UNIVERSITY OF PLYMOUTH

Digital Forensics

Dr Hai-Van Dang

Centre for Security, Communications and Network Research

Learning outcome checklist

1. See the difference between digital investigation and digital forensics investigation [1]
2. Recognize where digital forensics can help
3. Understand how scientific method is applied in digital forensics investigation [2]
4. Understand phases of a forensics process [3]
5. Understand what are expected while acquisition [4]
6. Examination/analysis [5]
7. Understand how file carving works [6]
8. Understand the requirements of a report/presentation

References

1. https://www.youtube.com/watch?v=m3W87r6MO8c&list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD&index=16
2. https://www.youtube.com/watch?v=UYxKdcGBSx4&list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD&index=17
3. https://www.youtube.com/watch?v=ZTZ_GnFR-GE&list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD&index=18
4. Clarke, Nathan. "Computer Forensics: A Pocket Guide", chapter 3
5. Clarke, Nathan. "Computer Forensics: A Pocket Guide", chapter 4
6. https://resources.infosecinstitute.com/topic/file-carving/
7. https://www.youtube.com/watch?v=tsRLGHzo79w&list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD&index=26

Session Content

Introduction to Digital Forensics

Forensic Process & Methodology

Forensic Laboratory

Acquisition

Examination & Analysis

Proactive Forensics

Anti-Forensics

Conclusions

Introduction to Digital Forensics

What are differences in the two scenarios?

menti

1. Forensics investigator Alice recovers files on her personal computer.
2. Forensics investigator Alice recovers files on a suspect’s computer.

Examples

- Emotet botnet taken down by international police swoop : "Police from the UK, EU, US and Canada worked together to "disrupt" Emotet"
- US Military Contractors 'Hit by Chinese Hackers'- US : "A year-long investigation was concluded in March, but the findings have only just been made public."
- Cybercrime: 'Illegal' SIMs Seller Gets Six Years – India
- Cybercrime in 2025: Where do you go when there's nowhere to hide – Philippines
- Cybercrime Law Threats Freedom of Speech in Qatar
- eBay Flaw has existed for Months –US/Global
- Israel launches National Cyber-Defense Authority

Why do we need to investigate?

Menti.com

Image: https://www.theguardian.com/books/2021/feb/04/i-think-ive-written-more-sherlock-holmes-than-even-conan-doyle-the-ongoing-fight-to-reimagine-holmes

Why do we need to investigate?

https://www.bbc.co.uk/programmes/p078tr3w

In which case would digital forensics help? (1/2)

1. A got suspected of computer intrusion by having tricked the victim B into giving up the credentials to his Web site. A had then used the credentials to modify B’s Web site in malicious ways and later destroy it completely.
2. In a murder case, the suspect had shot a person. There were some pieces of evidence pointing to the suspect, but he was given alibi. by his girlfriend who said that he was at home at the time of the crime. Home in this case was about 90 min away from the murder site, by car.
3. An employee of a company was suspected of placing a Trojan horse in the company network. The employment had been terminated, and the suspicion was that the employee had placed a Trojan horse to get back at the company for sacking him.

In which case would digital forensics help? (2/2)

4. A new start-up SME (small-medium enterprise) based in Luton with an E-government model has recently begun to notice anomalies in its accounting and product records. It has undertaken an initial check of system log files, and there are a number of suspicious entries and IP addresses with a large amount of data being sent outside the company firewall. They have also recently received a number of customer complaints saying that there is often a strange message displayed during order processing, and they are often re-directed to a payment page that does not look legitimate.

Why do we need to investigate?

- Recover damages/monetary compensation
- Bring culprits to justice
- Make sure it does not happen again!
  - Take remedial action
- Prevent leakage of confidential information
- Prove innocence

Example

- A man was accused of backdating a document to cover up alleged environmental violations. Forensic analysis of his computer and e-mail, as well as the e-mail of his attorney, all combined to show that the document had not been fabricated. They had simply used a prior document as a template and had forgotten to update the date typed at the top of the page.

The need for Forensics

menti

- National Security
- Information Security
- Corporate Espionage
- White Collar Crime
- Child Pornography
- Traditional Crime
- Incident Response
- Employee Monitoring
- Privacy Issues

Definition

- Digital Forensic Science (DFS):

“The use of **scientifically** derived and proven methods toward the **preservation, collection, validation, identification, analysis, interpretation, documentation and presentation** of **digital evidence** derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Source: Digital Forensic Research Workshop (DFRWS), 2001

Possible bias in investigation

- Bias from personal beliefs
  - very emotional cases
  - influence from media/ social media
- Bias from cultural beliefs
- How to avoid bias (and subjectivity)?

Applying scientific method to digital forensics investigation

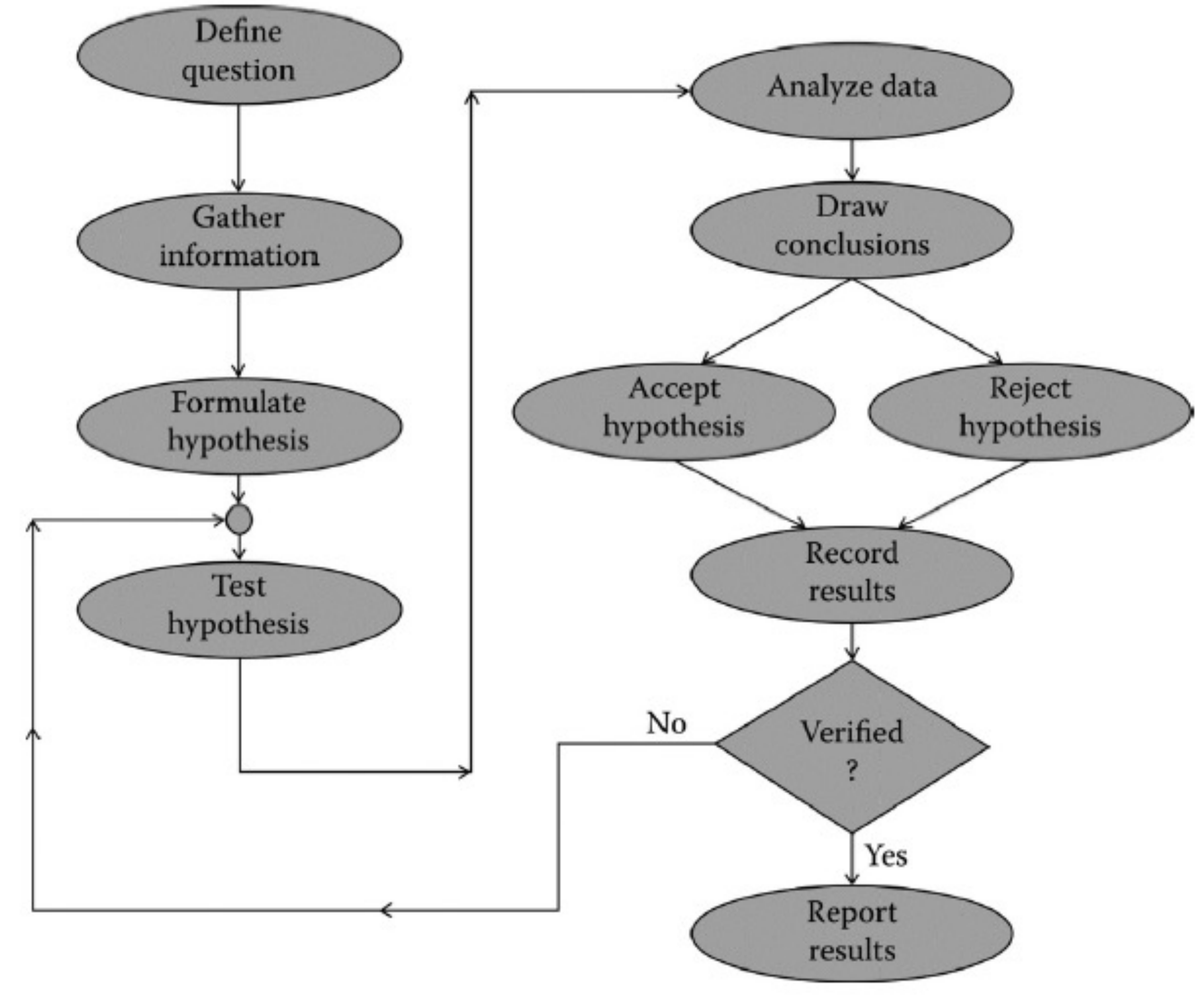


Figure 1.1 The scientific process.

The scientific method is the application of a set of **accepted** and **verifiable** steps to investigate a question or problem

Ref: Gogolin, Greg, ed. *Digital forensics explained*. CRC Press, 2021 (page 3, 15)

Which is a better question and why?

menti

1. Is there something illegal in the suspect’s computer?
2. Was the computer used by a human to process stalking photos of the victim?

Define question

1. What is the investigating member trying to prove, exactly?
2. What questions will the defense likely ask?

Gather information

Gather relevant information

- what type of case: hacking, child exploitation, financial thief;
- profile of the suspect: their digital capabilities, their working time;
- any other suspect(s): who else can access the computers;
- available and accessible data for investigation;
- …

Form hypotheses

Question: Was the computer used by a human to process stalking photos of the victim?

- H1: A human copied stalking photos into the computer from an external device
- H2: A human downloaded the stalking photos using a web browser
- H3: A virus downloaded the stalking photos

...

Form your hypotheses from the following question

menti

- Defined question: “Was the computer used by a human to download illegal images?”
- What hypotheses will you form?

Test hypothesis

Prerequisite: Knowledge of a system (operating system, devices,…) to know how evidences might be created: If we have a Windows XP computer like the suspect, we would like to figure out what it looks like if we downloaded photos from a browser.

- Go look at the suspect’s computer and look for the same traces
- Analyse the data in forensic sound manner

Where would you look for evidences?

menti

- H2: A human downloaded the stalking photos using a web browser
- H3: A virus downloaded the stalking photos

Conclusion about the hypothesis

Can we conclude a hypothesis is 100% true (or 100% false)?

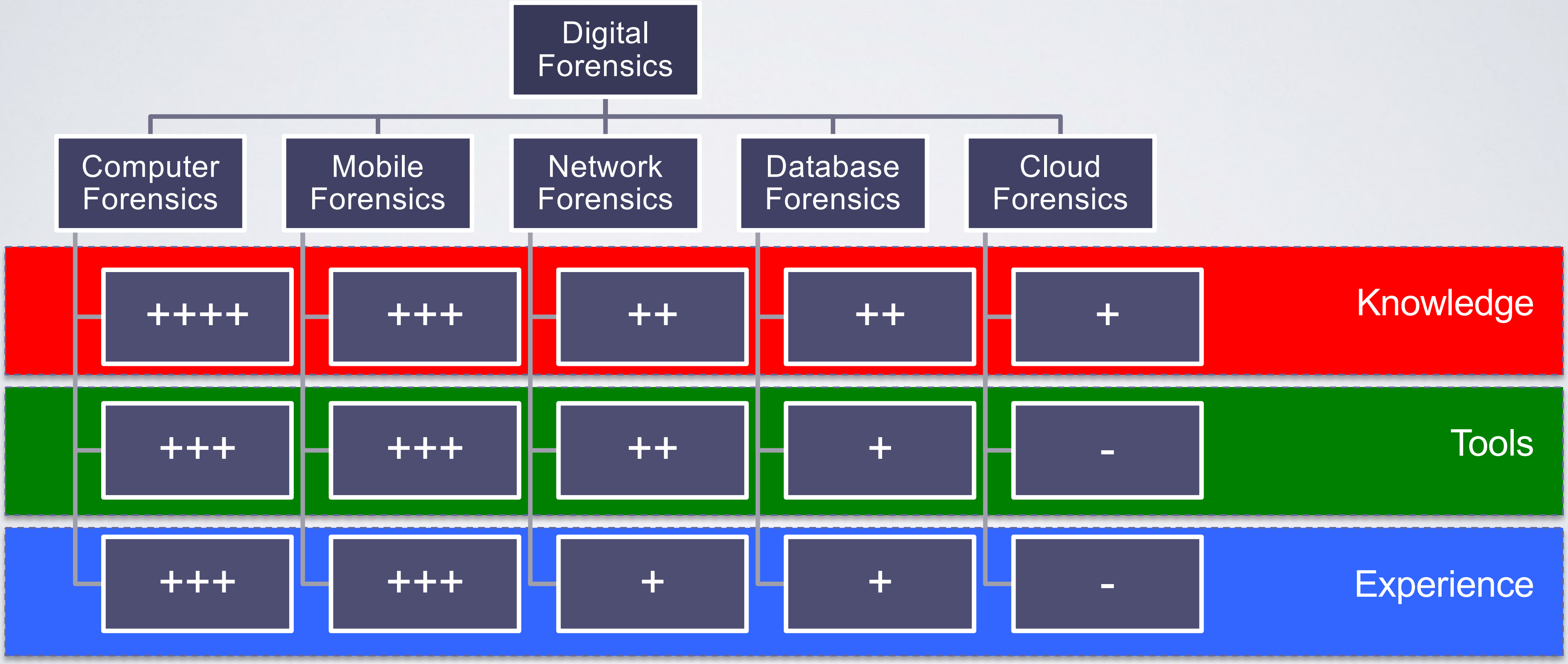
Conclusion about the hypothesis

No conclusion 100% definitely happened.

Found evidence increases or decrease the **probability** of a hypothesis.

Example: Some evidence to **support** that Internet Explorer was used by a human to download suspected illegal images.

Taxonomy



Digital Forensics

	Computer Forensics	Mobile Forensics	Network Forensics	Database Forensics	Cloud Forensics
Knowledge	++++	+++	++	++	+
Tools	+++	+++	++	+	-
Experience	+++	+++	+	+	-

Forensics – A reactive Process!

- Forensics is a reactive *not* proactive!
- Other tools are utilized to detect if a problem exists:
  - Intrusion Detection
  - Incident Response
  - Skilled administrators or security professionals
  - System acting weird..☺
- Digital forensic vendors are however moving into the proactive space!
  - Guidance Software

Forensic Process & Methodology

Standards & Guidelines

- ISO 27037 – Guidelines for Identification, Collection and/or Acquisition and Preservation of Digital Evidence
- ISO 27041 – Guidance on Assuring Suitability and Adequacy of Incident Investigative Method
- ISO 27042 – Guidelines for the Analysis and Interpretation of Digital Evidence
- ISO 27043 – Incident Investigation Principles and Processes
- NIST – Guideline to Cell Phone Forensics
- NIST – Guideline to Mobile Device Forensics
- NIST – Guide to Integrating Forensic Techniques into Incident Response
- CERT – First Responders Guide to Computer Forensics
- Association of Chief Police Officers (ACPO) – Good Practice Guide for Digital Evidence

ACPO Guidelines

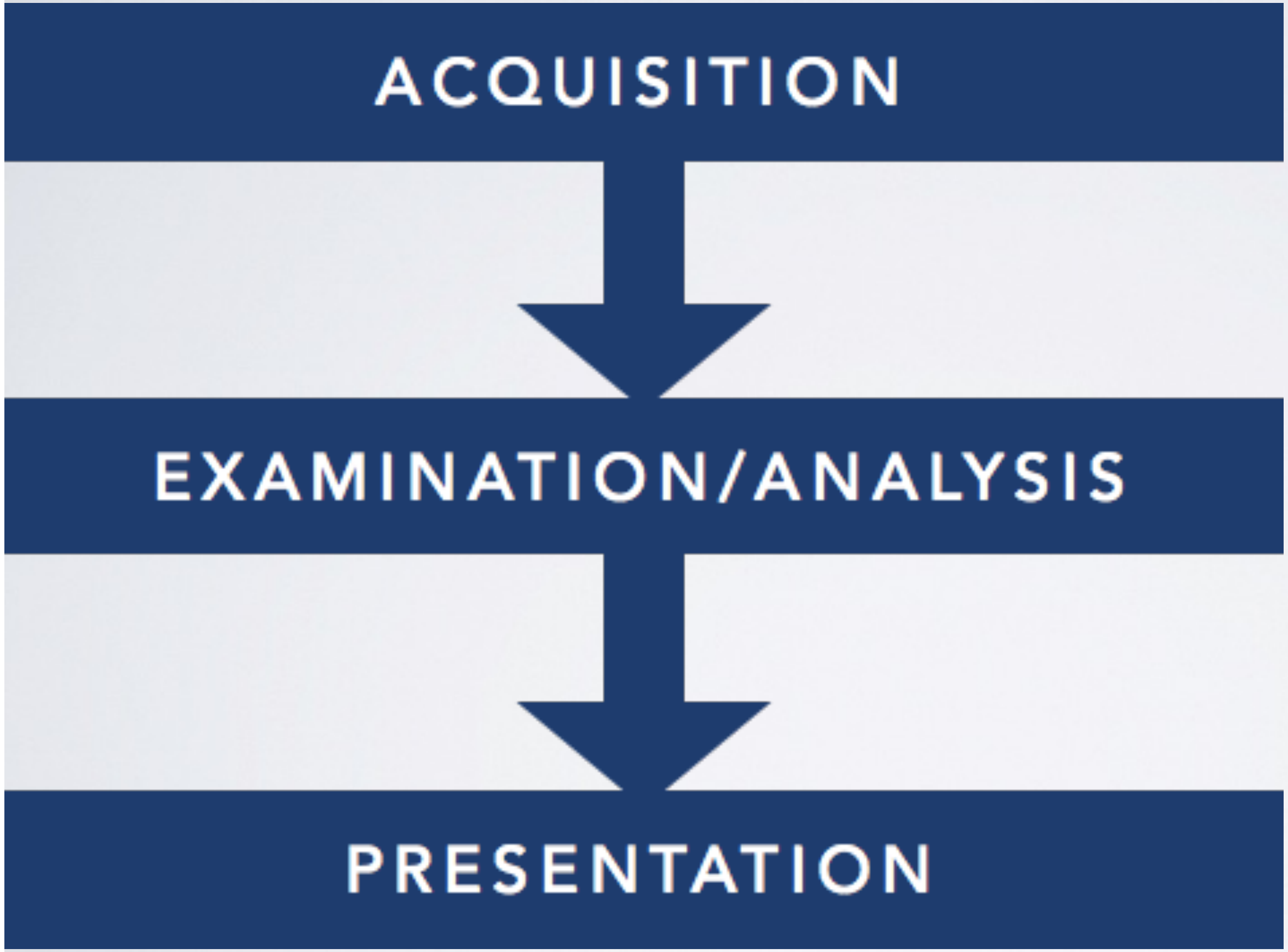
- Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

- Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and implications of their actions

- Principle 3: An audit trial or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result

- Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to

Forensic Process



ACQUISITION

Acquire data without altering or damaging the data (if possible)

Verify recovered data as the same as the original

EXAMINATION/ANALYSIS

Analyze the data without modifying it

PRESENTATION

Clearly report and present findings

Forensic Methodology

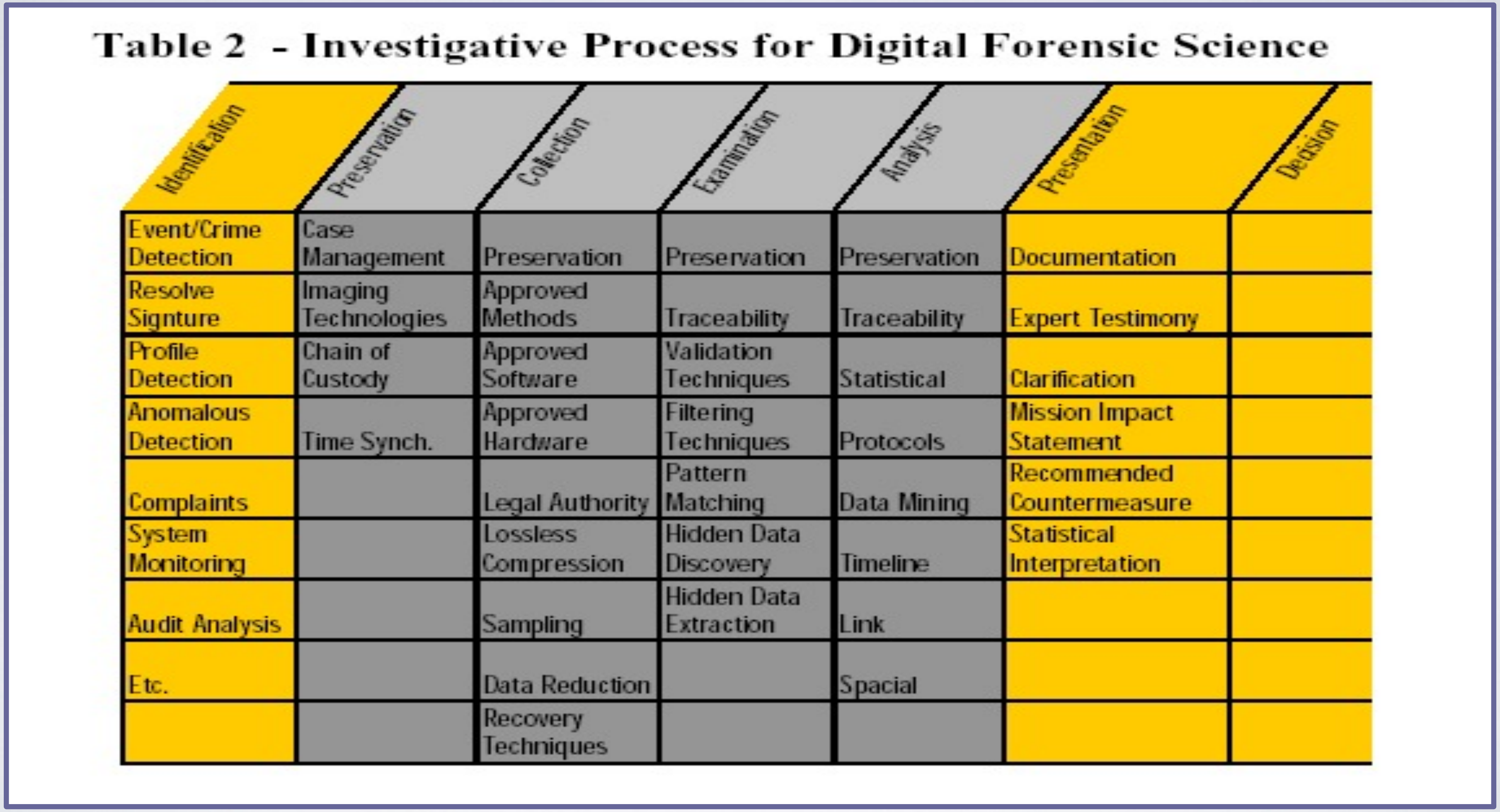


Table 2 - Investigative Process for Digital Forensic Science

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Source: Digital Forensic Workshop, 2001

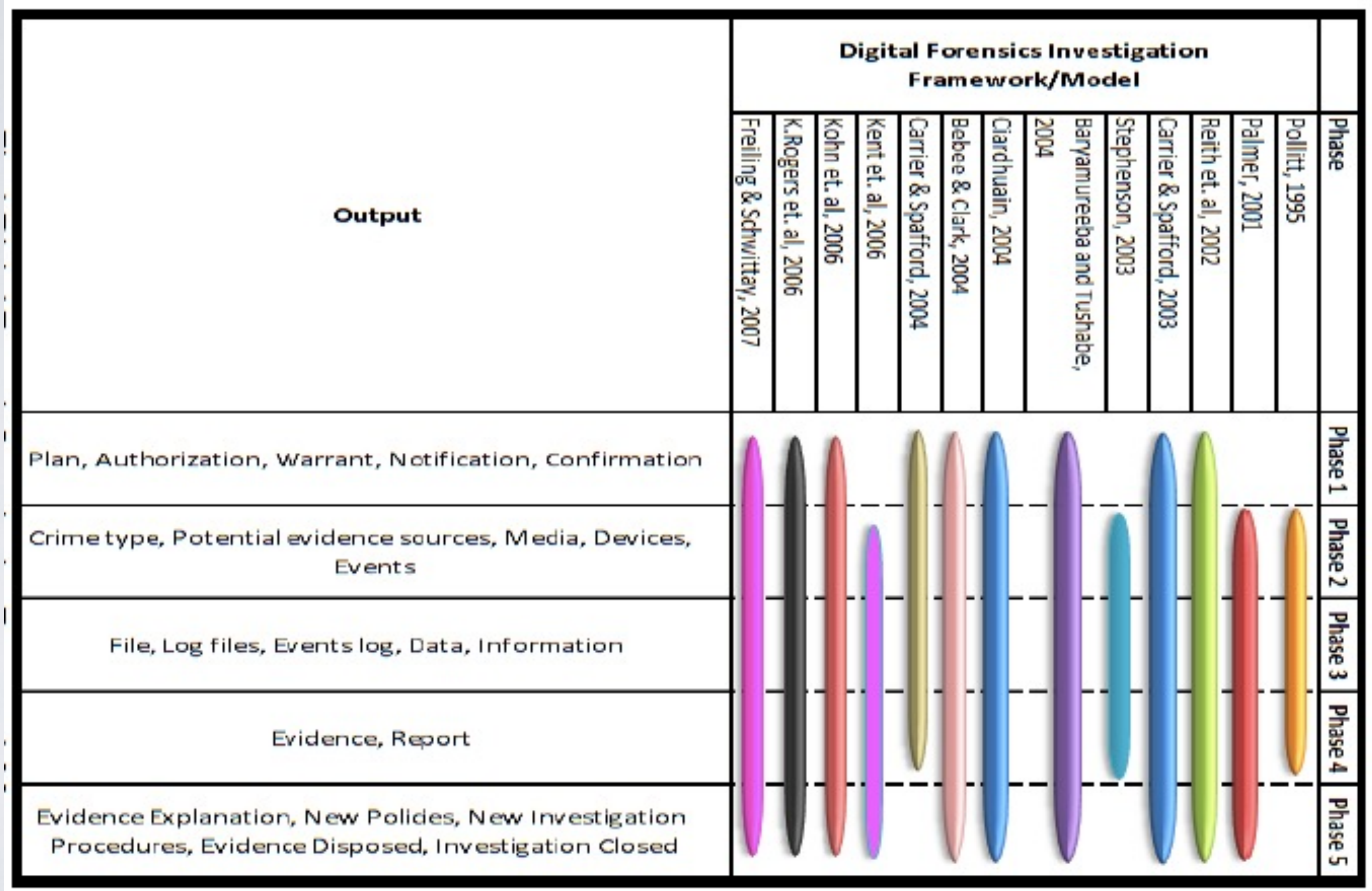
Digital Forensics process

1. Identification – the initial identification that something is wrong and requires forensic investigation.
2. Preservation – to ensure data is acquired in a forensically sound manner with an appropriate chain of custody being maintained.
3. Collection – the use of approved software and hardware and appropriate legal authority where necessary in collecting the evidence.

Digital Forensics process (cont)

4. Examination – through the use of filtering and data extraction techniques identify artefacts of interest.
5. Analysis – understand the chronology of events and link together artefacts in order to understand the complete picture.
6. Presentation – document and present the findings in an appropriate manner.
7. Decision – in a legal situation this would be whether sufficient evidence exists to proceed with a criminal case. Within an organisational environment, it could be the point at which a decision is made to proceed with civil proceedings or an action is taken against an employee.

Forensic Methodology



Output	Digital Forensics Investigation Framework/Model													Phase
	Freiling & Schwittay, 2007	K.Rogers et. al, 2006	Kohn et. al, 2006	Kent et. al, 2006	Carrier & Spafford, 2004	Bebee & Clark, 2004	Ciardhuain, 2004	Baryamureeba and Tushabe, 2004	Stephenson, 2003	Carrier & Spafford, 2003	Reith et. al, 2002	Palmer, 2001	Pollitt, 1995	
Plan, Authorization, Warrant, Notification, Confirmation	●	●	●		●	●	●	●		●	●			Phase 1
Crime type, Potential evidence sources, Media, Devices, Events	●	●	●	●	●	●	●	●	●	●	●	●	●	Phase 2
File, Log files, Events log, Data, Information	●	●	●	●	●	●	●	●	●	●	●	●	●	Phase 3
Evidence, Report	●	●	●	●	●	●	●	●	●	●	●	●	●	Phase 4
Evidence Explanation, New Policies, New Investigation Procedures, Evidence Disposed, Investigation Closed	●	●	●	●		●	●	●		●	●	●		Phase 5

Source: Mapping Process of Digital Forensic Investigation Frameworks" – Selamat, Yusof, and Sahib [IJCSNS Vol 8 No 10, Oct 2008]

Proactive Forensics

- Whilst forensics is inherently reactive, it is far more efficient to be proactive in the approach
- Planning is essential!
  - Minimize number of supported Operating and File Systems
  - Enable comprehensive logging on systems
  - Ensure systems are supported with the available forensic tools (RAID configurations!)
  - Prior thought to acquisition considerations - physical equipment required, acquisition time
  - Develop appropriate policies and procedures (for every eventuality!)

Forensic Laboratory

Lab Requirements

- ISO/IEC 17025:2005 – Accreditation of the digital forensics discipline
- Compliance to digital forensics procedures
- Chain of custody
- Secure handling and storage of original data – lockable room/safe
- Ensure screens are not viewable by others
- Physical building complies with security requirements (depending upon the nature of the organisation)

Equipment Requirements

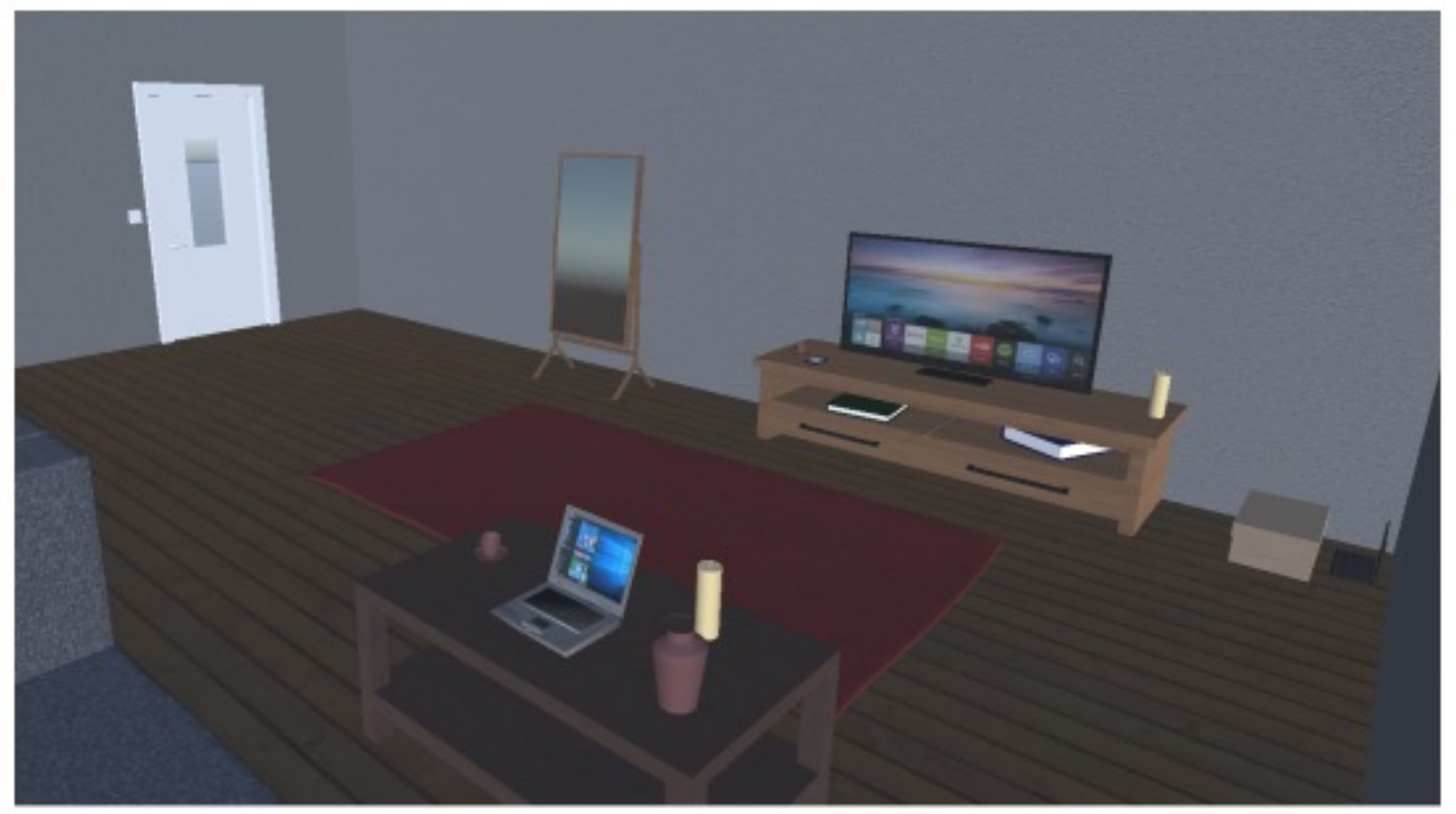
- Dependant on the organisational requirements
- Closed network – yet requirement to ensure software is patched
- Acquisition system – independent of the analysis workstations – hardware write blockers, cables, software – communication speed is the bottleneck
- Analysis system – Extremely high spec PC – forensic software and tools - hard drive speed is the bottleneck
  - Mac Pro 3.7GHz Quad Core, 32GB, 8TB Thunderbolt 2 Stripped (RAID 0)
- Short-term and long-term storage of forensic images

Person Specification

- Technical knowledge and awareness
  - Hardware, software, file systems, operating systems, applications, desktops, laptops, mobile phones, network architectures, applications
- Knowing the implications of your actions
- Understand how data can be modified
- Clever, curious and open minded
- Extremely ethical
- Degree in computer science? Traditionally no!

Acquisition

Identify what to acquire for digital evidence



Menti,

Image: Karabiyik, Umit, et al. "A virtual reality framework for training incident first responders and digital forensic investigators." *International Symposium on Visual Computing*. Springer, Cham, 2019.

Considerations

- How can we preserve all the data?
- How can we preserve the best possible copy of data?
- How can we ensure the acquired data is correct?
- How can we ensure the acquired data can be verified by a third party?

Considerations

- To make sure that no alterations are made to the original evidence
  - **write blockers** are used when connecting a piece of digital evidence to a computer
  - (forensics sound) **imaging** is used to create an exact replica of the original
  - **cryptographic hashing** is used to validate a copy to be an exact duplicate of the original

Example

- An examination was conducted in August 2022, of the Hewlett Packard Desktop Tower dc6000MT DZ446A4 2UB198041R running Windows 10 sp3 build.08513-211 with an accurate BIOS time/date configuration. Further, technical characteristics are listed subsequently in the Administrative Information portion of this report. This investigation was conducted using EnCase Forensic version 8.13 with a Tableau T35es **write blocker** with serial number TB352322. The **MD5 hash of the original drive** was 004fsbf5fe806f- 41ca4ef4e556a8a8e9. The **MD5 hash of the acquisition/image** was 004fsbf5fe-806f41ca4ef4e556a8a8e9.

Write blocker

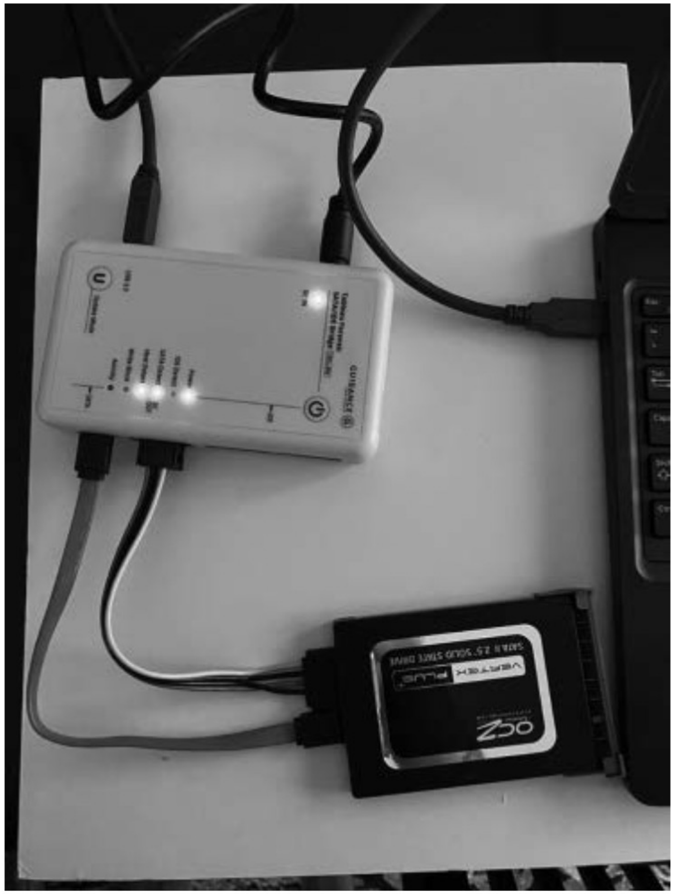


Figure 3.3 Tableau write blocker.

- Write blockers ensure that data are not altered when accessed.

Imaging

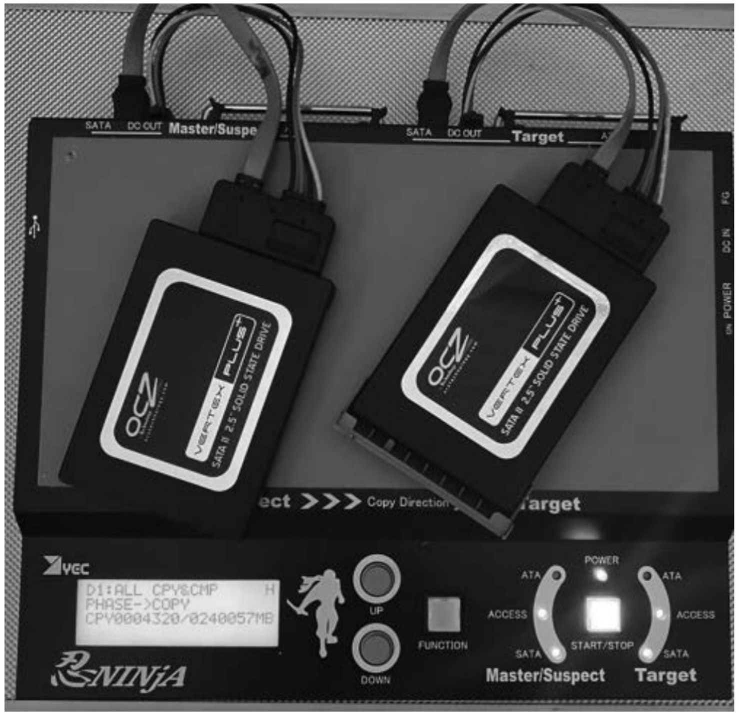


Figure 3.4 Ninja disk imager.

- Imaging is taking a **bit for bit copy** that is an exact replica of the original.
- With imaging, the copy can be **validated** to be an exact duplicate of the original by using hash algorithms such as **Message Digest 5 (MD5) or Secure Hash Algorithm (SHA).**

In which case, the copy is an exact duplicate of the original?

1. The MD5 hash of the original drive was 004fsbf5fe806f41ca4ef4e556a8a8e9.

The MD5 hash of the acquisition/image was 004fsbf5fe806f41ca4ef4e556a8a8e9.

2. The MD5 hash of the original drive was 004fsbf5fe806f41ca4ef4e556a8a8e9.

The MD5 hash of the acquisition/image was 004fsbf5fe806f41ca4ef4e556a8a7e9.

Imaging a damaged media

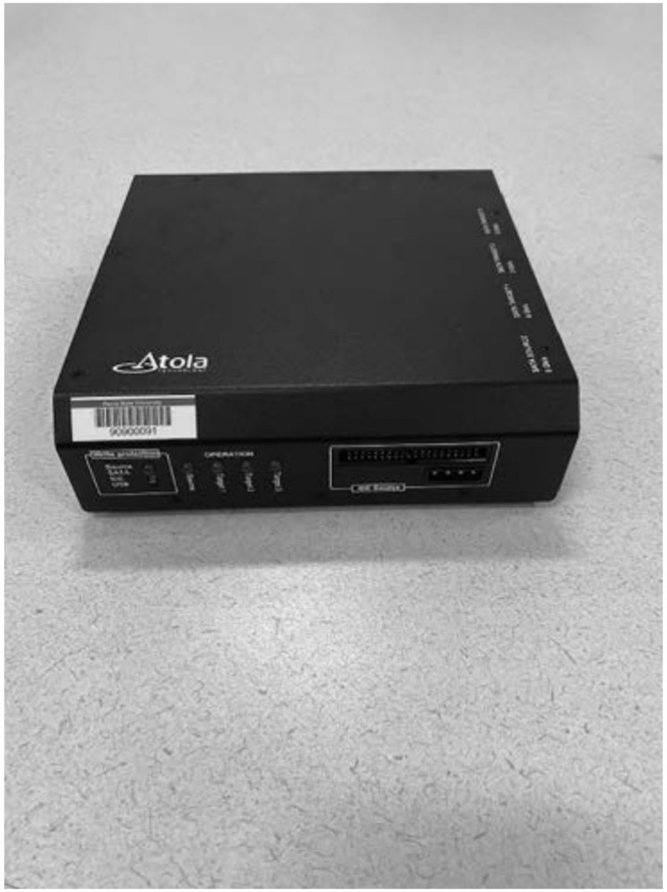


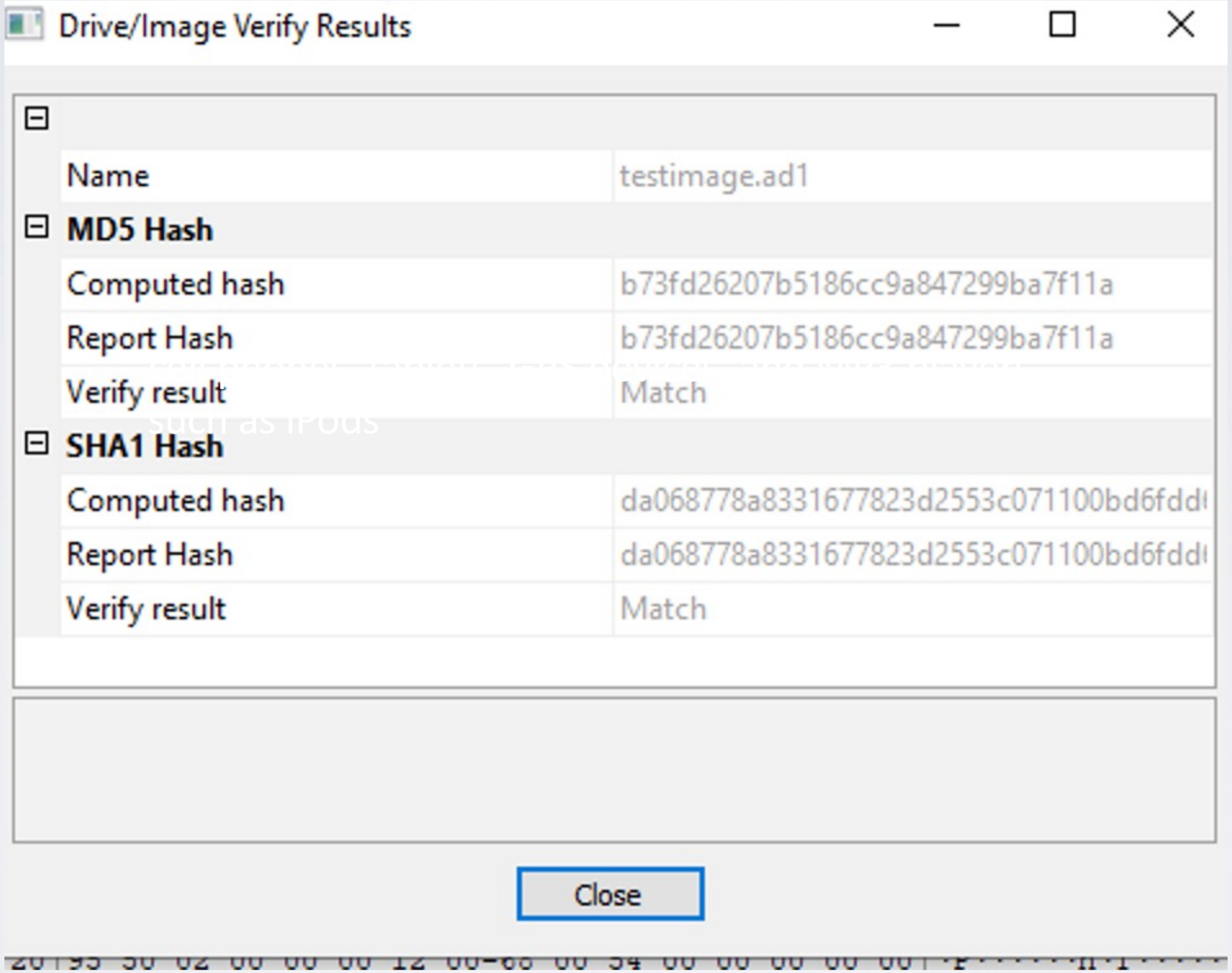
Figure 3.5 Atola Insight Forensic.

A specialized imaging tool for recovering data from damaged media. Specialized imaging tools will attempt to **read all of the areas that are not impacted by the head crash rather than just producing a read failure** for the entire drive

Considerations

- Imaging can take a considerable amount time. It depends on the speed of the drives, verification and the method used. If an estimate of 100GB per hour is a rough benchmark, imaging 1 terabyte drive will takes 10 hours.

Demo – Imaging with FTK imager



Drive/Image Verify Results

Name	testimage.ad1
MD5 Hash	
Computed hash	b73fd26207b5186cc9a847299ba7f11a
Report Hash	b73fd26207b5186cc9a847299ba7f11a
Verify result	Match
SHA1 Hash	
Computed hash	da068778a8331677823d2553c071100bd6fdd
Report Hash	da068778a8331677823d2553c071100bd6fdd
Verify result	Match

Live acquisition or not?

- Would you conduct live acquisition or not, and why?
- menti

Considerations

- Would there be any damage by keeping the machine running? Examples: include a process running on the machine that is forensically wiping the hard drive, a virus or worm that is corrupting data, or a machine being used to attack another system.
- If not, they typically perform a live acquisition and analysis to avoid losing volatile data
- Once the live analysis is complete, the system can be powered down and taken to the forensic laboratory for acquisition of non-volatile memory.

Which is volatile media?

- menti

Volatile data acquisition

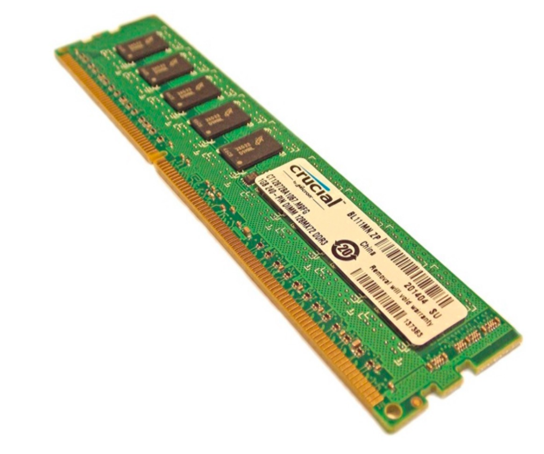


Figure 3.14 RAM chip

When a computer is powered off, the contents of RAM (Random Access Memory) are generally erased.

When a computer is on, volatile data can be extracted. Ex:

- processes currently running on a computer
- Evidentiary files and data related to Internet searches and websites visited
- User's current activity: open files, and active network connections
- If any of the active hard drives are encrypted. If so, decrypted data can be extracted when the computer is on

Acquisition

- Preservation of data essential
- Documentation and chain of custody
- Order of volatility
- Range of options available - full disk acquisition, sensitive files, live analysis tools
- Hardware write blocker
- Time consuming process - implications for operations

Examination & Analysis

What traces/ data would you look at?

- (menti) You are a computer forensics investigator in local law enforcement and have been assigned to a criminal investigation. The suspect, Michael Murphy, worked as the director of product development for a computer software company. He was questioned about a number of expensive international telephone calls. Further inspection of his telephone records revealed that he had been calling a software development competitor based in China with offices here in the United States. When confronted, he stated that he would need to consult with his lawyer and had no further comment. He did not show up for work the next day. The local authorities were contacted the following day. Murphy was caught trying to board a one-way flight to Beijing two days after being questioned about his contact with a competitor. At the airport, TSA officials discovered a bag filled with CDs, three SATA hard drives, and five USB thumb drives.
- Detail potential types of digital evidence you will need for this investigation.

Where/ what to examine?

- Assuming the suspect’s computer is running Windows OS.
- Where/ what would you look at?
- menti

Where/ what to examine?

Depending on the context, the device, the OS and the case. Examples:

- Files in Downloads folder
- Files in Desktop folder
- My Documents
- Recycle bin
- Deleted files
- Hidden files
- Files with extensions different from files format
- Files in browsers cache, temporary
- Email clients
- Messaging clients
- Windows registry entries
- TypeURLs registry entries
- Images
- Database
- RAM
- Pagefile.sys

Where/ what not to examine?

- Many trusted system files, application files

Deleted files scenarios

1. The file system still contains the record with all metadata and file data.
2. The file system contains the record with metadata, but the file contents themselves have been overwritten.
3. The file system no longer contains the record with metadata, but the file contents still exist on the image.

Recover deleted files

1. Recovering files from Recycle bin
2. Recovering files deleted from the MFT (master file table) in NTFS (new technology file system)
3. Recover files using File carving: find files that cannot just be restored using (1,2). Reasons for why a file cannot be restored can be that pointers to where the file is located have been broken; the file may be partially overwritten or located in some unorganized area such as the Pagefile.

…

File carving

- It is common for a file to have a header, in the beginning of the file, containing a file signature and a trailer at the end of the file.
- Thus, search for file signatures and trailers and try to rebuild the files.

Example: JPEG—”xFFxD8″ header and “xFFxD9” footer

GIF—”x47x49x46x38x37x61″ header and “x00x3B” footer

Examination & Analysis

- Forensic tools allow dead analysis - maintaining preservation and reducing complexity
- Live analysis via the forensic tools maintain integrity
- Ignore key FS characteristics to provide the analyst with a range of information that an inspection of the live system would not provide - registry, FS meta-files, pagefile.sys
- Functionality that highlights simple data hiding techniques - File Signature Analysis, recovery of Recycle Bin records, hidden folders
- Data reduction through hashing and known datasets
- Data carving

Examination & Analysis

- Pattern matching
- Indexing
- Supports a variety of email clients, web browsers
- Focus upon image-based analysis
- Password cracking
- Reporting

Forensic Tools

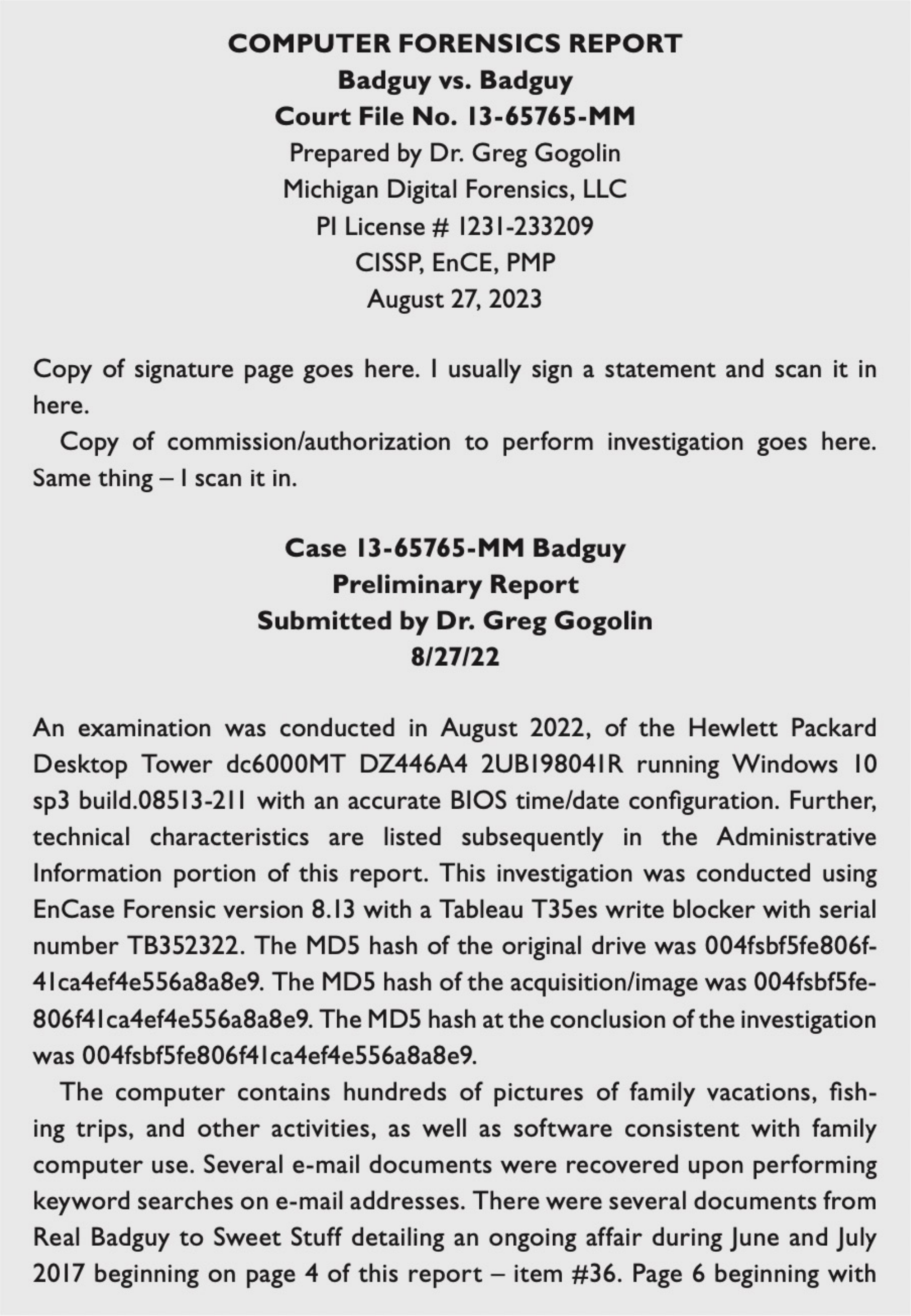
- Commercial Options:
  - Guidance Software EnCase ($4500)
  - AccessData Forensic Toolkit ($3000)
  - X-Ways Forensics (€1100)
  - Internet Evidence Finder ($999+)

- Open Source Options:
  - Autopsy/Sleuth Kit (Windows version available)
  - Digital Forensics Framework
  - SANS Investigative Forensics Toolkit (SIFT)

- …Many specific tools for targeted analyses

Presentation and report

- Example



COMPUTER FORENSICS REPORT
Badguy vs. Badguy
Court File No. 13-65765-MM
Prepared by Dr. Greg Gogolin
Michigan Digital Forensics, LLC
PI License # 1231-233209
CISSP, EnCE, PMP
August 27, 2023

Copy of signature page goes here. I usually sign a statement and scan it in here.

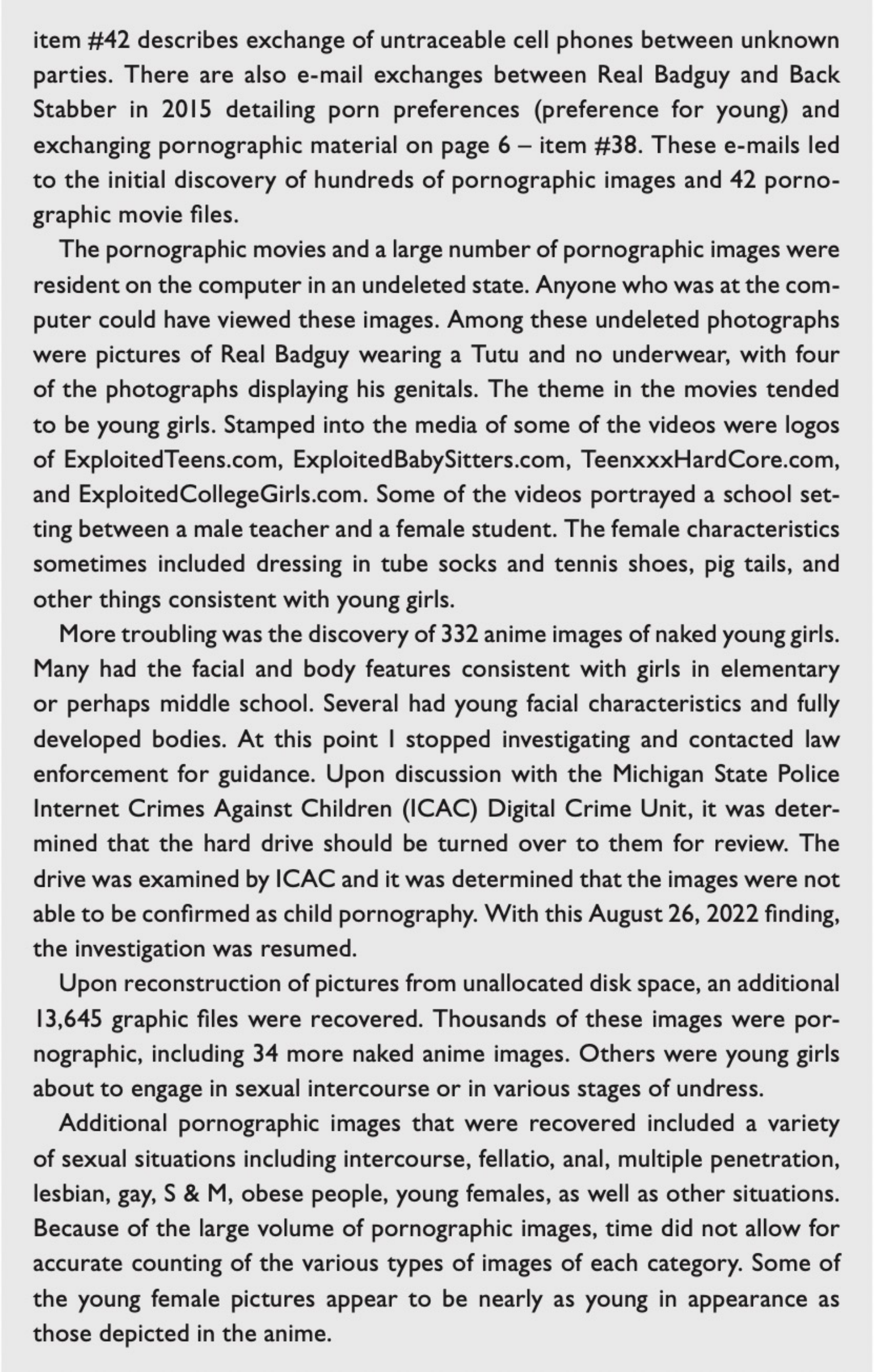
Copy of commission/authorization to perform investigation goes here. Same thing – I scan it in.

Case 13-65765-MM Badguy
Preliminary Report
Submitted by Dr. Greg Gogolin
8/27/22

An examination was conducted in August 2022, of the Hewlett Packard Desktop Tower dc6000MT DZ446A4 2UB198041R running Windows 10 sp3 build.08513-211 with an accurate BIOS time/date configuration. Further, technical characteristics are listed subsequently in the Administrative Information portion of this report. This investigation was conducted using EnCase Forensic version 8.13 with a Tableau T35es write blocker with serial number TB352322. The MD5 hash of the original drive was 004fsbf5fe806f41ca4ef4e556a8a8e9. The MD5 hash of the acquisition/image was 004fsbf5fe806f41ca4ef4e556a8a8e9. The MD5 hash at the conclusion of the investigation was 004fsbf5fe806f41ca4ef4e556a8a8e9.

The computer contains hundreds of pictures of family vacations, fishing trips, and other activities, as well as software consistent with family computer use. Several e-mail documents were recovered upon performing keyword searches on e-mail addresses. There were several documents from Real Badguy to Sweet Stuff detailing an ongoing affair during June and July 2017 beginning on page 4 of this report – item #36. Page 6 beginning with

Ref: Gogolin, Greg, ed. *Digital forensics explained*. CRC Press, 2021 (page 119)



item #42 describes exchange of untraceable cell phones between unknown parties. There are also e-mail exchanges between Real Badguy and Back Stabber in 2015 detailing porn preferences (preference for young) and exchanging pornographic material on page 6 – item #38. These e-mails led to the initial discovery of hundreds of pornographic images and 42 pornographic movie files.

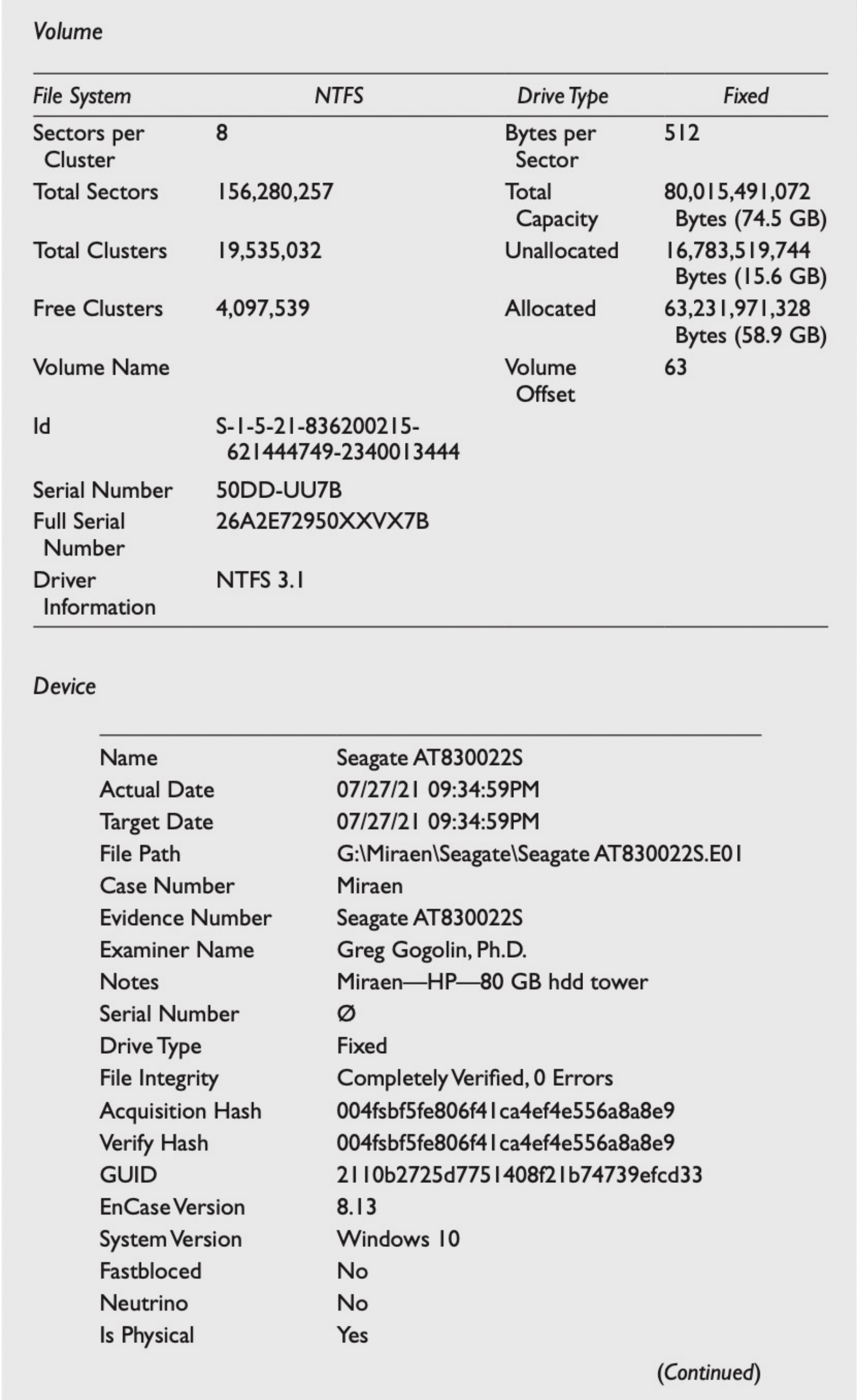
The pornographic movies and a large number of pornographic images were resident on the computer in an undeleted state. Anyone who was at the computer could have viewed these images. Among these undeleted photographs were pictures of Real Badguy wearing a Tutu and no underwear, with four of the photographs displaying his genitals. The theme in the movies tended to be young girls. Stamped into the media of some of the videos were logos of ExploitedTeens.com, ExploitedBabySitters.com, TeenxxxHardCore.com, and ExploitedCollegeGirls.com. Some of the videos portrayed a school setting between a male teacher and a female student. The female characteristics sometimes included dressing in tube socks and tennis shoes, pig tails, and other things consistent with young girls.

More troubling was the discovery of 332 anime images of naked young girls. Many had the facial and body features consistent with girls in elementary or perhaps middle school. Several had young facial characteristics and fully developed bodies. At this point I stopped investigating and contacted law enforcement for guidance. Upon discussion with the Michigan State Police Internet Crimes Against Children (ICAC) Digital Crime Unit, it was determined that the hard drive should be turned over to them for review. The drive was examined by ICAC and it was determined that the images were not able to be confirmed as child pornography. With this August 26, 2022 finding, the investigation was resumed.

Upon reconstruction of pictures from unallocated disk space, an additional 13,645 graphic files were recovered. Thousands of these images were pornographic, including 34 more naked anime images. Others were young girls about to engage in sexual intercourse or in various stages of undress.

Additional pornographic images that were recovered included a variety of sexual situations including intercourse, fellatio, anal, multiple penetration, lesbian, gay, S & M, obese people, young females, as well as other situations. Because of the large volume of pornographic images, time did not allow for accurate counting of the various types of images of each category. Some of the young female pictures appear to be nearly as young in appearance as those depicted in the anime.

Ref: Gogolin, Greg, ed. *Digital forensics explained*. CRC Press, 2021 (page 120)



Volume

File System	*NTFS*	*Drive Type*	*Fixed*
Sectors per Cluster	8	Bytes per Sector	512
Total Sectors	156,280,257	Total Capacity	80,015,491,072 Bytes (74.5 GB)
Total Clusters	19,535,032	Unallocated	16,783,519,744 Bytes (15.6 GB)
Free Clusters	4,097,539	Allocated	63,231,971,328 Bytes (58.9 GB)
Volume Name		Volume Offset	63
Id	S-1-5-21-836200215-621444749-2340013444		
Serial Number	50DD-UU7B		
Full Serial Number	26A2E72950XXVX7B		
Driver Information	NTFS 3.1		

Device

Name	Seagate AT830022S
Actual Date	07/27/21 09:34:59PM
Target Date	07/27/21 09:34:59PM
File Path	G:\Miraen\Seagate\Seagate AT830022S.E01
Case Number	Miraen
Evidence Number	Seagate AT830022S
Examiner Name	Greg Gogolin, Ph.D.
Notes	Miraen—HP—80 GB hdd tower
Serial Number	Ø
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition Hash	004fsbf5fe806f41ca4ef4e556a8a8e9
Verify Hash	004fsbf5fe806f41ca4ef4e556a8a8e9
GUID	2110b2725d7751408f21b74739efcd33
EnCase Version	8.13
System Version	Windows 10
Fastbloced	No
Neutrino	No
Is Physical	Yes

(*Continued*)

Ref: Gogolin, Greg, ed. *Digital forensics explained*. CRC Press, 2021, page 122

Proactive Forensics

Anti-Forensics

Anti-Forensics

- Data hiding
- Artefact wiping
- Trial obfuscation
- Forensic tool vulnerabilities

Conclusions

Conclusions

- In a world with increasing cyber crime, digital forensics is becoming increasingly important

- The majority of the focus to date has been upon computer forensics

- Future areas of development include:
  - Network Forensics
  - Embedded Forensics

- Appropriate tools and applications are need to be developed to help assist in the sourcing and collection of evidence

UNIVERSITY OF PLYMOUTH

Hai-Van Dang

Hai-van.dang@Plymouth.ac.uk

Centre for Security, Communications & Network Research

www.plymouth.ac.uk/cscan