutes such as the Wiretap Act
 - Digital communication **interception** deemed analogous to telephone wiretaps
- LEAs have circumvented the notion of “interception”
 - e.g., the FBI installed keylogging software that would only collect keystrokes while the computer was not using its modem to communicate with other computers
 - The court held that such capture was not a violation of the Wiretap Act.

Letter Opinion and Order, United States v. Nicodemo S. Scarfo, et al. Criminal Action No. 0040 4

Several definitions pertaining to (electronic) documentary evidence:

- 31.1 - Authentication of electronic documents
- 31.2 - Application of best evidence rule — electronic documents
- 31.3 - Presumption of integrity
- 31.4 - Presumptions regarding secure electronic signatures
- 31.5 - Standards may be considered

Canada Evidence Act (page 3): <https://laws-lois.justice.gc.ca/eng/acts/c-5/page-3.html>

The Case of the Stolen Exams²

²The Open University: <https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3>

The Case of the Stolen Exams



My name is Blaine Price – I'm the Course Team Chair of the Open University course C1080: computer forensics and investigations. I'd like to show you something I found on eBay last week.

The Case of the Stolen Exams

Open University Exam Questions & Answers for NEXT exam! on eBay (end time 23-Jun-10 22:21:53 BST) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://cgi.ebay.co.uk/ws/ebayESAPI.dll?ViewItem&item=120594582468

Most Visited Getting Started Latest Headlines

- Problem loc...
- Problem loc...
- Problem loc...
- Flickr: Orga...
- Open ...
- Porto6 R6...
- Satellite Pro...
- Lenovo Th...

Open University Exam Questions & Answers for NEXT exam!

- Revise your item
- Sell a similar item
- Create postage discounts

Listing info

Duration: 7 days
Start price: £0.99

Open University Exam Questions & Answers for NEXT exam!

Item condition: **New**

Time left: 6d 23h (23 Jun, 2010 22:21:53 BST)

Bid history: 0 bids

Starting bid: **£0.99**

Enter maximum bid: £ **Place bid**


(Enter £0.99 or more)


This item is being tracked in My eBay.


Postage: **£5.00** Seller's Standard Rate | [See all details](#)
Check the item description for special conditions on delivery time.


Payments: **PayPal** | [See details](#)

Returns: No Returns Accepted

 **eBay Buyer Protection**
Shop with confidence. [Learn more](#)





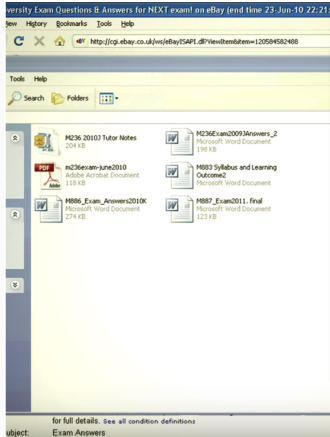


This is an ad for a memory stick containing the answers for upcoming Open University exams. So I asked a friend to buy it for me.

The Case of the Stolen Exams



The Case of the Stolen Exams



OK, there are the files for the answers and the questions for the exams for the next year for a couple of courses.

Now USB devices like this often contain serial numbers. And the computer keeps a record of almost all the USB devices ever plugged into it, including the date and time it was first plugged in and the last time it was plugged in. Let's see what we've got on this one.

I'm going to run a program called USBDeview. This asks the computer to list all the USB devices on it and all the characteristics.

The Case of the Stolen Exams

	USB Hub	Drive L...	Serial Number	Created Date		
	No			06/04/2010 12:07:29		
	No	E:	1515040027363505	18/05/2010 10:30:37		
	No		15162500710C3F11	24/05/2010 17:02:01		
	No		A100000000000123	24/05/2010 16:25:31		
	No		a9813b4e6698619a...	10/06/2010 22:28:44		
	No			21/05/2010 09:37:35	N/A	045e
	No			17/05/2010 11:51:05	N/A	045e
	No		5758453041433953...	09/06/2010 11:37:32	N/A	1058
	No		1207041000403	28/04/2010 18:15:32	N/A	054c
	No			21/05/2010 10:53:51	N/A	0b8c
	No			14/05/2010 11:29:50	N/A	0b8c
	No			09/06/2010 11:56:25	N/A	0840
	No	D:		01/04/2010 11:49:27	16/06/2010 22:33:24	0930

Here's the flash drive I just plugged in and it's got a serial number, so I'll take a note of it. Now let's go and see if we can find a computer that's had this memory stick plugged into it and find out whose it is.

The Case of the Stolen Exams



I've heard that Crispin, one of our Course Managers, is selling things on eBay, so let's see if he's at his desk. He's there, let's see if we can lure him away.

The Case of the Stolen Exams

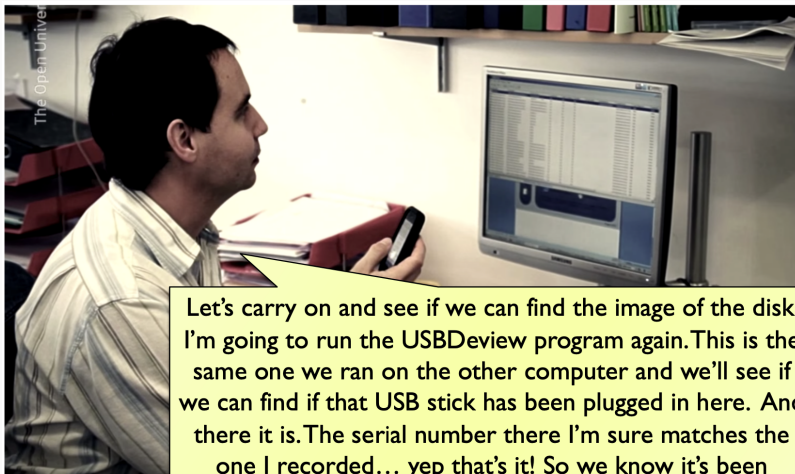


Crispin, it's Blaine here. Listen, I've got an Associate Dean on my back, I really need those consultancy contracts now. I'm in the Perry Building, room 12, can you run over and bring them over? Thanks, bye.

The Case of the Stolen Exams



The Case of the Stolen Exams



Let's carry on and see if we can find the image of the disk. I'm going to run the USBDeview program again. This is the same one we ran on the other computer and we'll see if we can find if that USB stick has been plugged in here. And there it is. The serial number there I'm sure matches the one I recorded... yep that's it! So we know it's been plugged in here.

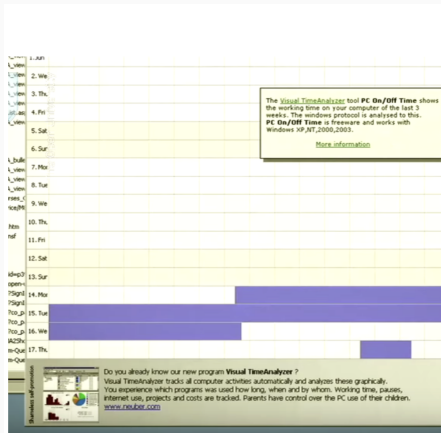
The Case of the Stolen Exams

<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)	8	17/06/2010 13:33:20	13/07/2010 13:33:22	cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> http://css2.open.ac.uk/webdesk/Student/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> http://letrinet.open.ac.uk/outlife-home				cb9294
<input type="checkbox"/> https://letrinet.open.ac.uk/students				cb9294
<input type="checkbox"/> http://www.open.ac.uk/etma/admin				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> https://css3.open.ac.uk/etma/admin/etmaA_viewtutor.asp?674... eTMA Admin System - View Tutor - cb9294 (01925893-V1)				cb9294
<input type="checkbox"/> file:///penelope/MCSUsers/MCS-Groups/For_Blaire				cb9294
<input type="checkbox"/> file:///penelope/MCS-Common/For_Blaire				cb9294
<input type="checkbox"/> http://www.google.com/webhp				cb9294
<input type="checkbox"/> http://mcs-notes1.open.ac.uk:8080/ibay				cb9294
<input type="checkbox"/> http://mcs-notes2.open.ac.uk/mcsintern				cb9294
<input type="checkbox"/> http://letrinet.open.ac.uk				cb9294
<input type="checkbox"/> http://www.ebay.co.uk				cb9294
<input type="checkbox"/> http://shop.ebay.co.uk				cb9294
<input type="checkbox"/> http://shop.ebay.co.uk/?_from=R40&t...				cb9294
<input type="checkbox"/> http://shop.ebay.co.uk/ebayadvice/				cb9294
<input type="checkbox"/> https://signin.ebay.co.uk/ws/ebayISAPI...				cb9294
<input type="checkbox"/> https://signin.ebay.co.uk/ws/ebayISAPI...				cb9294
<input type="checkbox"/> https://signin.ebay.co.uk/ws/ebayISAPI.d?co_partnerId=28sk...	1	17/06/2010 14:19:50	13/07/2010 14:12:42	cb9294
<input type="checkbox"/> https://signin.ebay.co.uk/ws/ebayISAPI.d?co_partnerId=28sk...	2	17/06/2010 14:19:51	13/07/2010 14:12:42	cb9294
<input type="checkbox"/> https://signin.ebay.co.uk/ws/ebayISAPI.d?co_partnerId=28sk...	5	17/06/2010 14:19:51	13/07/2010 14:12:42	cb9294
<input type="checkbox"/> http://completed.shop.ebay.co.uk/i.html?MA25showItems&_img=...	7	17/06/2010 14:19:55	13/07/2010 14:12:46	cb9294
<input type="checkbox"/> http://cg.ebay.co.uk/Open-University-Exam-Questions-Answer...	11	17/06/2010 14:20:02	13/07/2010 14:12:54	cb9294
<input type="checkbox"/> http://cg.ebay.co.uk/Open-University-Exam-Questions-Answer...	10	17/06/2010 14:20:02	13/07/2010 14:12:54	cb9294

We don't know if it was a long time ago or if Crispy actually was the one who put the ad on eBay, so let's see if we can find evidence of him having put the ad on.

Here we've got a program that will show us a history of everything that's ever been looked at on Internet Explorer in the cache. OK, here's a list of all the files he's looked at with Internet Explorer. And if I look down the list... there, eBay! And there is the title matching the title of the ad we saw, so we know that this computer was used to look at the ad on eBay.

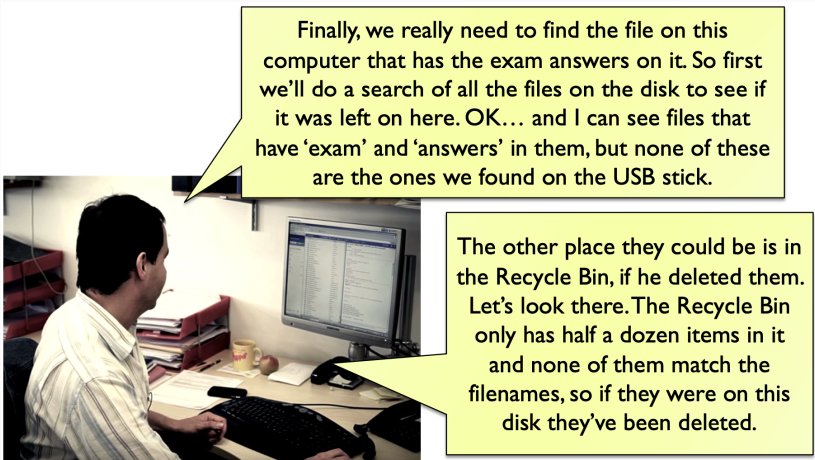
The Case of the Stolen Exams



So we know that the ad was placed on Crispin's machine, we need to find out that Crispin was at the machine at the time. One way to do that is to look at the operating system to see when he was logged in.

This program shows all the times that someone is logged in and out of this computer and we can see that someone was logged in at the time. We'll have to check the network records to make sure it was Crispin who was logged in.

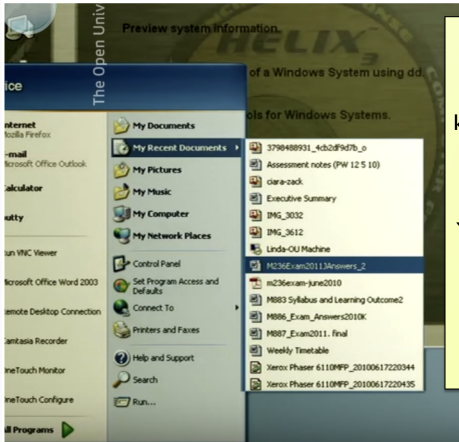
The Case of the Stolen Exams



Finally, we really need to find the file on this computer that has the exam answers on it. So first we'll do a search of all the files on the disk to see if it was left on here. OK... and I can see files that have 'exam' and 'answers' in them, but none of these are the ones we found on the USB stick.

The other place they could be is in the Recycle Bin, if he deleted them. Let's look there. The Recycle Bin only has half a dozen items in it and none of them match the filenames, so if they were on this disk they've been deleted.

The Case of the Stolen Exams



One other thing that people often forget is that Windows keeps a record of the files you've used recently. Let's look in the 'recently used files' list and see what comes up. And there it is. You can see in the list of the last ten used documents that the filenames of these files were here, so these files were probably on this computer.

The Case of the Stolen Exams



If we had some more time, I'd take an image of this disk, take it away and look at it with another tool because when Windows deletes a file it doesn't actually erase it, it just marks it for reuse. And if Windows hasn't had to reuse that space, then the whole file will still be there.

So what do we do now? We have a fair amount of evidence against Crispin. Do we call his boss? The Dean? Campus Security? The Police? Or, should we call my boss? Did I do anything wrong?

Takeaways

- Computers can be used in a wide variety of criminal activities, which are sanctioned by law
- Evidence must be **admissible**, which is determined by the judge according to a set of exclusionary rules: relevance, authenticity, credibility, and proper search and seizure
- To reduce the chance of producing inadmissible evidence, digital investigators must follow a strict **methodology**

- **Textbook:**
 - Casey – Chapters 2 & 3
- **Other resources:**
 - RCMP: Cybercrime defined
 - The Criminal Code of Canada
 - Ontario Superior Court of Justice - R. v. J.B., 2018 ONSC 4726 (CanLII)
 - The eQUALITY Project - Tech-Facilitated Violence: Criminal Case Law
 - The Case of the Stolen Exams
- **Acknowledgements:**
 - Slides adapted from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon