CS 798: Digital Forensics and Incident Response

Lecture 3 - Digital Investigation Process

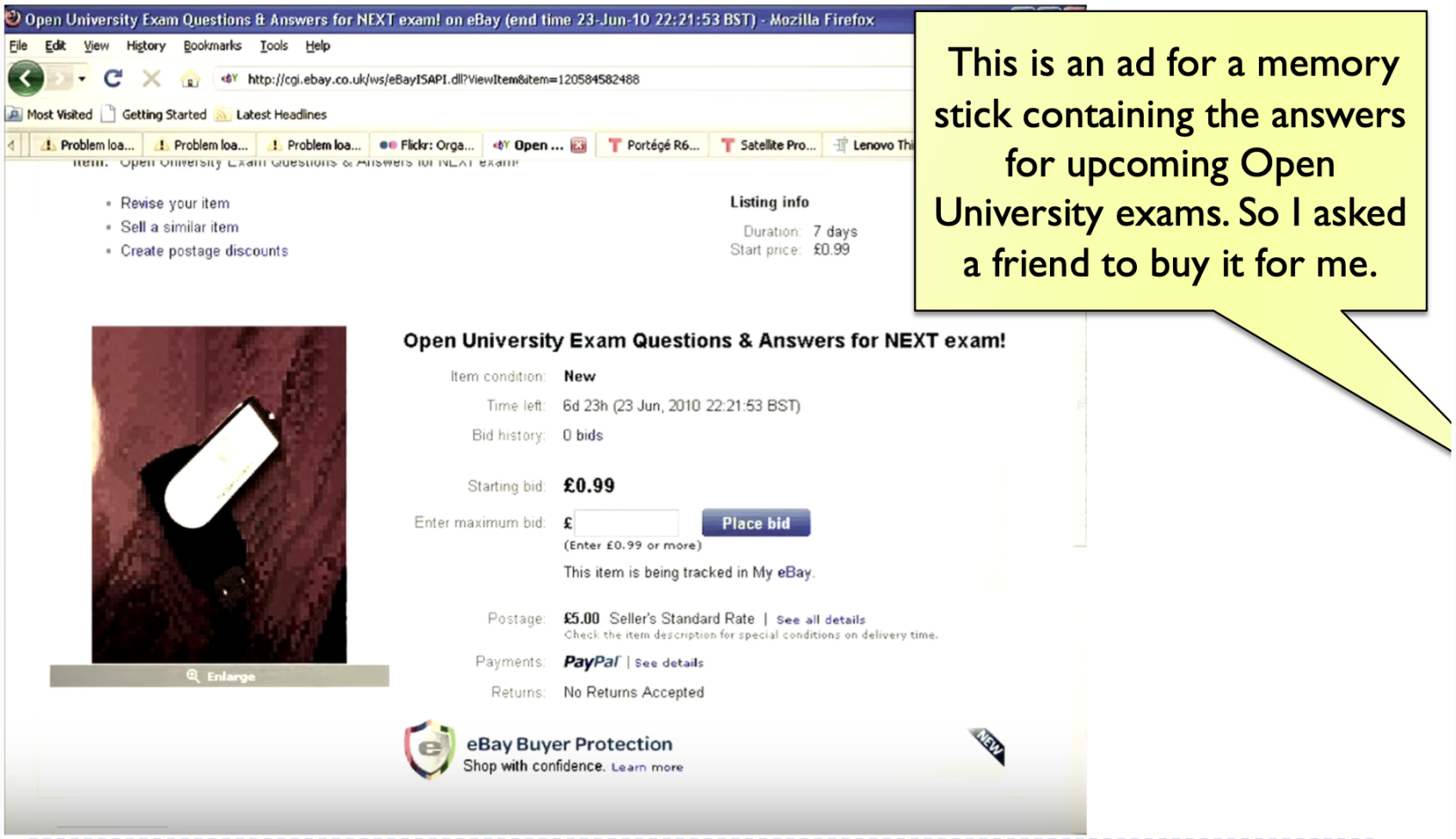
Diogo Barradas

Winter 2025

University of Waterloo

Recall...

- The Case of the Stolen Exams



The goal of a digital investigation

- To uncover the truth by producing admissible evidence
- To be admissible, evidence must meet the following criteria:
  - **Relevance:** be related to the case and prove something
  - **Authenticity:** evidence is the same as the originally seized
  - **Credibility:** the original evidence or admissible hearsay
  - **Legality:** search and seizure are authorized
- Ultimately, the judge decides, but the digital investigator is responsible for ensuring all these criteria are met

Outline

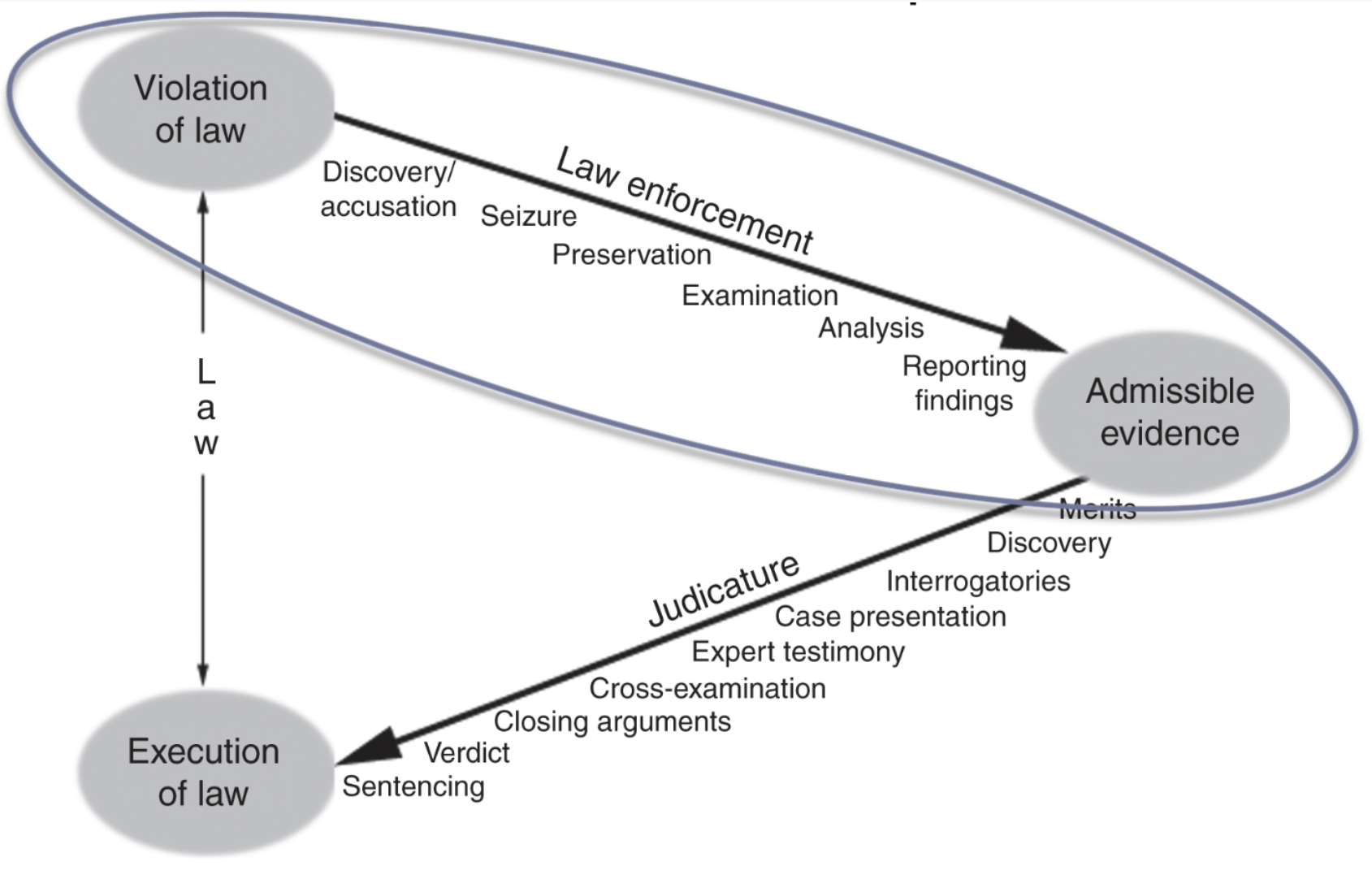
1. Digital Investigation Models

2. The Scientific Method

Digital Investigation Models

Path to producing admissible evidence

- Case / incident resolution process

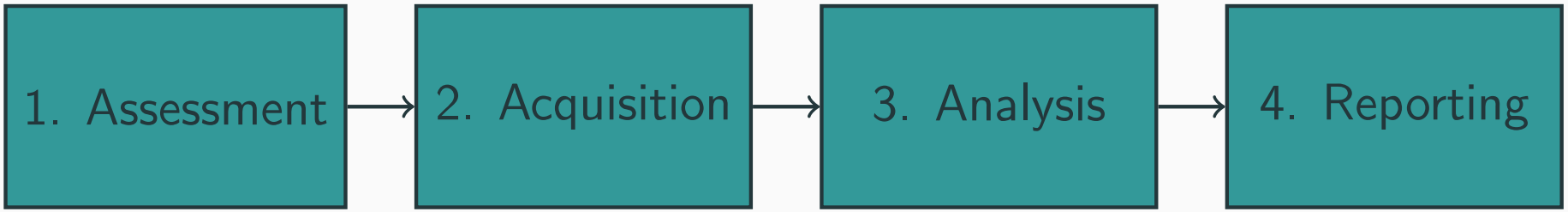


Digital investigation model

- Predefined pattern of activities when performing an investigation to generate admissible evidence
- Serve as useful points of reference for reflecting on the state and nature of the field
- Independent of a particular technology in corporate, military, and law enforcement environments

Models encourage a complete, rigorous investigation, ensures proper evidence handling, and reduce the chance of mistakes created by preconceived theories, time pressures, etc.

First reference model for digital forensics



- The Kruse & Heiser model (2001) comprises four steps:
  - **1. Assessment:** Prepare plan of action, and find potential sources of digital evidence
  - **2. Acquisition:** Prevent changes of in situ digital evidence and collects them
  - **3. Analysis:** Search for and interpret evidence trace in order to reconstruct the crime scene
  - **4. Reporting:** Reporting of findings in a manner which satisfies the context of the investigation

1. Assessment

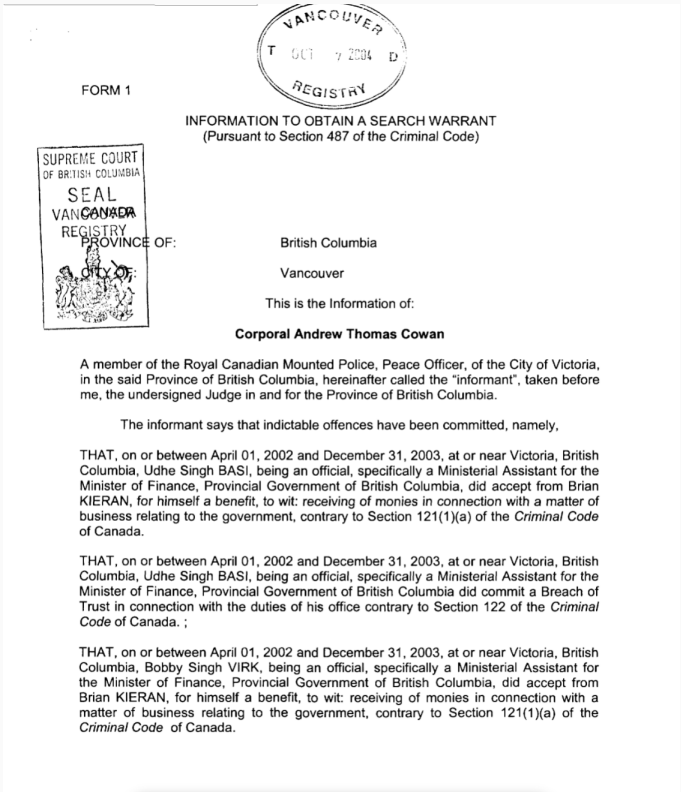
- Define the scope and likely venue of the examination
- Collect all legal documentation needed
  - Get any permissions for resources not covered by warrants
- Determine likely sources of evidence for the case
  - Sources of data are reliable

Authorization level set by the investigation type

- **Internal investigations**
  - Sponsored by an organization. They generally start out as a deep, dark secret that the company doesn't want getting out. Courts rarely involved at the outset (e.g., insider suspicious activity)
- **Civil investigations**
  - Require involvement of courts. The plaintiff and the defendant are two litigants asking the courts to settle a dispute (e.g., patent- related dispute)
- **Criminal investigations**
  - Involve the courts. The defendant is the person accused of a crime and the plaintiff is the one making the accusation, which will always be some level of government authority (e.g., homicide case)

Required Authorization Levels

- For **internal investigations**
  - You need a signed letter of agreement outlining the scope of the investigation along with contractual details
- For **civil** and **criminal** investigations
  - You need a court order prior to starting



VANCOUVER REGISTRY

FORM 1

INFORMATION TO OBTAIN A SEARCH WARRANT
(Pursuant to Section 487 of the Criminal Code)

SUPREME COURT OF BRITISH COLUMBIA SEAL VANCOUVER REGISTRY

PROVINCE OF: British Columbia

CITY OF: Vancouver

This is the Information of:

Corporal Andrew Thomas Cowan

A member of the Royal Canadian Mounted Police, Peace Officer, of the City of Victoria, in the said Province of British Columbia, hereinafter called the "informant", taken before me, the undersigned Judge in and for the Province of British Columbia.

The informant says that indictable offences have been committed, namely,

THAT, on or between April 01, 2002 and December 31, 2003, at or near Victoria, British Columbia, Udhe Singh BASI, being an official, specifically a Ministerial Assistant for the Minister of Finance, Provincial Government of British Columbia, did accept from Brian KIERAN, for himself a benefit, to wit: receiving of monies in connection with a matter of business relating to the government, contrary to Section 121(1)(a) of the *Criminal Code* of Canada.

THAT, on or between April 01, 2002 and December 31, 2003, at or near Victoria, British Columbia, Udhe Singh BASI, being an official, specifically a Ministerial Assistant for the Minister of Finance, Provincial Government of British Columbia did commit a Breach of Trust in connection with the duties of his office contrary to Section 122 of the *Criminal Code* of Canada. ;

THAT, on or between April 01, 2002 and December 31, 2003, at or near Victoria, British Columbia, Bobby Singh VIRK, being an official, specifically a Ministerial Assistant for the Minister of Finance, Provincial Government of British Columbia, did accept from Brian KIERAN, for himself a benefit, to wit: receiving of monies in connection with a matter of business relating to the government, contrary to Section 121(1)(a) of the *Criminal Code* of Canada.

Identification of sources of evidence

- General hint: Follow the data path
- Depends on the kind of case or crime category
  - e.g., recommendations from (NIJ04):

E-mail Threats, Harassment, and Stalking

Potential digital evidence in e-mail threat, harassment, and stalking investigations includes:

- Computers.
- Handheld mobile devices.
- PDAs and address books.
- Telephone records.
- Diaries or records of surveillance.
- Evidence of victim background research.
- E-mail, notes, and letters.
- Financial or asset records.
- Printed photos or images.
- Legal documents.
- Information regarding Internet activity.
- Printed maps.

Additional steps in assessment stage

- Identify the forensic tool required
  - Evidence to be collected w/ court-recognized dependable tools
- Identify the personnel needed
  - Personnel must be qualified to do their jobs
- Identify the stakeholders

2. Acquisition

- Evidence collection methods must assure that:
  - All issues of legal "search & seizure" are followed
  - Evidence integrity was preserved upon extraction
  - Evidence presented to the court is authentic
  - Evidence collection is as complete as possible

Maintaining chain of custody

- Maintain a chain of custody, a.k.a continuity of possession:
  - One of the most important aspects of authentication is maintaining and documenting the chain of custody of evidence
  - Begins when evidentiary materials are first seized
    - Time and date taken
    - From whom and where
    - Complete description of each item
  - Every time an item changes hands, time, date and people involved (get signatures)

Chain of custody form

EVIDENCE

Agency: _____

Item No.: _____ Case No.: _____

Date of Collection: _____ Time of Collection: _____

Collected By: _____

Description of Evidence: _____

_____

_____

_____

Location of Collection: _____

_____

_____

Type of Offense: _____

Victim: _____

Suspect: _____

CHAIN OF CUSTODY

Received From: _____ By: _____

Date: _____ Time: _____

Received From: _____ By: _____

Date: _____ Time: _____

Received From: _____ By: _____

Date: _____ Time: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

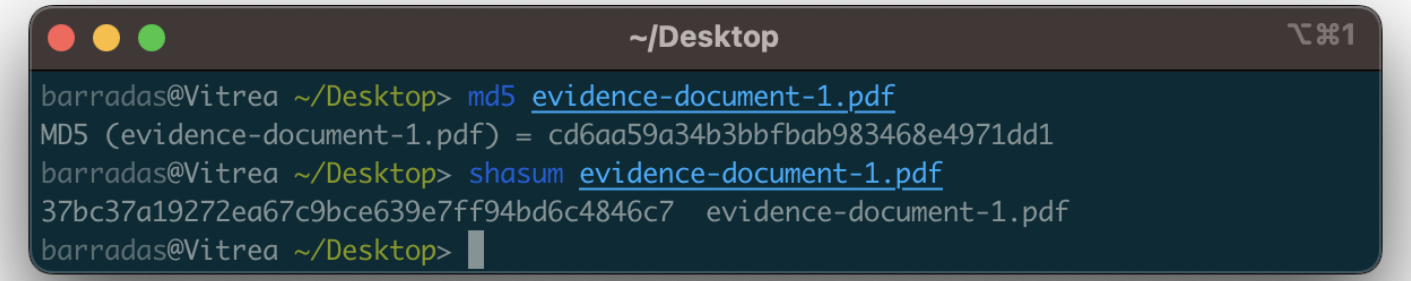
Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Potential issues with the chain of custody

- Incomplete: gaps
- Inconsistent dates
- Lacking custodians' signatures or identification
- Custodian is not competent or authorized

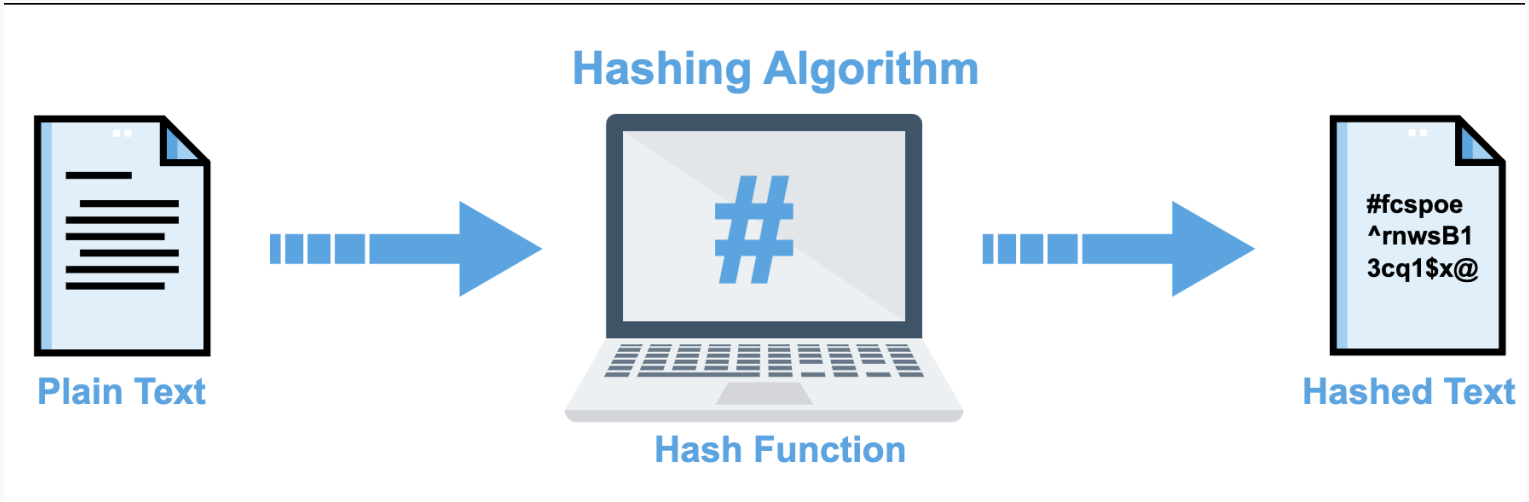
Integrity checks

- Integrity checks help us check that evidence has not been altered from the time it was collected, thus supporting the authentication process
- Verifying the integrity of evidence generally involves a comparison of the digital fingerprint for that evidence taken at the time of collection with the digital fingerprint of the evidence in its current state
- A digital fingerprint is produced by a message digest algorithm, e.g., MD5, or SHA-1



Generation of integrity checks

- A message digest algorithm (hash function) has two important properties (hopefully):
  - Produces the same number for a given input
  - Produces a different number for different inputs



Why do hash functions help us

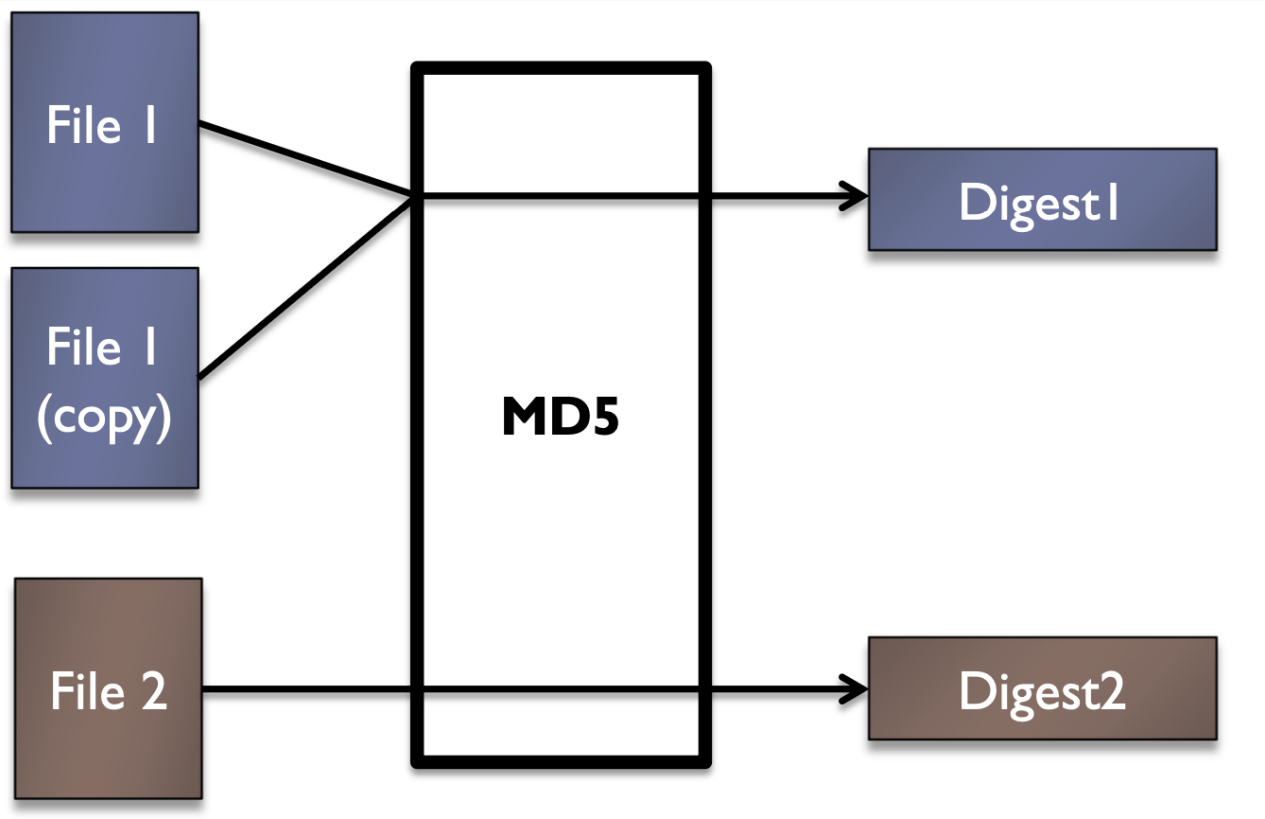
- A file's exact copy will have the same message digest as the original but slight changes will have an effect on the output

Digital input	**MD5 output**
The suspect's name is John	0dc789ca62a3799abca7f1199f7c6d8c
The suspect's name is Joan	d5b5034d2f3bd578a136e18946e5777a

- Most commonly used cryptographic hash functions:
  - MD5: produces a 128-bit hash value
  - SHA-1: produces a 160-bit hash value

Integrity check generation using MD5

- The word fingerprint emphasizes the near uniqueness of a message digest calculated using a digest algorithm

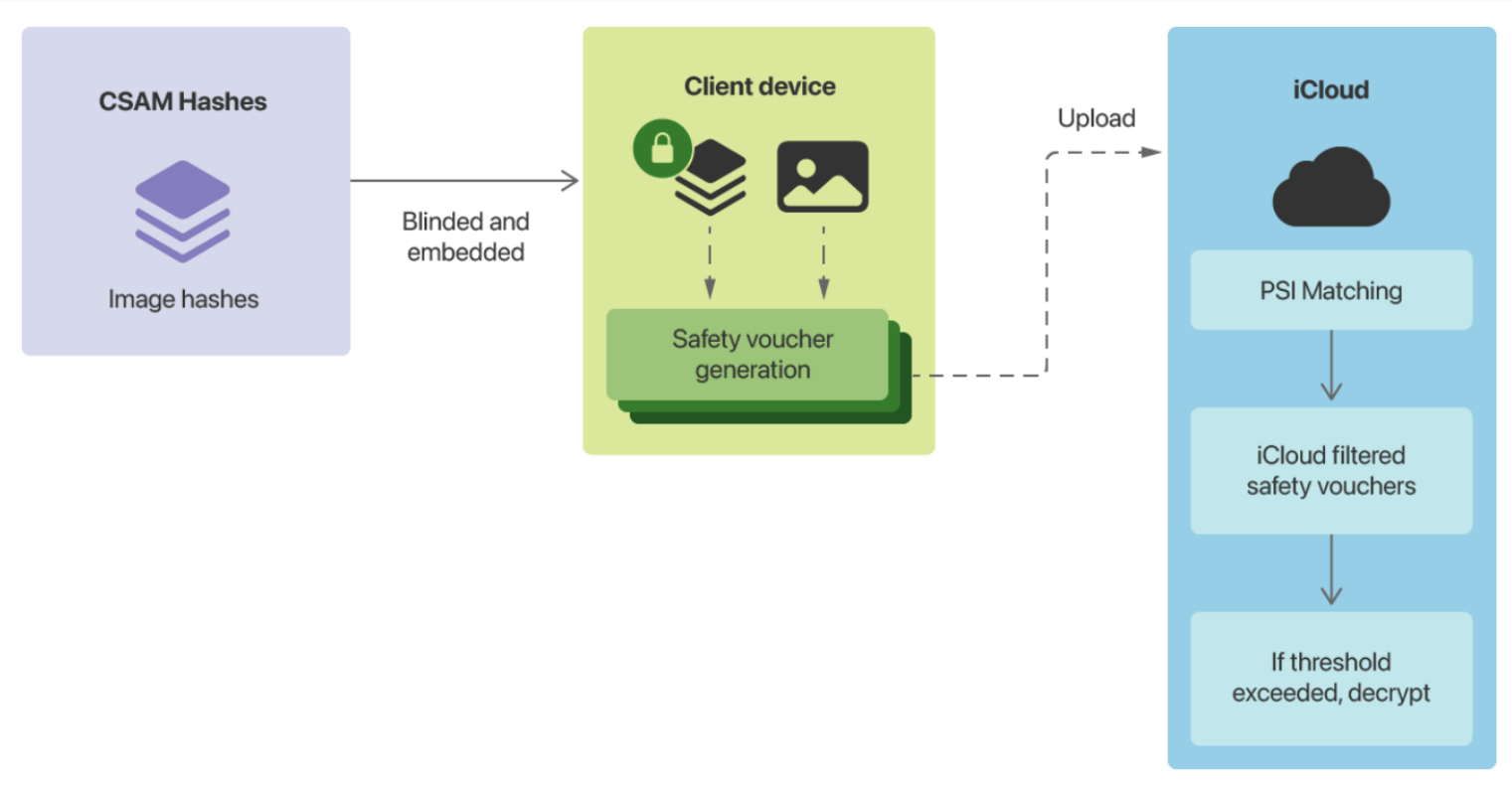


- Authenticate that the copy is identical to the original (i.e., hash values).

Alternative integrity check methods

- Perceptual hashing

Apple's CSAM Detection w/ perceptual hashing



https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

Handling Digital Evidence

- Handle the digital evidence properly (more in the next class)
  - Other than in exceptional situations, never work on original data sources: create a copy of the original data
  - In a "live acquisition", use proper procedures to capture data on-site: live forensics vs. post mortem analysis
  - Store the original and the 2nd copy (or other collected evidence) in a secure location where you can control access
  - Document all steps taken to collect the devices from the initial contact through arrival at the forensic lab

3. Analysis

- Using whatever forensic tools you deem necessary, locate and extract all material evidence, both:
  - Inculpatory: evidence that supports a given theory
  - Exculpatory: evidence that contradicts a given theory
- Use court recognized tools and document everything

Examine existing artifacts looking for evidence

- **Overt evidence**
  - Look through your data image for overt evidence. For example, pictures, documents, spreadsheets, etc. that could be evidence
- **Hidden evidence**
  - Look for evidence that the system may have hidden
- **Deleted evidence**
  - Look for evidence that the user may have deleted, but is still recoverable
- **Anti-forensic trails**
  - Look for evidence of anti-forensic techniques being employed. E.g., encryption, hidden partitions, etc.

Offense reconstituition

- **Temporal** (when)
  - Helps identify sequences and patterns in time of events
- **Relational** (who, what, where)
  - Components of crime, their positions and interactions
- **Functional** (how)
  - What was possible and impossible (e.g., was a suspect's computer capable of displaying the files presented as incriminating evidence)

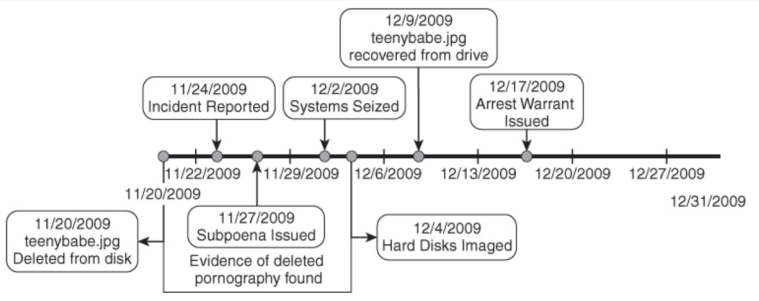


Figure 1: Timeline rec.

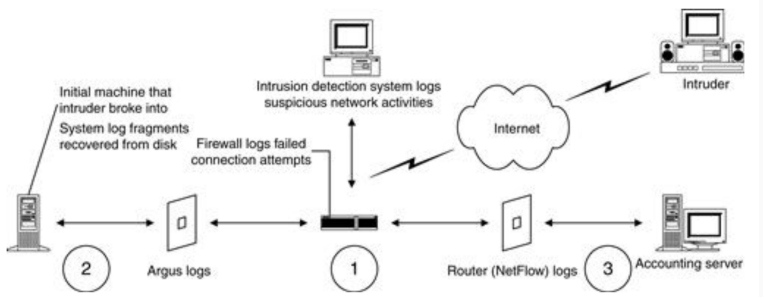


Figure 2: Relational rec.

4. Reporting

- The work product of your analysis is the documentation
- Without good documentation, you can't present a robust case
  - Must be such that it allows for the reproducibility of findings
- 5 levels of documentation are needed:
  1. General case documentation
  2. Procedural documentation
  3. Process documentation
  4. Case timeline
  5. Evidence chain of custody (already covered)

Levels of collected documentation

- **General case documentation**
  - Contact information for everyone involved, all legal authorizations
  - First response documentation: notes, photographs, videos, etc.
- **Procedural documentation**
  - Every task that was performed related to the investigation, list of equipment seized, steps taken and tools used, detailed data analysis
- **Process documentation**
  - User manuals, installation manuals, update history logs, results of testing, README logs
- **Case timeline**
  - Systematic analysis of what transpired, times and dates of related events

Producing the final report

- Using the detailed documentation that you have collected:
  - Begin writing the report in a standard format appropriate for the audience
  - Fully explain all evidence that was retrieved
  - Fully explain any problems or discrepancies encountered during your analysis
  - Do not make any assertions of innocence or guilt; just present the facts as you found them

Final Report (Crawford'15)

EXAMPLE OF AN
EXPERT WITNESS

DIGITAL FORENSIC REPORT

By: Vincenzo Crawford

BS. FORENSIC SCIENCE, University of Technology (U-Tech), Jamaica

INVESTIGATOR:	**Patrick Linton**
	CEO
	Digital Inc.
DIGITAL FORENSICS EXAMINER:	**Vincenzo Crawford**
	Detective #1005315
	Faculty of Science and Sports (FOSS), Digital Forensics Expert
	Portmore, St. Catherine
	(876) 782-0696
SUBJECT:	**Digital Forensics Examination Report**
OFFENCE:	Money Laundering, Embezzlement, Insider Trading, Scamming, Racketeering activities, Fraud,Terrorism and Forgery
ACCUSED:	**Therese Brainchild**
DATE OF REQUEST	Oct. 27, 2013
DATE OF CONCLUSION	Nov. 09, 2013

Final Report (Crawford'15)

Contents Page

Background to the Case

Therese Brain child, a master accountant hired by Safe Data Associates was suspected of being engaged in cyber crimes, industrial espionage, embezzlement and terrorism. The aid of Digital forensics along with legal authorities was employed by Patrick Linton's Digital Inc. in order to exonerate or convict the accused (Therese Brainchild). Brainchild opted to delete files from her thumb drive kept at her workstation before being escorted from the building and her administrative duties. She swears she is innocent of all accusations, However, intelligence shows that in 2008, Therese Brainchild converted J$30M of criminal proceedings to start a construction business in order to legitimize her illicit earnings.

To conduct an effective and efficient investigation, I employed the use of the Forensic Tool Kit Imager software (FTK Imager) in order to recover the files deleted from the thumb drive said to be that of Brainchild's;
Based on my expert knowledge of digital forensics, these deleted files will still be lingering in what is called the 'unallocated space' of the thumb drive.

1. Questions Asked Relevant To The Case

Further background Checks were conducted on Brainchild. She was questioned in order to acquire legitimacy for data acquisition. The following questions were brought forward:

	Questions
1.	Is the computer system, thumb drive and other devices personal or were they assigned to Brainchild by the company?
2.	Does anyone else in or out of the company have any form of access to these devices or to the assigned workstation of Brainchild's?
3.	If these devices were assigned by the company, were they being used before, during and or shortly after they were assigned to the accused (Therese Brainchild)?

2. Search and seizer and transport of evidence

A request was filed for legal authorities to enter the dwelling of Theresa Brainchild. The warrant was issued for the search and seizer of devices which may be analyzed and serve as digital evidence, in order to convict or exonerate her. Upon the search and seizer of the necessary devices which may provide digital evidence, the acquired materials were carefully package and a chain of custody was efficiently established; so to ensure the integrity of the evidence.

Exhibits Submitted for Analysis

Cons#	Exhibits Description and Model	Serial number
1.	Burgundy Wi-Fi Mobile Cellphone	355600084947547
2.	Nokia Mobile Phone	359831087172837
3.	Grey and Silver Kingston Thumb drive	F13225YY
4.	Black and Grey Compaq Presario C600 laptop	CND6752RJN
5.	Black Dapeng cellphone	358729025499270

Final Report (Crawford'15)

	Further Questions Asked Relative To The Case
4.	Were the three(3) cell phones; exhibits 1, 2 and 4 [serial- (355600084947547), (359831087172837) and (358729025499270), respectively] used to call individuals, or browse for information which may be deemed as incriminating and of relevance to the investigation?
5.	Did anyone else other than the accused have access to the thumb drive; exhibit 3 [serial- (F13225YY)] before, during and or after Brainchild's possession of it?

3. Evidence to Search For

Based on the nature of the case and all that which have been made against the accused (Therese Brainchild), to begin analysis of the obtained evidence, the search for data of probative value to the investigation will be in the area of; (A) acquiring the browsing data from the laptop and cell phones' browsers, (B) investigate the previous locations and calls made to and from the cell phones, (C) The acquisition of files deleted from the laptop, phone memories and most importantly files deleted from the thumb drive.

4. List of Criminal Offence

The criminal offences facing 'Therese Brainchild' are; money laundering, embezzlement, terrorism, Racketeering Activities, Insider Trading/ industrial espionage, fraud, forgery and scamming.

5.	Deleted files of evidentiary value to the case
5.1	Three (3) folders containing files of probative interest to this investigation were recovered from the Grey and Silver Kingston Thumb drive bearing the serial number F13225YY. These documents contained; code clues, encrypted and steganographic files, erroneous documents, stolen credit cards information, cheque details, information on lottery winners.
5.2	From the documents acquired, the files contained; bank account details of Therese Brainchild, names, address, telephone numbers and credit card numbers of persons who might have won the lottery, along with employees' information of the company which she was hired.
5.3	Five (5) notepad files disguised by the steganographic techniques were uncovered from the thumb drive of Therese Brainchild. The five (5) txt files recovered contained names, address, phone numbers and credit card information of individuals. Among these files, were steganographic clues to encrypted data.
5.5	Two (2) Microsoft excel documents were recovered; the first excel document identifying that files were copied and transferred to another company, and the second excel document containing Therese Brainchild's personal account number (43524324-234234324324).
5.6	Five (5) Microsoft word documents were recovered, containing Therese Brainchild Swiss bank account number (4332432432-4324324324324-234324423), Transaction information, and contractual/lottery forms.
5.7	Twenty four (25) photo files were recovered, some of which were steganographic files. However, only 4 of these documents were relevant to the investigation as they contained, lottery leads, bank cheque, stolen credit cards information and a terrorist map.
5.8	One (1) Microsoft access (Database) document was found containing customer and employees' detailed information (names, positions, ID numbers, bill payments and account numbers, accounts above 3000 dollars).

6. Corporate Breach

Theresa Brainchild, deemed to have committed corporate breaches such as; the breach of contract to maintain data integrity and company confidentiality, falsification of data, Embezzlement and industrial espionage.

7. Examination Details

I employed the use of FTK imaging technique in order to recover the deleted files from the Grey and Silver Kingston Thumb drive (serial# F13225YY) confiscated from the accused (Therese Brainchild). The sha1 hash value (904e2abcf6f559e70bd9e6516ef3429dd) and MD5 hash value (3b50d4fd1421e5c5c29e3345f7fd0561bc1d5370) were obtained in order to aid in proving the legitimacy of the files recovered. Among the files recovered, there was a database document named 'Snowden Employee.mdb', containing the following information; (i) customers' names and account numbers, (ii) Employees' names, ID numbers and address, (iii) Quarterly bill cycle and Employee accounts below and 'above $3000'.

7.1 Sha1 and MD5 hash value for all documents and deleted files obtained from Brainchild's Thumb drive [serial- F13225YY] via FTK imager.

MD5	SHA1
4516bc7e2b2f68b8dcf3fbc1a256256e	1d899c89e8224b022ed9cb3619d036ea08195bf6
422e327a54b49e2bc50f0ef3dd218795	ce75b695ae3e78bd78f1fbe41d21da895823c077
bccb74803cdad52a4f0eadec92403e4a	7f4f6ea48edf0bb8722b4a68b499293216f0887b
5e2b09eb0b05d9e124613eb1ffac27ee	0132d6aa5a581a179c16fe19bedf426a77031120
d0db850ad982b1640182acec9b75aa35	3606629d1f8d3314832423ba101c3f08d14834b2
421c6a356358ca20ef750e7cbb04c140	49b48ab09d0f2542a7f0012542c530c36ded7caf
1be6c5be960851477469fca61e86dc3f	8f2074940ee5056a8ecafebf2a28bd1d055fe702
4418fe61f16bebf1dd7b22d7d1a67a9e	0184a98c612f235d32f8053b5d47eefc6f65ada9
bec831382b2c37f09f115e23d3067afa	1df94e0d71ba9d30c77c821abb674f48167b60e8
718ba18fd768df5f814d1d12ec3d9d4b	8f51fac1b506936523be5143c66fc34b379eb506
b4b9e59b1ca6d9ae04bf5f45127e52af	916c05d397b36761bc016b080b76c57fe0420906
bacadf3e9df696f96446db014295e8d8	d39aff4ea5061e52e9fa4f6142700fc9ae02738d
55496c77e2c0532c0310c69dadd30f21	a8b566da5d9142a33da1cdae3b67b064dd016eaf
0b9a0f3d3b36af6f38762cc9544e92a0	97cd0235451ee6a32e4602973ac41c756b7d291e
2d525550813433980417 7c037cf086b8	c93fdec71dea265093d8311146babc286dcb9fc8
eb8731db825e01260761fed95d16c77a	3b049f654804ba89d3d976f7bf99e8c8f627b276
9d8f063b3cfaca03b0be7b3c39fc09b8	39a9446af56fccd92d65ffe3852bbd49b613847d
f5aa1d1da28224ee0dd8e55fc40bcc53	029643f9c426a1d396372398874f4cdd3b4f745d
3470d5c0746deeb68484c8fd69225a8a	4be2d7b990714f574923c8d355c381d9d7536382
34956da8ec293972513ba1d0943d4479	e6e15f29daeca48003ccbc448a256053bd674198
d34d89cd328f6edd410273988d68a483	d39c90a5d101707069f327f93db2c77b4d3e76c
e27938ff3830fa6ed5a4bc0775484fb2	3d0091bceb32bb0f99090407d36d968e28a2b59b
0fa71c70567d26092615435c86830827	b9509292fd0f1cd08ab7725bc854c9f81eb319da
ef0bd6deb4f04e241eeffff19e80cc82d	851026c80bb1122c6b9d2094447d90e05e185cc3
b5f45ed1c3f331df2962005f485bfa48	ec870d4cab1800a707028596bfdb488927bde6e9
4d24b2f799fe007239df880ec3aaf051	78767a5c3978b8c266ea1eda98221e572f2ff3cb
12f1e05d2bc553bf981721229818e6ec	d936bb81ef45b1e03aa71040c9a11e1d94c0010f

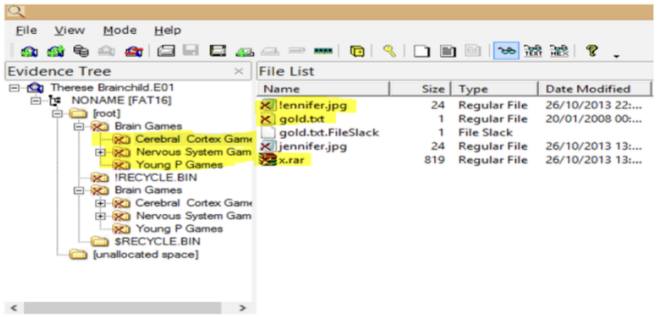
8. Deleted, Encrypted and Steganographic files

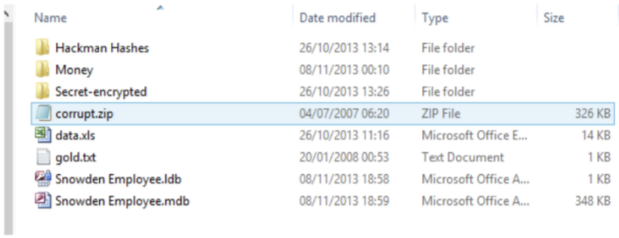
Approximately forty-one (41) files of different formats were deleted. Of all the files retrieved, two (2) files and one (1) folder was encrypted. The encrypted files were cracked as a result of steganograpic files which contained clues and passwords to break the encryption. The encrypted files and passwords are as follows; .Rar file entitled 'x' containing; 1) Database documents of customer and employees' detailed information (names, positions, ID numbers, bill payments and account numbers, accounts

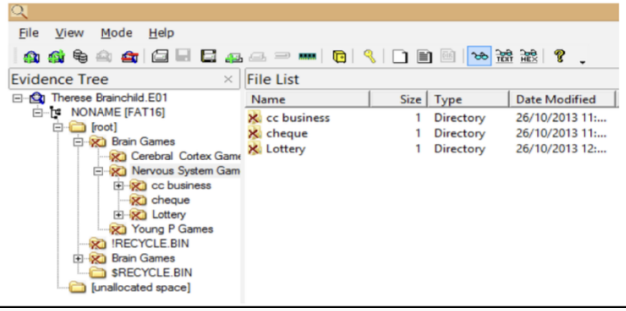
Final Report (Crawford'15)

above 3000 dollars). 2) A Microsoft Excel file entitled 'MONEY' containing a Microsoft Excel document with the accused personal bank account number. 3) A Microsoft Word file entitles 'SECRET-ENCRYPTED' containing the accused Swiss bank account number.

The steganographic files obtained were hidden in various forms (.txt .jpg .zip etc). All steganographic files were recovered and are as follows: (1) The Password [alpha] for Therese Brainchild's personal account was hidden in what APPEARED to be an .mp3 file named ' me.mp3'. (2) The Password [love] for Brainchild's Swiss bank account was hidden in what APPEARED to be a .jpg file named ' sample.jpg'. (3) A file entitled 'corrupt' which APPEARED to be a .zip folder, contained a picture of a map. (5) The hackman hash files containing random pictures (irrelevant to the investigation).
The Personal and Swiss bank account numbers of Therese Brainchild recovered from encryption is; [(43524324-234234324324) and (4332432432-4324324324324-234324423) respectively]. separate and aside from the bank account numbers were the terrorist map which was hidden in the file entitled 'corrupt' which APPEARED to be zip folder.







9. Analysis Results

From the above exhibits;
The cell phones confiscated for analysis, 'Burgundy Wi-Fi Mobile Cellphone', 'Nokia Mobile Phone' and 'Black Dapeng cellphone', exhibits 1, 2 and 5 [serial- (355600084947547), (359831087172837) and (358729025499270), respectively], were analyzed and I calculated their check digit in order to verify the IMEIs which intern reveals the make, model, date and country of origin of all three exhibits.

The check digits calculated are as follows:
Exhibit 1, Wi-Fi Mobile Cellphone, [serial - 355600084947547, corrected was found to be '6'].
Exhibit 2, Nokia Mobile Phone, [serial - 359831087172837, correct check digit found to be '4'].
Exhibit 5, Black Dapeng cellphone, [serial - 358729025499270, [check digit remains unchanged '0']
Further analysis brought to the forefront, identified metadata information which proved to be vital to this investigation. Password clue to the binary digits password [10101111] required to open the 'rar' file entitled 'x' containing fraudulent activities of Therese Brainchild. Passwords were also hidden in Steganography files which lead to brainchild's Personal bank account and Swiss bank account.

10. Conclusion

- The recovery of all data of evidentiary relevance to the investigation was made possible, and I managed to maintain the integrity of all the deleted data during its recovery as all the exhibits were protected and verified by checking hash values and recalculating check digits during the examination.
- I was able to recognize lottery related documents and leads lists, pitch documents, cheques and other documents pointing to fraudulent activities
- The digital devices analyzed showed many involvement of illegal activities.

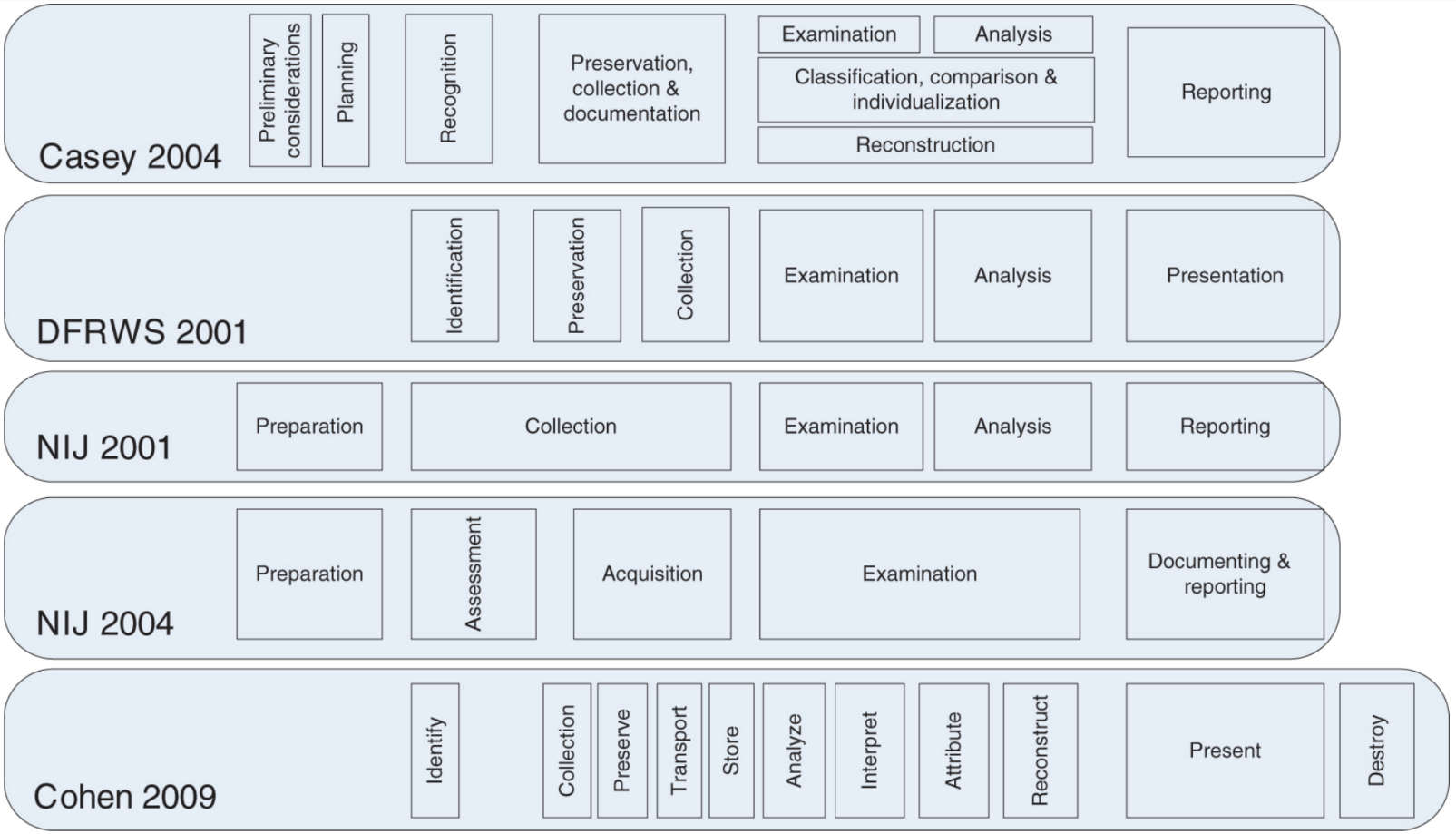
11. Generated Material

- Microsoft word document of Digital Forensic Report and Findings
- Evidence found on Exhibits

Alternative process models

- The Casey 2001 model expands the Kruse model to 6 steps:
  1. Identification / assessment
  2. Collection / acquisition
  3. Preservation
  4. Examination
  5. Analysis
  6. Reporting
- Main differences:
  - Emphasizes the importance (and process) of preserving the data
  - Distinguishes between the process of examination and analysis, whereas Kruse considered them to be two parts of a single process

Many different process models



- In general, end up being very complex and subtle

Some limitations of process models

- Complexity
  - Define many steps and cumbersome inter-relations
- Rigidness
  - In practice, most digital investigations do not proceed in linear fashion
- Incompleteness
  - Don't help digital investigators with some of the most important steps of each step of an investigation, including the completeness and repeatability of each step

The Scientific Method

Some limitations of process models

- In practice, digital investigators need to complement investigative models with simpler methodologies that:
  1. guide them in the right direction, while
  2. allowing them to maintain the flexibility to handle diverse situations
  3. and preserve the rigors of forensic science
- The scientific method provides such a simple, flexible methodology

Overview of the scientific method

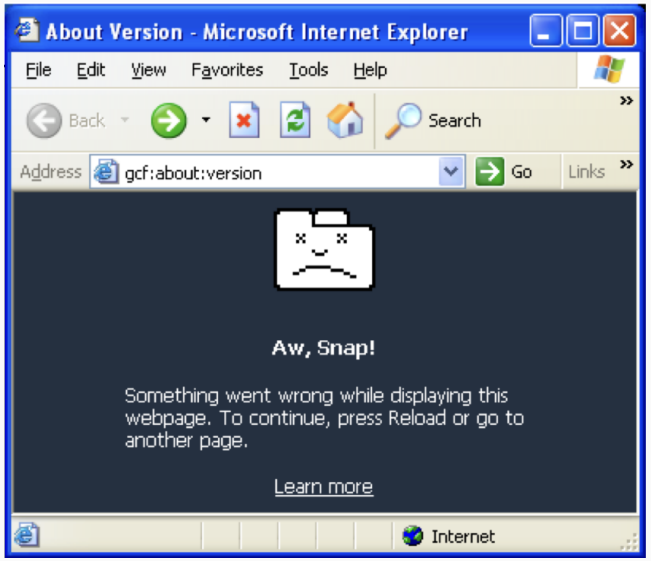
- Successful forensic examinations generally follow the scientific method:
  1. **Observation**
  2. **Hypothesis**
  3. **Testing**
  4. **Conclusions**

1. Observation

- Identify and research a problem
  - One or more events will occur that will initiate your investigation
  - Events which include observations that represent the initial incident's facts
  - Digital investigators proceed from these facts to form their investigation

Example

A user might have observed that his or her web browser crashed when she surfed to a specific Web site, and that an antivirus alert was triggered shortly afterward



2. Hypothesis

- Formulate a hypothesis and make a prediction
  - Based on the current facts of the incident, digital investigators will form a theory of what may have occurred, and then predict where the artifacts related to that event may be located

Example (cont.)

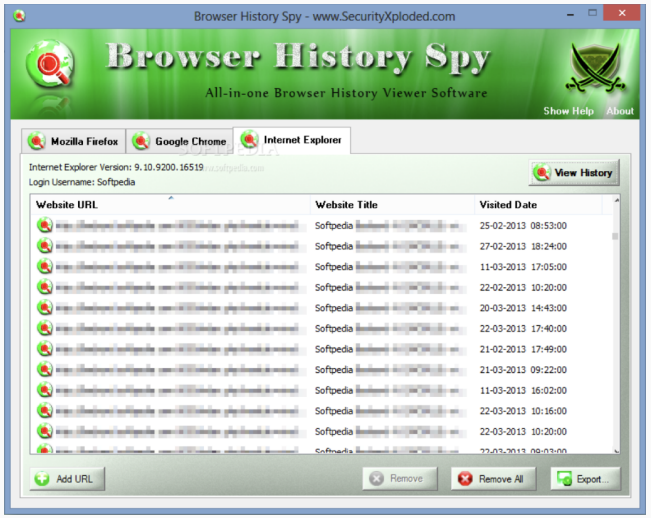
A digital investigator may hypothesize that the web site that crashed the user's web browser used a browser exploit to load a malicious executable onto the system. Using the hypothesis, and knowledge of the general operation of web browsers, operating systems, and viruses, a digital investigator may predict that there will be evidence of an executable download in the history of the web browser, and potentially, files related to the malware were created around the time of the incident.

3. Testing

- Conceptually and empirically test the hypothesis
  - Digital investigators will then analyze the available evidence to test the hypothesis, looking for the presence of the predicted artifacts

Example (cont.)

A digital investigator might create a forensic duplicate of the target system, and from that image extract the web browser history to check for executable downloads in the known timeframe



4. Conclusion

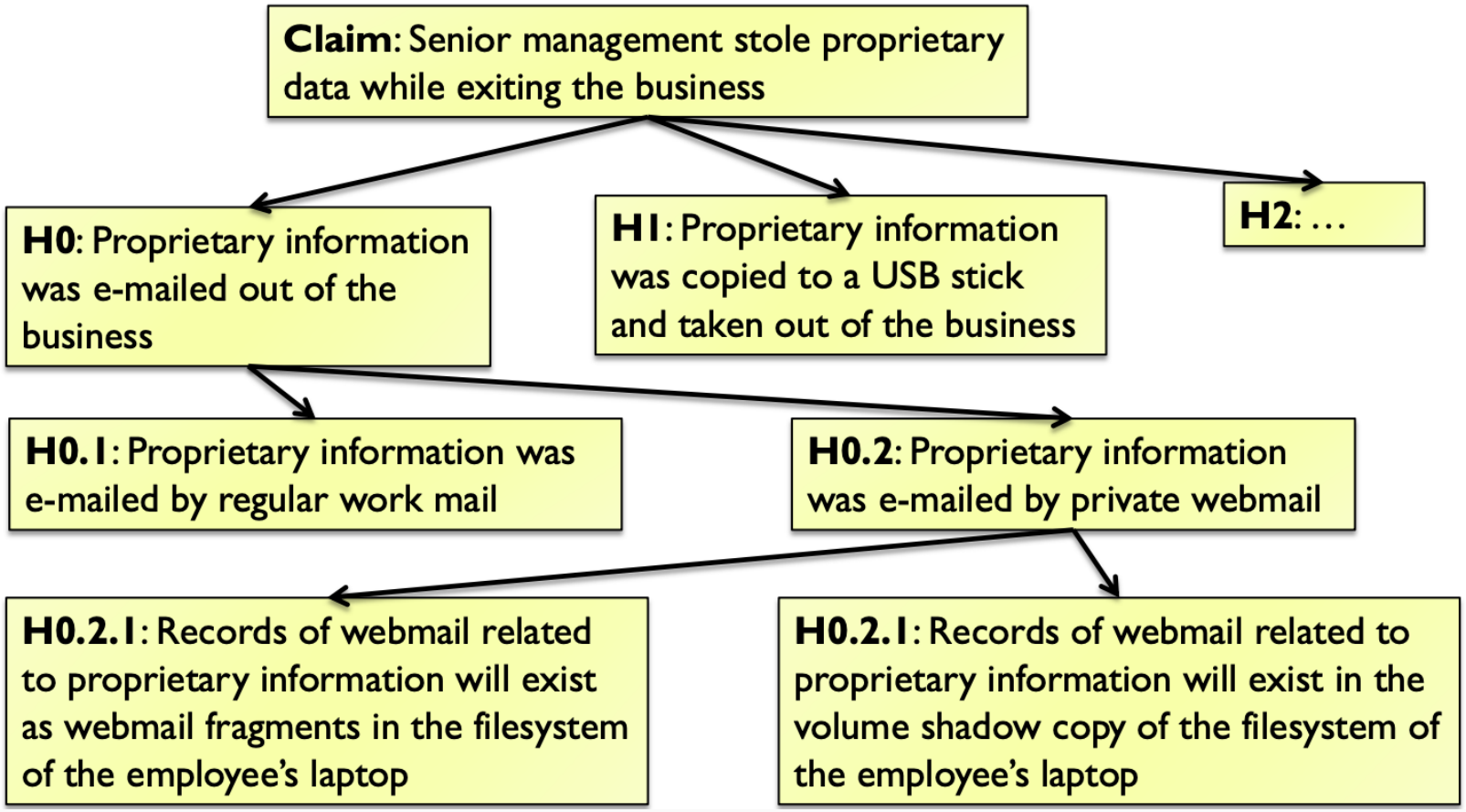
- Evaluate the hypothesis with regards to test results. If hypothesis is acceptable, evaluate its impact. If not, reevaluate the hypothesis
  - Digital investigators will then form a conclusion based upon the results of their findings
- A digital investigator may have found that:
  1. The evidence supports the hypothesis
  2. The evidence falsifies the hypothesis, or
  3. The evidence was inconclusive

Hypothesis unfolding

- Digital investigation are guided by identifying claims regarding events that have occurred which are relevant, and translating those claims into hypothesis
- Typically, these hypothesis will not be directly testable with regard to tracing evidence in the digital domain
- Hypothesis will need to be further translated into sub-hypotheses about which applications a user employed, and artifacts that applications leave behind

Example of hypothesis unfolding

- **Goal**: identifying theft of company proprietary information



The scientific method is useful in the entire process

- **Assessment phase**
  - E.g., in identifying the most likely sources of evidence based on the nature and circumstances of the crime (crucial in large networked systems)
- **Acquisition phase**
  - E.g., select pieces of digital evidence that may be relevant when the amounts of data are very large, the time available for collection is scarce, etc.
- **Analysis phase**
  - Highly important in this phase for extracting and looking relevant data and interpret the results

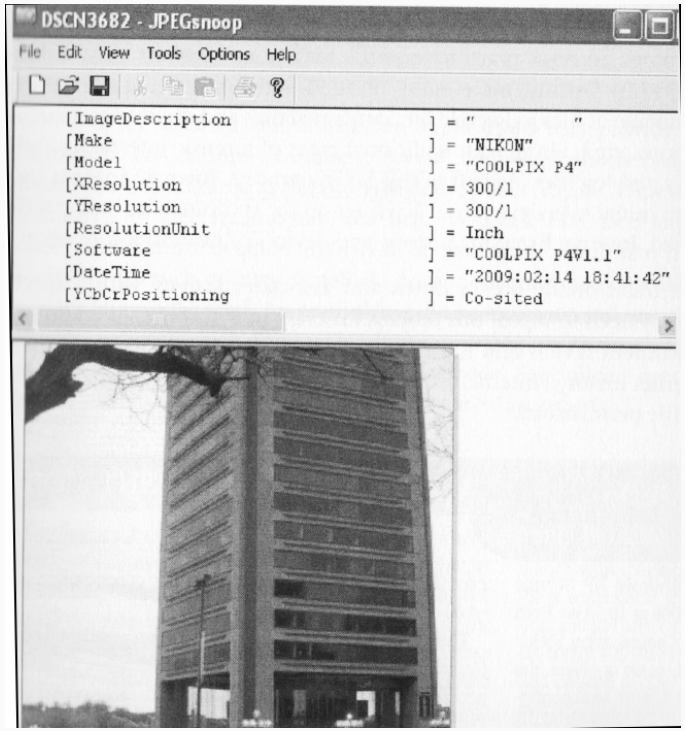
Baltimore case

- A suspect terrorist named "Roman" was observed purchasing explosive materials and investigators believe that he is involved in planning an attack in Baltimore, Maryland
- We have been asked to perform a forensic analysis of his laptop to determine the target of the attack and information that may lead to the identification of others involved in the terrorist plot

- What do we conclude from evidence (support, falsify, inconclusive)?
- Can you formulate alternative sub-hypotheses?

Evidence found: Embedded metadata

- 24 digital photographs were found in the folder `C:DocumentsandSettings\Roman\MyDocuments\MyPictures\ValentinesDay`
- Review of the header of these files using the JPEGsnoop tool, indicates they were digitized using a Nikon Coolpix P4 camera
- According to header information these images were digitized between 6:41 PM and 6:56 PM on February 14, 2009
- With a maximum of a two-second discrepancy, the File System Last Written dates on the subject system correlated to the EXIF header information



Evidence found: System config and usage

- The operating system was Microsoft Windows XP, Service Pack 3, (installed as SP2) December 22, 2008 at 10:10PM
- Both the Registered Owner and Registered Organization Fields contained "-" , and the assigned computer name "TEST13"
- The system was configured for "Eastern Standard Time" with an offset of -5 hours from GMT. The active time bias of acquisition was -4:00 offset from GMT
- The primary user account was "Roman", with a Logon Count of 22 and a Last Logon of May 23, 2009. This user account was not protected by a password.
- Utilizing Access-Data's Password Recovery Toolkit with associated Registry files (SAM/System) from the subject computer as input, the administrator account password was determined to be `L1b3r4t0r`.

Evidence found: Program files of interest

- On February 13, 2009, an installation file for Skype was created in the folder `C:\DocumentsandSettings\Roman\MyDocuments` folder, and the file `Vidalia-bundle-02.0.34-0.1.10.exe` was created in the same folder minutes later.
- This bundle included The Onion Router (Tor), an application that utilizes a network of virtual tunnels to help improve privacy and security, and Vidalia, a graphic user interface to Tor. Both Skype and Vidalia/Tor where installed on February 13, 2009
- Evidence of the existence of the file wiping utility Jetico BCWipe was detected on the subject system; however, there is no indication of recent use to overwrite data on the system

Evidence found: Internet access summary

- Web browsing activities were reconstructed from Firefox and Internet Explorer history, along with search hits in unallocated space for "`url:`", "`https://`" and "`file://`"
- On February 15, 2009 at 2:45PM, Firefox was used to access the account `bmoragent@hushmail.com`, which is a free privacy-enhanced web-based e-mail service
- Five minutes later, at 2:50 PM, the user executed a Google search for "check ip address". Subsequently the user accessed `http://whatismyipaddress.com` with a web page title of Lookup IP, Hide IP, Change IP, Trace IP, and more...

Evidence found: Internet access summary

- On March 19, 2009 at 12:32 PM, Firefox was used to execute a Google search for "WorldTrade Center Baltimore building plans" with subsequent access to the file `www.marylandports.com/opsalert/eBroadcast/2008/HPPwtc2008.pdf`
- Subsequently, at 1:18 PM, Internet Explorer and file system activity reflect access to the web page Account is Now Active at `www.gunbroker.com`
- The content of this page in conjunction with an earlier redirect page suggests the user received a `gunbroker.com` account activation e-mail at `bmoreagent@hushmail.me`

Evidence found: Embedded metadata

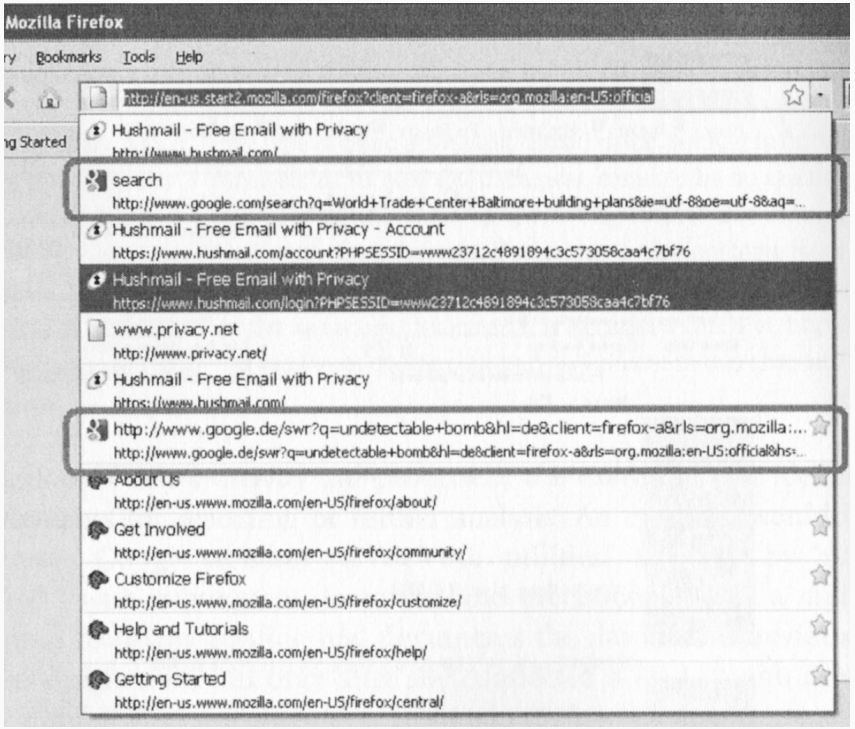
- After logging into the Gunbroker.com website, the user accessed the auction web page for a weapon: `www.gunbroker.com/Auction/ViewItem.asp?Item=125130891`, (SIGARMS, P229, 9MM, NIGHT SIGHTS, 13RD, 2 MAGS)
- The user then viewed a list of auctions for semi-automatic guns – the reconstructed web page is shown on the right

Evidence found: Web browsing artifacts

Following are some images from the Internet Explorer cache. Knowing that the individual has reviewed weapons sites, conducted searches on terms such as liquid explosives and undetectable bombs, one might see the image of the Coast Guard ship and make an assumption that the user may also be interested in targeting it.

Evidence found: Internet access summary

- On March 19, 2009 at 1:19PM, the user accessed a web page on Gunbroker.com to "Ask Seller A Question - Send Mail to User" for the specific auction item 125288486
- On March 20, 2009 at 12:00PM, a Firefox 3 Bookmark was created concerning a Google search for "undetectable bomb"
- Checking Mozilla Firefox in a virtualized clone of the subject system confirmed recent entries:

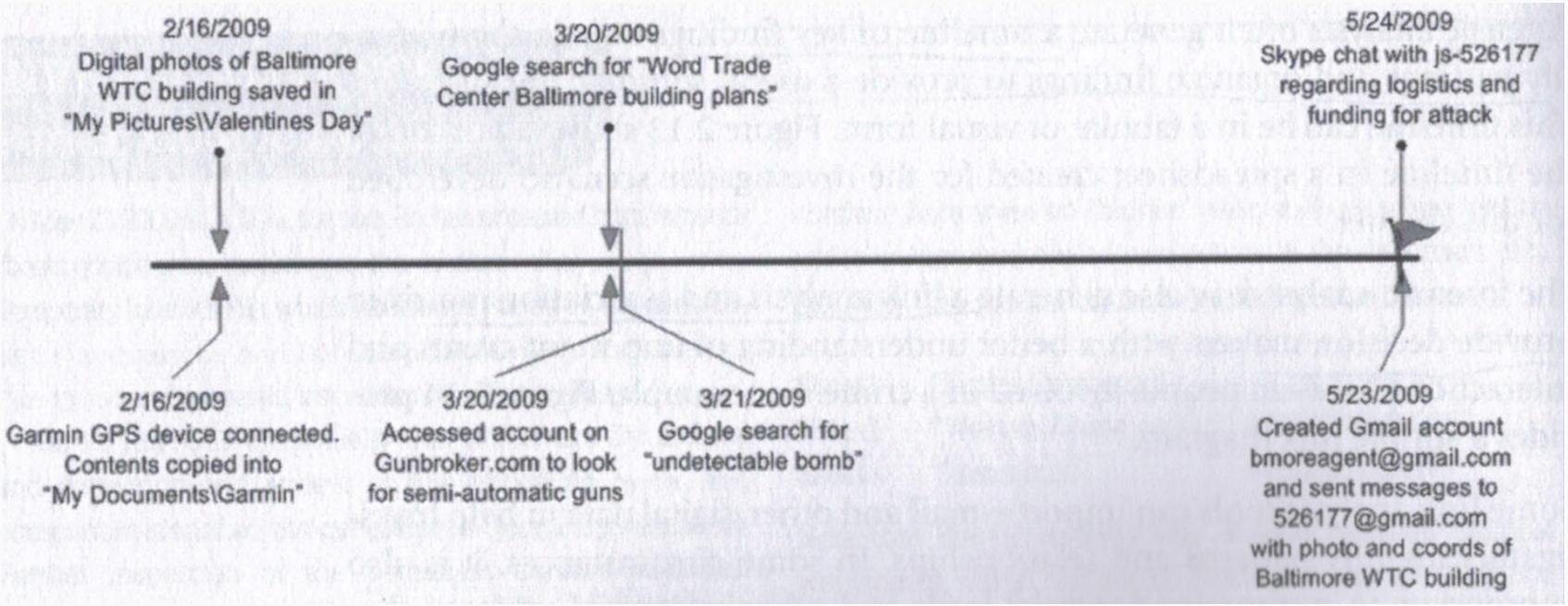


Baltimore: Skype chat log

Unix Numeric Value	Date/Time (Converted)	User	Name	Message
1243102641	Sat, 23 May 2009 14:17:21 -0400	bmoreagent	bmoreagent	Bmore agent here
1243102672	Sat, 23 May 2009 14:17:52 -0400	js-526177	John Smith	Operational status?
1243102695	Sat, 23 May 2009 14:18:15 -0400	bmoreagent	bmoreagent	Target selected and all plans in place.
1243102741	Sat, 23 May 2009 14:19:01 -0400	js-526177	John Smith	Please e-mail the target confirmation details to 526177@ gmail.com. This account won't be checked again after today.
1243102812	Sat, 23 May 2009 14:20:12 -0400	bmoreagent	bmoreagent	Will do. All that is needed for execution is final approval and funding.
1243102980	Sat, 23 May 2009 14:23:00 -0400	bmoreagent	bmoreagent	Here is a photograph of target location (coordinates lat ="39.286130" lon ="-76.609936")
1243103004	Sat, 23 May 2009 14:23:24 -0400	bmoreagent	bmoreagent	sent file "DSCN3684.JPG"<files alt=""><file size="1641245" index="0">DSCN3684.JPG</file></files>
1243103084	Sat, 23 May 2009 14:24:44 -0400	js-526177	John Smith	Action authorized and approved. Western Union code 170236723-00348. Use the ID card we previously coordinated. Also, you'll need to provide the password "Be3Ready2Serve" to pickup the cash.
1243103190	Sat, 23 May 2009 14:26:30 -0400	js-526177	John Smith	Received image. Target acknowledged.

Baltimore case (cont.)

- The seized computer contained minimal and selective use, with relevant activity ranging from approximately February 13, 2009 to May 24, 2009. A timeline of important events is provided:



Takeaways

- Digital investigation process models are very important to ensure admissibility of digital evidence
- The scientific method helps to guide digital investigations throughout the investigation process, especially in the analysis stage
- Document everything so that others can reproduce your results!

Pointers

- **Textbook:**
  - Casey – Chapters 6 & 8.1.1
- **Other resources:**
  - The Anatomy of a Digital Investigation
  - ACPO
  - NIJ04
  - Crawford15
- **Acknowledgements:**
  - Slides adapted from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon