DIGITAL FORENSIC FUNDAMENTALS (COCS70704)

By

MUYIDEEN KAZEEM OLUWADARE (21027842L)

MSc Computer Science (Cyber Security)

School of Digital, Technologies and Arts

Department of Computing

January 16, 2023.

Table of Contents

List Of Figures

List Of Tables

PART A – DIGITAL FORENSICS LABORATORY SETUP

1.0 Introduction

A digital forensics investigation that yields useful results can serve as a fair and verifiable basis for legal proceedings. While traditional digital forensics focused on desktops and servers, recent shifts in digital media and platforms have increased the need for digital forensic investigation techniques on small and mobile devices, databases, networks, cloud-based platforms, and the Internet of Things to corroborate a suspected security incident for court admissibility(Al-Dhaqm et al., 2021). A digital forensics lab is described in this report and its components. The first part of this paper will provide an overview of digital forensics, identify potential clients, and lay out a strategic plan for establishing and running the lab. It discusses digital forensics principles and guidelines and identifies the hardware, software, human, technical, and financial resources required to run a forensic lab. The study will conclude with an essential review of the results and future improvements, and the development of a standard operating procedure (SOP) based on a forensic investigation framework.

1.1 Introduction to Digital Forensics

National Institute of Standards and Technology (NIST) explain digital forensics as “The discipline of forensic science known as "digital forensics" which focuses on collection, preservation, and analysis of digital evidence that can be used in criminal investigations. Data from all electronic media, such as computers, removable drives (flash drives, memory cards etc.), mobile phones, etc., are included.” (National Institute of Standards and Technology, 2022) while Ramadhani et al. (2017) stated that the term "forensics" refers to the scientific method of collecting, evaluating, and severity evidence in a court of legislation concerning the existence of a lawsuit. This field has been expanding for quite some time, as the modern legal system continues to place a greater emphasis on the use of scientific evidence in legal proceedings. According to Al-Dhaqm et al. (2021), Information confidentiality, integrity, availability, and authenticity (CIAA) are rarely adequately protected by the cybersecurity systems and processes that are put in place. Thus, to probe possible security incidents and digital crimes in the event of a CIAA breach, digital forensic processes and techniques are frequently necessary. Since there is now a plethora of information that can be retrieved from digital devices to aid in solving various crimes, forensic analysis in the digital realm is no longer a new thing for investigators. Digital forensics analysis is crucial and must not be underestimated.

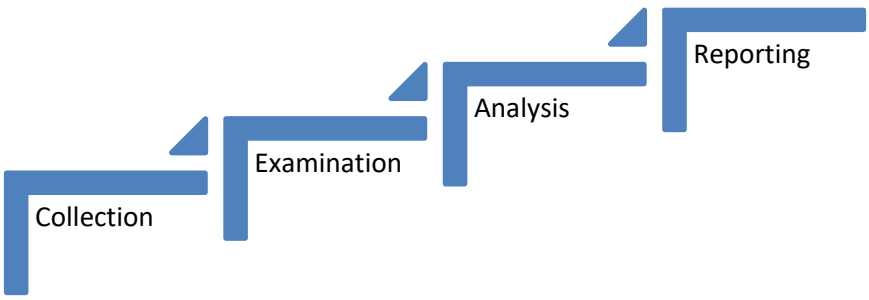


Figure 1: Phase of Digital Forensics (Institute of Electrical and Electronics Engineers & IEEE Communications Society, 2017)

2.0 Business Case

Many organizations, countries, and individuals have been attacked over the years through various forms of digital media, such as attacks on websites carried out by means of phishing, attacks on smartphones carried out by means of malware, and many other forms of attack, which frequently result in the loss of personally identifiable information (PII) and personal health information (PHI), IT Assets amongst other forms of information. As a direct result of this, an increased number of people are seeking the assistance of digital forensic services. In February 2016, the central bank of Bangladesh was the target of an attack that became known as the Bangladesh Bank Cyber Heist, and this attack resulted in the theft of $81 million through a fraudulent transaction that was sent via the SWIFT payment gateway and this theft was the culmination of months of activity in which the attacker used malware to target the bank infrastructure which also had the capability to manipulate the bank's legitimate SWIFT payment order system (NCSC & NCA, 2017). The Bank's governor consulted World Informatix Cyber Security to handle incident response, vulnerability assessment, and correction, so, therefore, World Informatix Cyber Security hired Mandiant to investigate this incident which they found the "hacker footprints" and malware installed in the bank system since January 2016 that gathered information on international payments, fund transfers and the investigators also found out that the hackers were outside Bangladesh (Balu, 2022). Regardless of the type of attack, network, botnet, system hacking, and more, a victim's or suspect's device always contains evidence. The Myanmar 2010 Cyberattacks also known as “Burma” as reported by Centre for Responsible Business (2013) was attacked by DDoS before the 2010 election which overwhelmed the country's main Internet service provider, where the Arbour Networks discovered the attack, which was larger than the 2007 Estonian attack, but couldn't determine its origin. Speculation ranged from blaming Myanmar's government to external hackers with unknown motives and it has been a major worry for law enforcement agencies to rely on Forensic Service providers (FSP) to analyze digital evidence gathered at crime scenes.

According to NPCC (2020), while some police departments use FSPs for routine analysis, others only engage them for specialized analysis they cannot perform in-house, creating the need to ensure that only

accredited service providers are involved in such sensitive investigations as one of the many obstacles law enforcements must overcome. While some law enforcement agencies are unable to afford personal laboratories for some digital case examinations, the worries have anticipated the need to have a well-equipped forensic laboratory that will assist the law enforcement agencies to investigate a case involving different aspects of digital devices and maintain a high-quality ACPO standard to be acceptable in the court of law which this forensic lab will be filling the gap. For small enforcement agencies and other law enforcement agencies that are unable to meet up with the forensic standard, the concerns anticipated the need for a well-equipped forensic laboratory that will assist law enforcement agencies in investigating cases involving various aspects of digital devices while maintaining a high-quality ACPO standard that will be acceptable in a court of law. This forensic laboratory will fill the gap for small enforcement agencies and other law enforcement organizations that cannot afford their own personal laboratory for some digital case examination. This report's primary objective is to solicit a proposal for establishing a forensic laboratory; however, permission is hereby requested before continuing to the subsequent stages.

3.0 Computing Laboratory for Forensic Investigations

Inside this section, we would then discuss the ancillary components of the lab, such as the necessary supplies and equipment, as well as the guidelines for conducting a forensic investigation. In light of this big picture, the laboratory services will adopt the CFSAP (Computer Forensic Secure Analyze, Present) model investigation procedures, however, to make sure the evidence extracted and analyzed can be used in court, the case handling procedures will be adjusted to adhere to certain ACPO (Association of Chief Police Officers) and SWGDE (Scientific Working Group on Digital Evidence) rules (Rosselina et al., 2020).

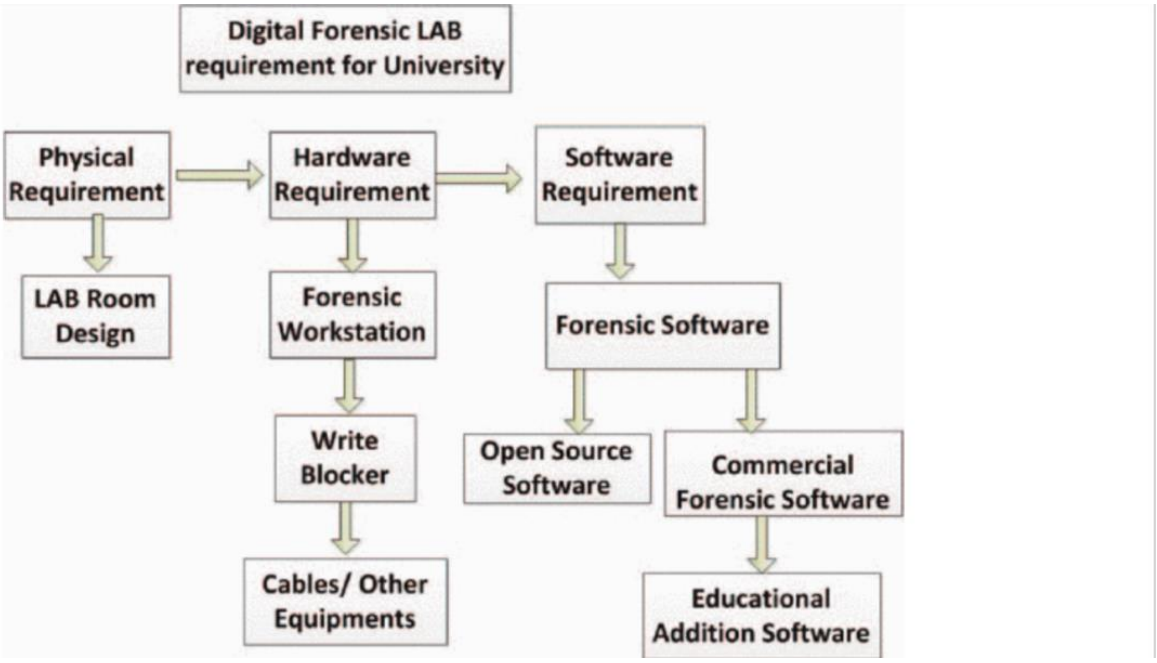


Figure 2: Expectations of a Digital Forensics Lab (Institute of Electrical and Electronics Engineers & IEEE Communications Society, 2017)

3.1 Roles and Responsibilities

According to ACPO (2011), Principle 2, stated that when accessing primary sources, one must be knowledgeable enough to do so and provide evidence justifying the necessity and consequences of doing so. First and foremost, this lab will seek out certified and train qualified personnel to ensure that everyone working there is fully capable in their assigned roles. The laboratory will consist of the following staffs with the total average salary of (£240,000) as listed in the Budget shown in Table 2.

- **Digital Forensic Lab Manager (1 staff)**: The Digital Forensics Manager oversees the daily operations of the primary digital device's lab (Metropolitan Police Service, 2022). The average salary will be £50,000 for one staff.
- **Computer Forensic Analyst (1 staff)**: The primary responsibilities of this position include electronic discovery, data recovery, and computer forensics investigations (San Jose State University, 2022). The average salary will be £40,000 for one staff.
- **Digital Forensic Examiner (2 staffs)**: The responsibilities are to collect forensic evidence, conduct an analysis on it, and then provide a report on their findings using their expertise, knowledge, and training in digital forensics (FBI, 2022). The total average salary will be £40,000 for two staffs (£20,000 each).
- **Digital Forensic Imaging Technician (2 staffs):** This role will be responsible for copying a physical storage device; however, the image will be an exact copy of the drive's structures as well as its contents (Study.com, 2022). The total average salary will be £30,000 for two staffs (£15,000 each)
- **Document Owners (1 staff)**: They'll document lab management systems. Document Owners assign authors, manage, update, circulate, and approve final documents. He or she supervises the Document Author, Reviewer, and Registrar. The total salary will be £20,000 for one staff.
- **Auditors (2 staffs)**: Their role is to ensure that all departments perform as expected. They will be evaluating the management system policies and scope and ensure all lab sections are audited. The total average salary will be £30,000 for two personnel (£15,000 each)
- **Office Cleaner (2 staffs)**: The employees in this department are responsible for maintaining a clean and orderly workplace that is welcoming to both clients and staff. The total average salary will be £30,000 for two personnel (£15,000 each).

3.2 Forensic Laboratory Tools

To conduct a forensic investigation and produce a forensic result that meets legal standards, specialized hardware and software are required.

3.2.1 Hardware Requirement

Below are some of the hardware equipment needed in the forensic laboratory which will cost the total sum of £32,620 as listed in Table 2:

- Write Blocker Hardware (2) – This hardware connects the hard drive (SATA, IDE, SSD) to the computer and prevents write permission to prevent evidence manipulation.
- Computer (10): If you want to process data quickly and efficiently, you need a system with a high configuration speed with a fast processor, plenty of storage space, and at least 32GB of RAM to function properly.
- Cooling Devices (4): This is essential for the health and efficiency of the lab's human and mechanical inhabitants.
- Forensic Lab Furniture (10): It is necessary to have cabinets, comfortable chairs, and large tables for putting computer systems, monitors, mobile devices, and extraction equipment.
- Toolbox (3): The toolbox containing all tools such a screwdriver, plier etc. required to investigate all aspects of forensic investigation (Mobile, Computer, Network).

A faraday bag, hard drive, lead adaptors, cameras, exhibit labels, storage bags, and much more are just some of the other tools needed.

3.2.2 Software Requirement

Due to the lack of support for open sources tool and limited acceptance in the court of law, commercial software will be considered for this forensic laboratory, but some open sources software is also considered. Table 1 below shows tools that are considered for the laboratory as recommended by (Institute of Electrical and Electronics Engineers & IEEE Communications Society, 2017b). All the software and licensing will cost the total sum of £62,000 as shown in Table 2.

S/N	Tools	Features
1	Access Data Forensic	Image Acquisition, Registry Analysis, Data

	Toolkits (FTK)	carving Reporting
2	Encase	Acquisition, File recovery, signature analysis, hash analysis, reporting
3.	Sleuth Kit (Autopsy)	Password recovery, cookie viewer, internet history, email analysis, picture analysis
4.	Cellebrite	Unlock locked files, restore lost data, and view erased files. Apps' location data, along with call logs, text messages, multimedia, emails, calendar and contact files, and other data are all part of the proposed.
5.	Oxygen Forensic	Find information about your contacts by scouring a variety of online and offline sources.
6	John The Ripper, Cain Abel, Hash Cat, Dumpit	Password recovery for windows and Linux Operating System
7.	Virtual Machine	The virtual machine's guest Operating System (Windows, Ubuntu, Kali, and Caine) is installed on the host. This prevents damage to the host OS, hardware, or malware while investigating or extracting.

Table 1: Software Tools (Institute of Electrical and Electronics Engineers & IEEE Communications Society, 2017)

3.2.3 Laboratory Budget for Hardware, Software and Staffs

Below is a table estimating the annual cost of setting up the laboratory, noting that some equipment is purchased only once, while other equipment requires a yearly subscription.

S/N	Item	Specification	Units	Unit Price (£)	Total Cost (£)
1	Hardware	Desktop Computers *Requirements: Intel Core i7 1TB SSD, 32Gb RAM, NVIDIA GeForce RTX 3070 8 GB windows 11, together with Virtualized Linux and Windows 10 & 7 Operating System, 22'' LED Monitor and UPS*	10	1,800	18,000

		Hardware Write Blocker	2	475	950
		Digital Cameras	2	350	700
		Worktables and Chairs	10	400	4000
		Toolbox	3	2500	7500
		Cooling Devices	4	250	1000
		NAS Backup Drive	1	370	370
		Backup Hard Drive	2	50	100
2	Software Licenses	Encase	Yearly	25,000	25,000
		Autopsy	Yearly	0	0
		XRY Complete	Yearly	10,000	10,000
3	Cloud Services	Azure Cloud Service Subscription	Yearly	29,700	27,000
4	Human Resources	Laboratory Manager, Digital Forensic Analyst, Digital Forensic Examiner, Forensic Imaging Technician, Document Owner, Auditors, Cleaners	11	240,000	240, 000
		Total			**334,620**

Table 2: Minimum Annual Budget Forecast

3.2.4 Accreditation and License Requirement

It is essential to have the proper accreditations and certifications in place before a forensic lab can be considered "standard". Forensic units providing digital forensic science services must be accredited to either ISO17020 for any inspection or testing activity at the scene of the incident or

ISO17025 for any laboratory function (such as the recovery or imaging of electron micrographs) (the Codes) (The Forensic Science Regulator, 2020). According to (ISO/IEC, 2021), The following are some international standards for laboratory accreditation that have been established to promote worldwide acknowledgement: ISO/IEC Guide 58, "Calibration and Testing Laboratory Accreditation Systems - General Prerequisites for Operation and Recognition," ISO/IEC Guide 46, "Comparative Testing of Consumer Products and Related Services - General Principles," and ISO/IEC DIS 17025 are the new standards (ISO/IEC Guide 25 was obsoleted in 2001) for the competence of calibration and testing laboratories. Therefore, the laboratory will undergo evaluation by the United Kingdom Accreditation Service (UKAS) to receive the ISO17020/ISO17025 accreditation and license after all the above hardware and license software such (Encase and XRY) are in place.

3.2.5 Laboratory Security

Constant attention to laboratory security and safety is always required. Evidence storage, internal workspace security, and external workspace security are all important factors to consider when ensuring the safety of forensic laboratory evidence, employees, and the integrity of its investigations, as stated by (SalvationData Technology, 2022). The standard forensic laboratory should have the following:

- an access register,
- physical locks,
- biometric control,
- Sipe cards in case the biometric control fails,
- Fire extinguishers and a fire suppression system to prevent fire outbreaks and loss of property and life.
- CCTV surveillance should be installed both inside and outside the laboratory, adequate ventilation and heating conditions must be present. In contrast, evidence and other data should be stored in the cloud, while a Network Access Storage (NAS Drive) should be used for internal operations, replicating, and backing up of files/data to the stored in the cloud and offsite storage.

3.2.6 Facility Management

The laboratory's excluded areas will be clearly labelled. Outside of the laboratory, forensic

analysts do things like analyze data, write reports, testify in court, and it would be preferable if the analyst had a sanitized and peaceful place to do paperwork outside of the potentially hazardous laboratory setting by providing desks, cubicles, and conference rooms for reviewing cases and administrative paperwork. Except for the supervisors' offices, all other administrative areas may make use of open office systems. Experts in the document and latent print examination are trained to conduct a wide range of technical analyses outside the laboratory (Office of Justice Programs & Institute of Justice, 2022). According to Jones et al., (2016), vetting, staff development and human resources are crucial for maintaining a pleasant and risk-free workplace because when employees are happy and healthy, they tend to achieve their goals easily and are more motivated to show up to work and give all their best which this laboratory will strongly consider.

3.2.7 Standard Operation Procedure (SOP)

Establishing a standardized process for handling digital evidence can greatly enhance its effectiveness and credibility (SOP). For this reason, it is essential to the development of a highly developed information society that a standard operating procedure is developed and used to maintain standards for digital evidence (Lin et al., 2022). Table 3 shows the standard operating procedure this lab will follow as it examines digital evidence.

Table 3: Standard Operation Procedure

S/N	Stage	Description
1.	Identification & Law	The purpose of the investigation/analysis must be identified, granted and warrant should be obtained if necessary.
2.	Evidence Collection	The digital evidence should be collected either by physical drive (flash drive, disk drive and other storage media) standalone computer and multi-computer networks.
3.	Evidence Handling and Preservation	It is necessary to do this both before and after receiving evidence: Evidence should be handled with care, labeled appropriately, and stored safely. Evidence should not be left where it could be accidentally tampered with, which could result in the loss of electronic evidence. It is imperative that a copy of the digital evidence be made.
4.	Chain of Custody	How the evidence has been handled and transferred from different personal and department should be documented.

5.	Digital Evidence Integrity	The Hash value of the evidence should be taken, validated, maintained, and stored before and after the examination.
6.	Licensing	The examination of digital evidence should be conducted using only licensed tools and sanctioned open-source software such EnCase, FTK, OXYGEN, XRY, Autopsy.
7.	Analyzing and Examining	The evidence is the most crucial part, however, in order for the acquired digital evidence to be admissible in court, it must be professionally investigated to collect, examine, and evaluate all evidence contained in the image and must be presentable in the court of law.
8.	Reporting (Executive Summary, Summary of Evidence Findings, Conclusion and Recommendation)	A report detailing the outcomes of the investigation should be compiled and documenting everything from the software version(s) used to the collection tool and analysis methodology employed, as well as the rationale behind the collection and analysis of evidence, the findings must be stated explicitly so that in court, the pieces of evidence gathered can be adopted. A lawsuit can be established, however, a formal report after finishing an investigation to document the steps taken, the tools, methods used, and the results. Also, the report's title should provide a clear and concise summary of its contents and to detail the tasks accomplished, including conclusion on the analysis that was performed

3.2.8 Current Standards

It is imperative that forensic units offering digital forensic science services be accredited to the latest standard ISO 9001, NIST 800-86, ISO17020 (for on-site inspection and testing) or ISO17025 (for laboratory analysis) (The Forensic Science Regulator, 2020). According to NIST (2022), laboratory personnel play a crucial role in the need's evaluation process, so it's important that they have a thorough understanding of forensic guidelines, principles, and procedures, as well as the expertise, skill, and techniques to use forensic and anti-forensic tools available to provide input into research need to guarantee an early investigation and acceptable standard report (Aguilar et al., 2013). As explain by ACPO (2011), When it comes to cyber security incidents and crimes, the ACPO publishes updated and revised guidelines to help law enforcement agencies doing investigation. As a result, all recommendations contained in the ACPO guideline, NIST 800-86

and the ISO (9001, 17020,170250 standards will be implemented in this laboratory.

4.0 Conclusions

The practical and transparent dissemination of evidence in the judicial system continues to rely on digital forensic laboratories that are well-structured and efficient. Due to how sensitive an investigation is, all steps must be taken to abide by the rules. For a newly established lab to earn trust and credibility, it must employ a team with the right mix of skills and certification, use industry and peer-reviewed tools, and adopt and strictly adhere to standard operating procedures. Furthermore, the lab budget may increase or decrease due to the number software licenses, hardware equipment's, size of the lab, facilities, and number of personel employed. Future plans for the lab include offering Digital Forensic as a cloud service for remote investigations to help forensic investigators be more efficient in their work.

PART B – WASHER CASE EXAMINATION USING AUTOPSY

5.0 Introduction

This case requires a digital forensic examination of an image (Washer.E01), as requested by the Digital Forensic Staff at Staffordshire University as explain in SOP step 1 above. The investigator is tasked with writing up a detailed report of their findings as written in the SOP step 8 above. In any case, the investigator must handle the management, evaluation, and creation/preservation of all investigative records and evidence (See SOP step 3 and 7). A copy of the team contract detailing responsibilities is attached as Annex A. Also, an executive summary should be provided for the top management staff (See SOP step 8).

The evidence to be identified are as follows:

- Time Zone Analysis
- Operating System Information
- Installed Applications/Programme
- Documents, media, pictures, etc.
- User information.
- Details of system users
- Steganography/encryption if any

5.1 Case Details

This is carried out as explained in SOP step 2 and 3.

Table 4: Case Details Information

Case ID	08-12345
Evidence Number	AD-08-98
Acquired Date and Time	Mon Mar 10, 2008, 23:44:32
Examiner Names	Nick Drehel | Muyideen Kazeem Oluwadare
Examiner I.D Number	21027842
Client Name	Staffordshire University (Digital Forensic Fundamentals)
Laboratory	Laboratory S520 in the Mellor Building at Staffordshire University is where all forensic examinations are conducted.
Description	Washer.E01 Image was taken from office PC
Submission Date	16-01-2023

5.2 Chain of Custody

At 23:44:32 on Monday, March 10, 2008, Nick Drehel took control of the crime scene and delivered the evidence to the Digital Forensic lab 520, thereby beginning the chain of custody. Through the Digital Forensic Fundamentals blackboard, the Digital Forensic Staffs hand over the image to be investigated to the examiner (Muyideen Kazeem Oluwadare), who promptly seizes control of the image and holds on to it until the forensic investigation is complete. After finishing up on the 16th of January 2023, at 23:59, the examiner turned over the findings to Dr. Ange of Staffordshire University via the Digital Forensic Fundamentals blackboard facility. The chain of custody records is attached as Annex A. This is carried out as discuss in SOP step 4.

5.3 License Statement

The SOP step 6 discusses the forensic tools that are acceptable, however, there is no cost to use Autopsy version 4.19.3, an open-source forensic software application used to analyze the evidence, but its use requires a license, which is held by Staffordshire University in Stoke-on-Trent, England.

5.4 Case Management

The university's policies, ISO17020/17025, the Forensic Science Regulator's Standards of Conduct (FSR-C-108), and ACPO's Best Practice Guide for Digital Forensics were adhered to in all cases using the SOP guideline above.

5.5 Executive Summary

The purpose of this report is to conclude an investigation into allegations that a certain individual (Mr. John Washer) engaged in criminal activity by creating and printing counterfeit credit cards and stealing the credit card information of unsuspecting victims using various computer programmes. This has been identified and brought to light for further investigation and due process was followed using the SOP step 2 to 8.

6.0 Analysis, Acquisition and Validation

The SOP step 1 through SOP step 7 was followed for the examination of this evidence for Section 6 to 7.2. Conversely, to safeguard the original image from loss or alteration, a copy of the evidence file was taken from Staffordshire University's Digital Forensic Fundamentals Blackboard and a backup copy was made. The image Washer.E01. was given an acquisition MD5 hash sum of 147307d626aa2c090bd6abfe4a9a1909 (see SOP step 5) which is essential to ensure the integrity of the image both during and after the analysis process, and its analysis and verification of that hash sum are depicted in Figure 3 and 4 respectively.

Figure 3:Analyzing Washer.E01 Image

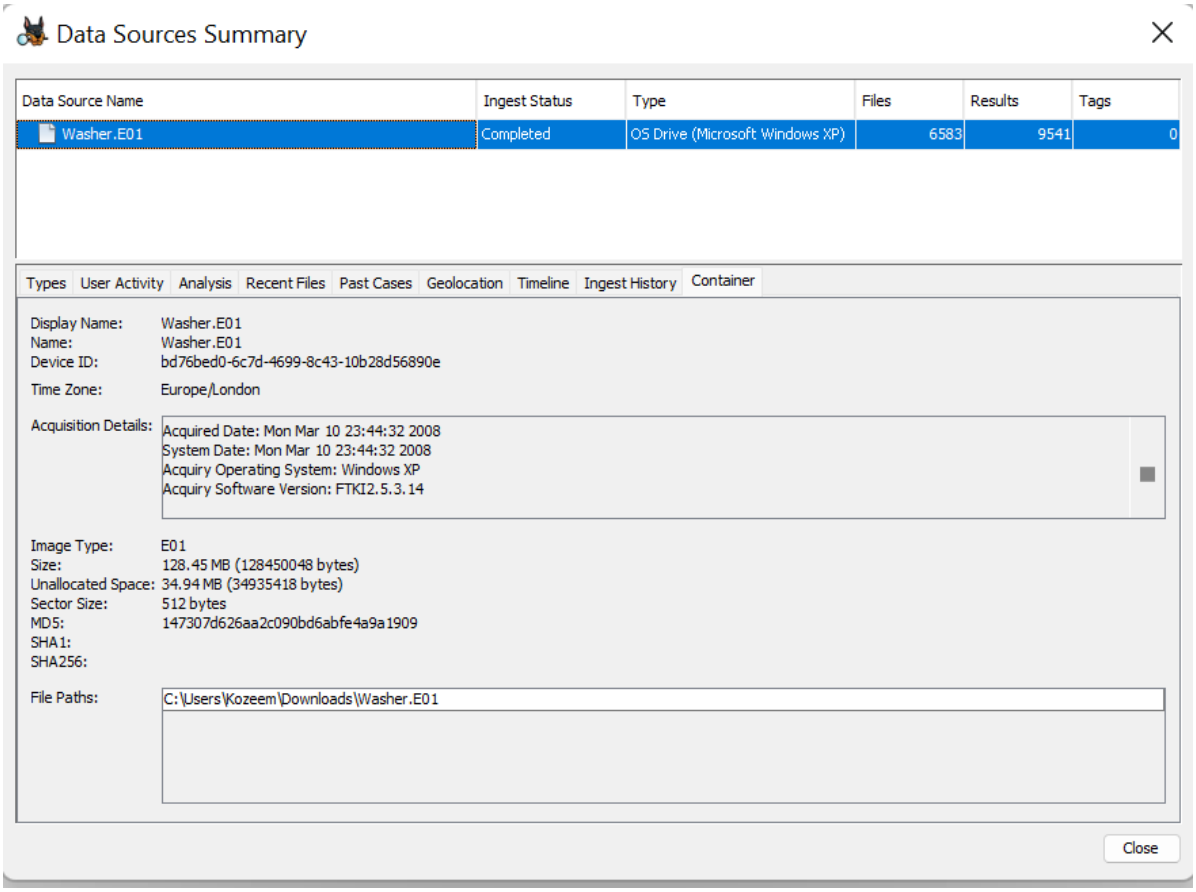
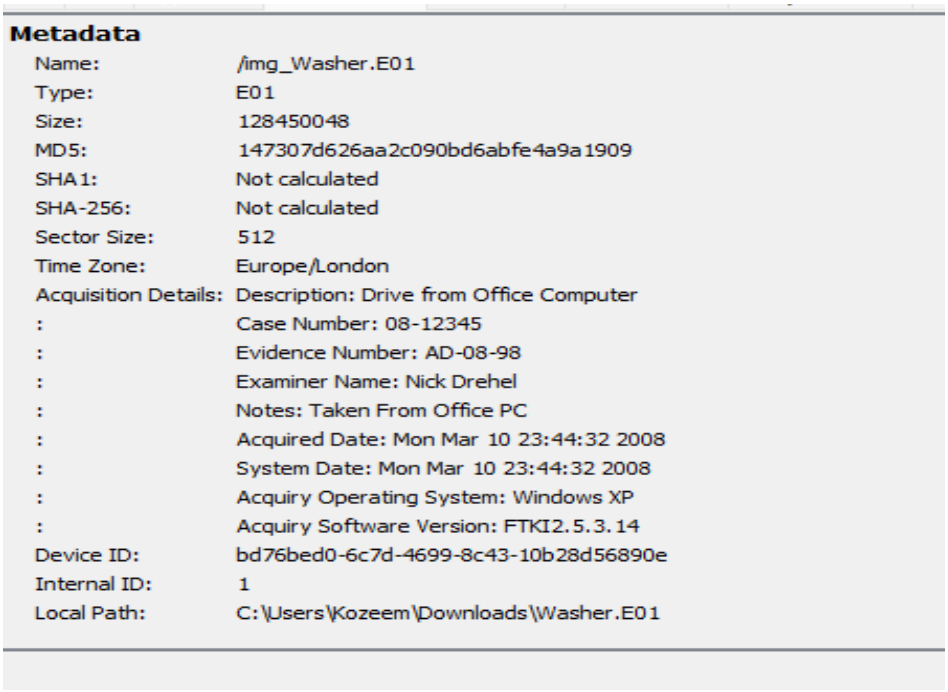


Figure 4: MD5 Hash Value

6.1 Time Zone

In Figure 5 below, we can see the system's time zone is Europe/London.



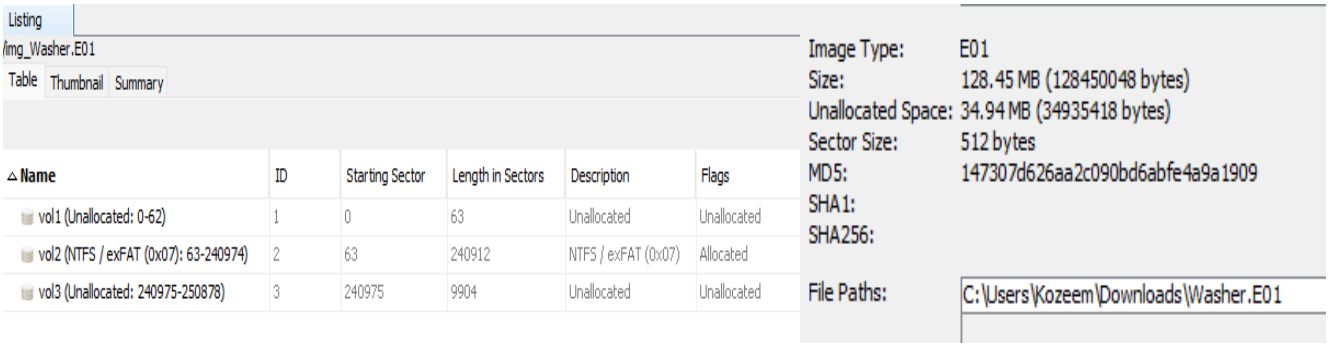
Metadata

Name:	/img_Washer.E01
Type:	E01
Size:	128450048
MD5:	147307d626aa2c090bd6abfe4a9a1909
SHA1:	Not calculated
SHA-256:	Not calculated
Sector Size:	512
Time Zone:	Europe/London
Acquisition Details:	Description: Drive from Office Computer
:	Case Number: 08-12345
:	Evidence Number: AD-08-98
:	Examiner Name: Nick Drehel
:	Notes: Taken From Office PC
:	Acquired Date: Mon Mar 10 23:44:32 2008
:	System Date: Mon Mar 10 23:44:32 2008
:	Acquiry Operating System: Windows XP
:	Acquiry Software Version: FTKI2.5.3.14
Device ID:	bd76bed0-6c7d-4699-8c43-10b28d56890e
Internal ID:	1
Local Path:	C:\Users\Kozeem\Downloads\Washer.E01

Figure 5:Time Zone

6.2 Disk Partitions

The acquired image includes three partitions labelled vol. 1, vol. 2, and vol. 3. The disc geometry also shows three partition volumes: the first (vol 1) is unallocated for the file system to begin on a properly aligned boundary, the second (NTFS/exFAT) is allocated and where the operating system is installed (C Drive), and the third is also unallocated. However, the total disk space is 128.45MB while total unallocated space is 34.94MB. Figure 6. The evidence is shown below.



Listing

/img_Washer.E01

Table | Thumbnail | Summary

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-62)	1	0	63	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 63-240974)	2	63	240912	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 240975-250878)	3	240975	9904	Unallocated	Unallocated

Image Type:	E01
Size:	128.45 MB (128450048 bytes)
Unallocated Space:	34.94 MB (34935418 bytes)
Sector Size:	512 bytes
MD5:	147307d626aa2c090bd6abfe4a9a1909
SHA1:	
SHA256:	
File Paths:	C:\Users\Kozeem\Downloads\Washer.E01

Figure 6: Disk Partitions and Allocated Space

6.3 Operating System Information

According to our analysis, the suspect's computer has been running Microsoft Windows XP. Date of installation: July 25, 2007, at approximately 02:16:00. Additionally, John Washer is registered as the owner on the official documents. See Figure 7 below for visual proof. (See SOP step 7)

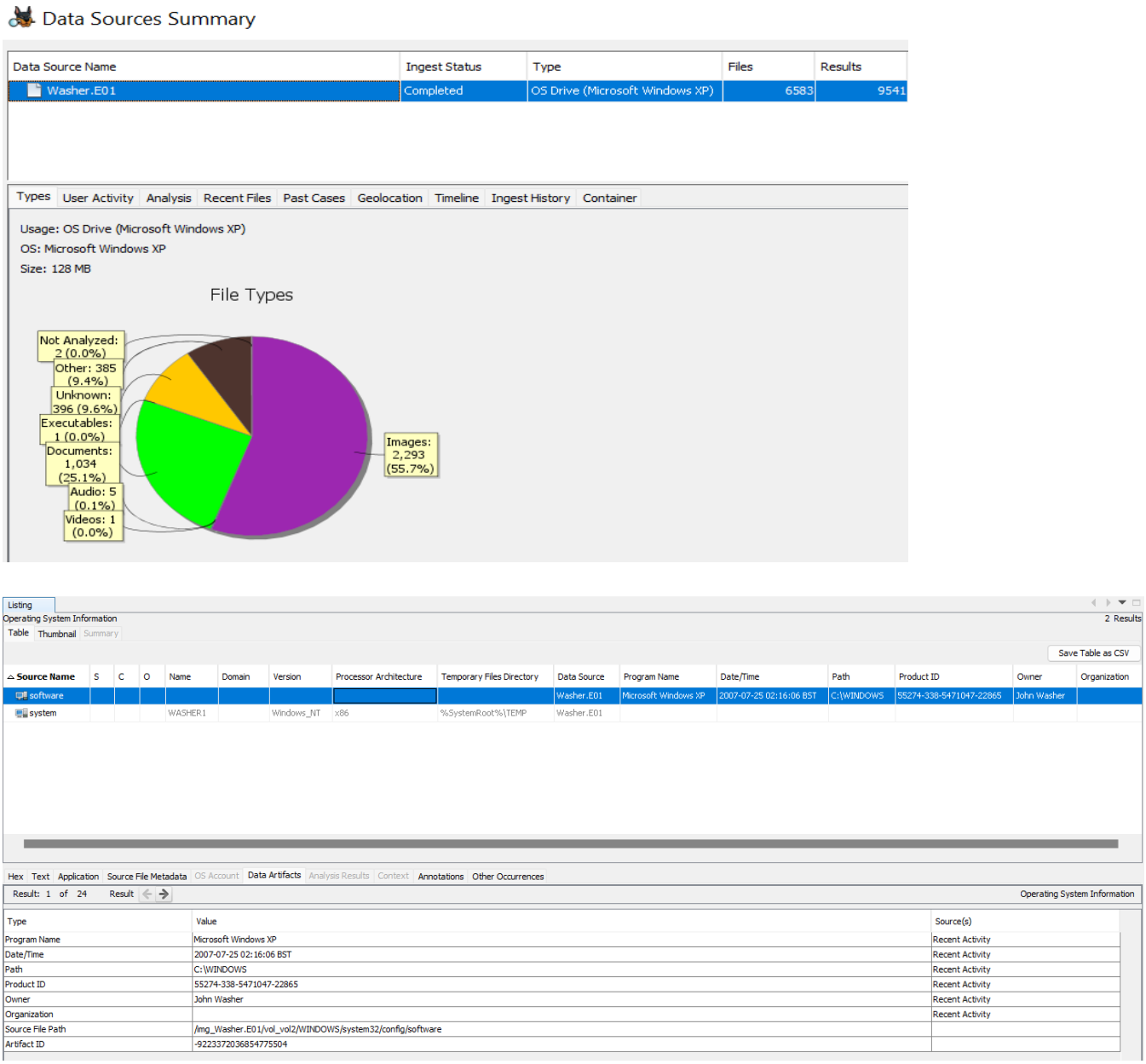


Figure 7: Operating System Information

6.4 Installed Software

The computer currently has 27 applications installed on it. Adobe Flash player, AOL Instant Messenger, DirectAnimation, and DirectDrawEx were discovered, as were file-transfer application like WebFldrs, Connection Manger for client remote access. Fontcore, MobileOptionPack are bad software application that are used to steal passwords and financial information from users. Observe the list of software that has been installed below in Figure 8.

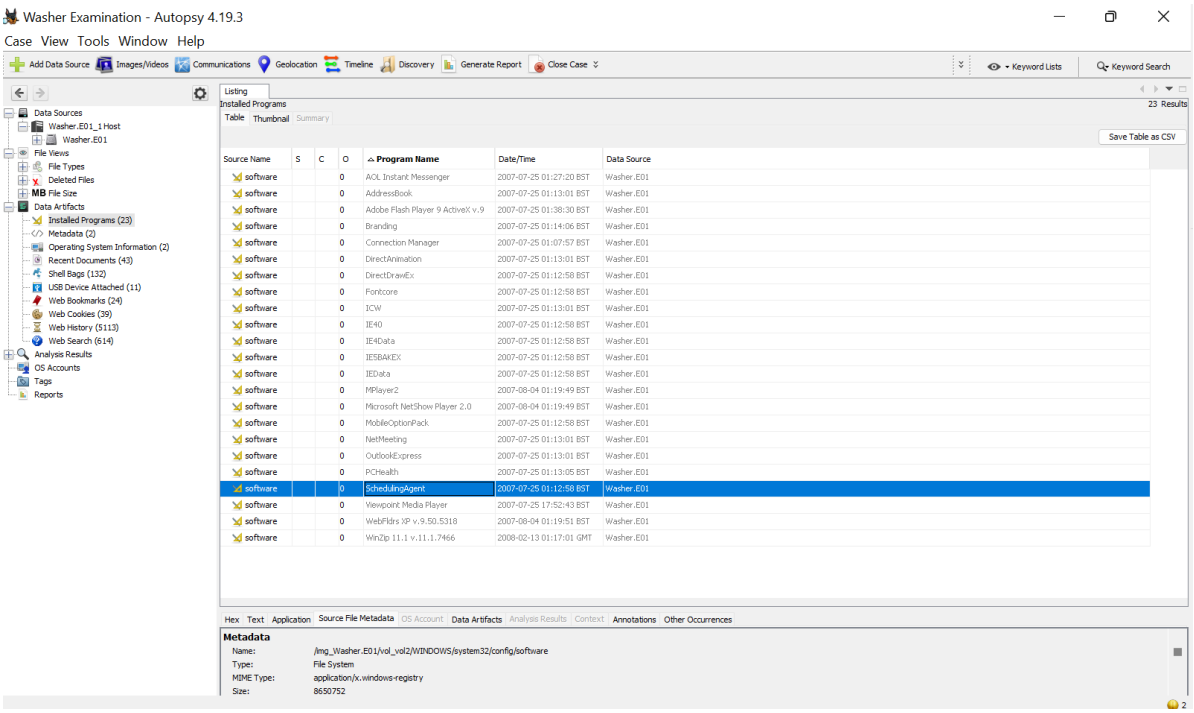


Figure 8:Installed softwares

6.5 User Accounts Information:

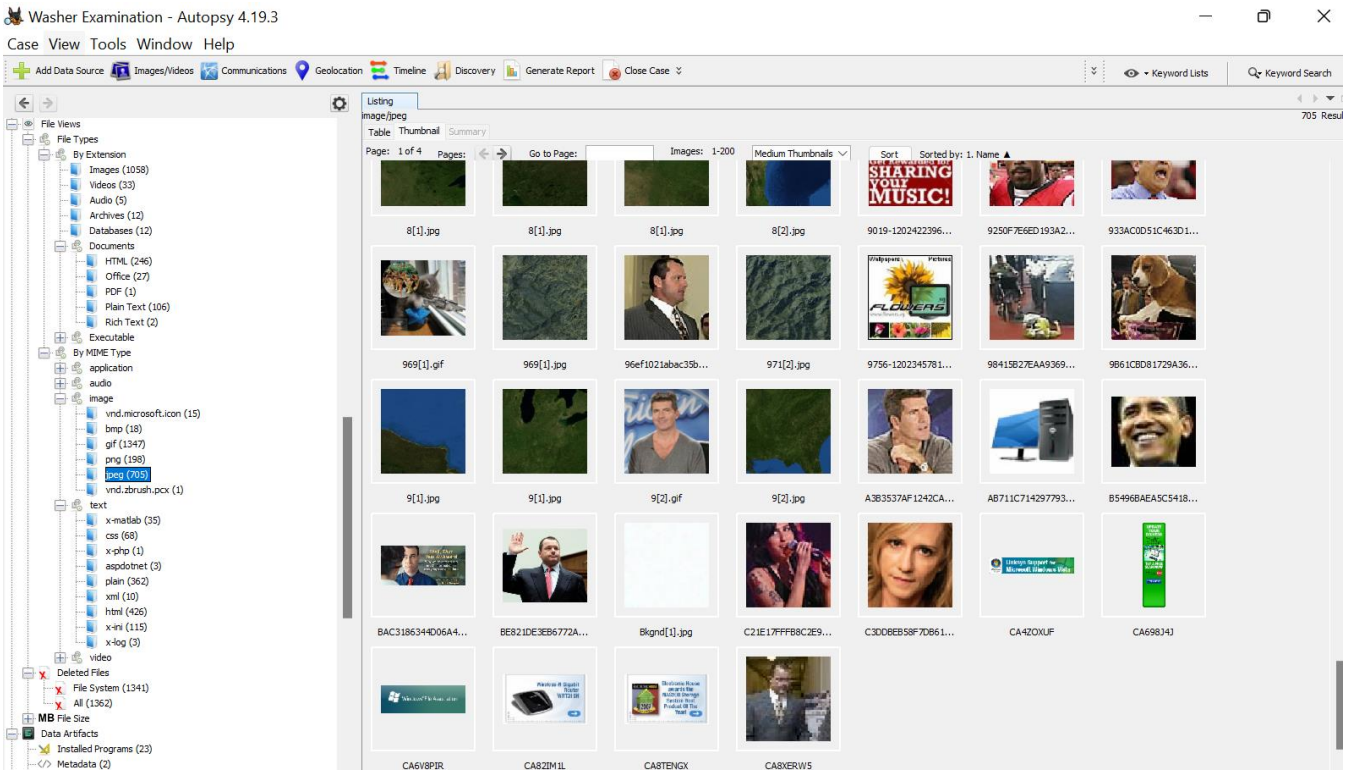
A total of twelve (12) accounts consisting of nine (9) user accounts and three (3) system service accounts have been created. It's also safe to assume that at the time the image was acquired, none of these accounts were being used.

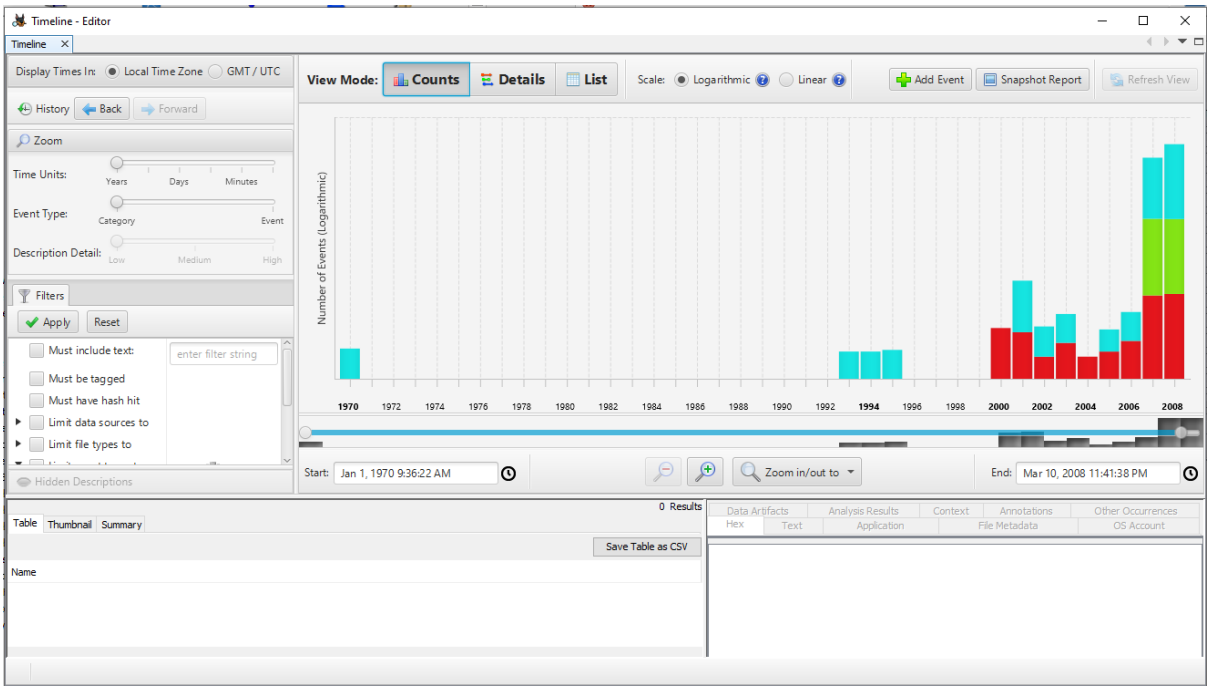
Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-1177238915-616249376-839522115-1000			0	HelpAssistant	Washer.E01_1 Host	Local		2007-07-25 02:11:56 BST
S-1-5-21-1177238915-616249376-839522115-1003			0	Billy Bob Brubeck	Washer.E01_1 Host	Local		2007-08-04 02:14:13 BST
S-1-5-21-1177238915-616249376-839522115-1002			0	SUPPORT_388945a0	Washer.E01_1 Host	Local		2007-07-25 02:13:42 BST
S-1-5-21-1177238915-616249376-839522115-1005			0	Mr Smee	Washer.E01_1 Host	Local		2007-08-04 02:18:00 BST
S-1-5-21-1177238915-616249376-839522115-1004			0	The Wolf	Washer.E01_1 Host	Local		2007-08-04 02:15:03 BST
S-1-5-21-1177238915-616249376-839522115-1006			0	Captian Hook	Washer.E01_1 Host	Local		2007-08-04 02:18:11 BST
S-1-5-21-1177238915-616249376-839522115-1008			0	Artimus	Washer.E01_1 Host	Local		2008-02-13 01:13:46 GMT
S-1-5-21-1177238915-616249376-839522115-501			0	Guest	Washer.E01_1 Host	Local		2007-07-24 19:57:36 BST
S-1-5-21-1177238915-616249376-839522115-500			0	Administrator	Washer.E01_1 Host	Local		2007-07-24 19:57:36 BST
S-1-5-18				systemprofile	Washer.E01_1 Host	Local		
S-1-5-19				LocalService	Washer.E01_1 Host	Local		
S-1-5-20				NetworkService	Washer.E01_1 Host	Local		

Figure 9: User Accounts

6.6 Images

The collection of all relevant tagged images is summarized in Figure 10 below.


Washer Examination - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
File Views
File Types
By Extension
Images (1058)
Videos (33)
Audio (5)
Archives (12)
Databases (12)
Documents
HTML (246)
Office (27)
PDF (1)
Plain Text (106)
Rich Text (2)
Executable
By MIME Type
application
audio
image
vnd.microsoft.icon (15)
bmp (18)
gif (1347)
png (198)
jpeg (705)
vnd.zbrush.pcx (1)
text
x-matlab (35)
css (68)
x-php (1)
aspdotnet (3)
plain (362)
xml (10)
html (426)
x-ini (115)
x-log (3)
video
Deleted Files
File System (1341)
All (1362)
MB File Size
Data Artifacts
Installed Programs (23)
Metadata (2)
Listing
image/jpeg
Table
Thumbnail
Summary
Page: 1 of 4
Pages:
Go to Page:
Images: 1-200
Medium Thumbnails
Sort
Sorted by: 1. Name
705 Resul
8[1].jpg
8[1].jpg
8[1].jpg
8[2].jpg
9019-1202422396...
9250F7E6ED193A2...
933AC0D51C463D1...
969[1].gif
969[1].jpg
96ef1021abac35b...
971[2].jpg
9756-1202345781...
98415B27EAA9369...
9B61CBD81729A36...
9[1].jpg
9[1].jpg
9[2].gif
9[2].jpg
A3B3537AF1242CA...
AB711C714297793...
B5496BAEA5C5418...
BAC3186344D06A4...
BE821DE3EB6772A...
Bkgnd[1].jpg
C21E17FFFB8C2E9...
C3DDBEB58F7DB61...
CA4ZOXUF
CA698J4J
CA6V8PIR
CA8ZIM1L
CA8TENGX
CA8XERW5


Timeline - Editor
Timeline
Display Times In:
Local Time Zone
GMT / UTC
History
Back
Forward
Zoom
Time Units:
Years
Days
Minutes
Event Type:
Category
Event
Description Detail:
Low
Medium
High
Filters
Apply
Reset
Must include text:
enter filter string
Must be tagged
Must have hash hit
Limit data sources to
Limit file types to
Hidden Descriptions
View Mode:
Counts
Details
List
Scale:
Logarithmic
Linear
Add Event
Snapshot Report
Refresh View
Number of Events (Logarithmic)
1970
1972
1974
1976
1978
1980
1982
1984
1986
1988
1990
1992
1994
1996
1998
2000
2002
2004
2006
2008
Start:
Jan 1, 1970 9:36:22 AM
Zoom in/out to
End:
Mar 10, 2008 11:41:38 PM
0 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Hex
Text
Application
File Metadata
OS Account

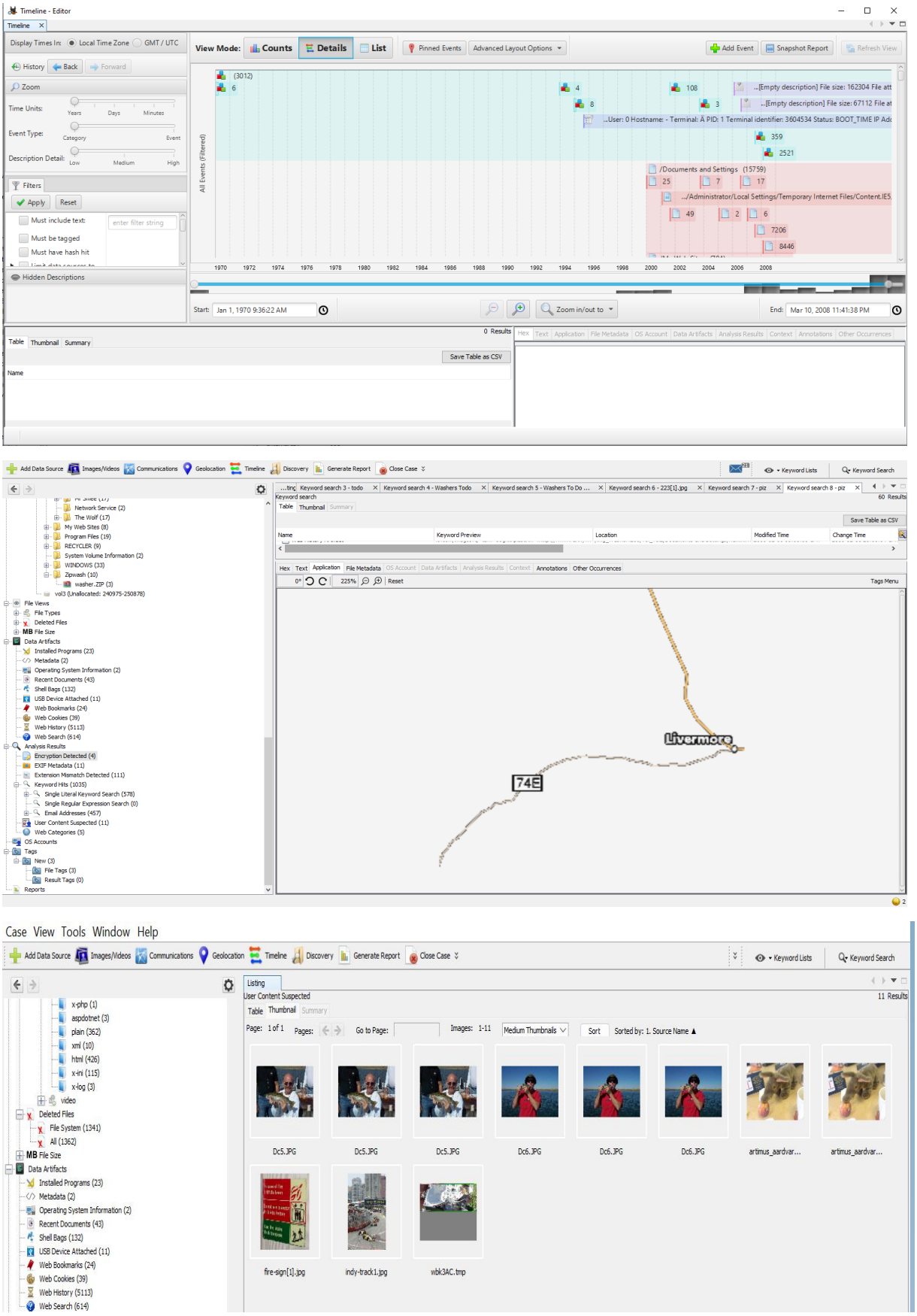


Figure 10: Images

6.7 Audio and Video Files

The Audio and Video discover on the suspect system is shown in figure 11 below.

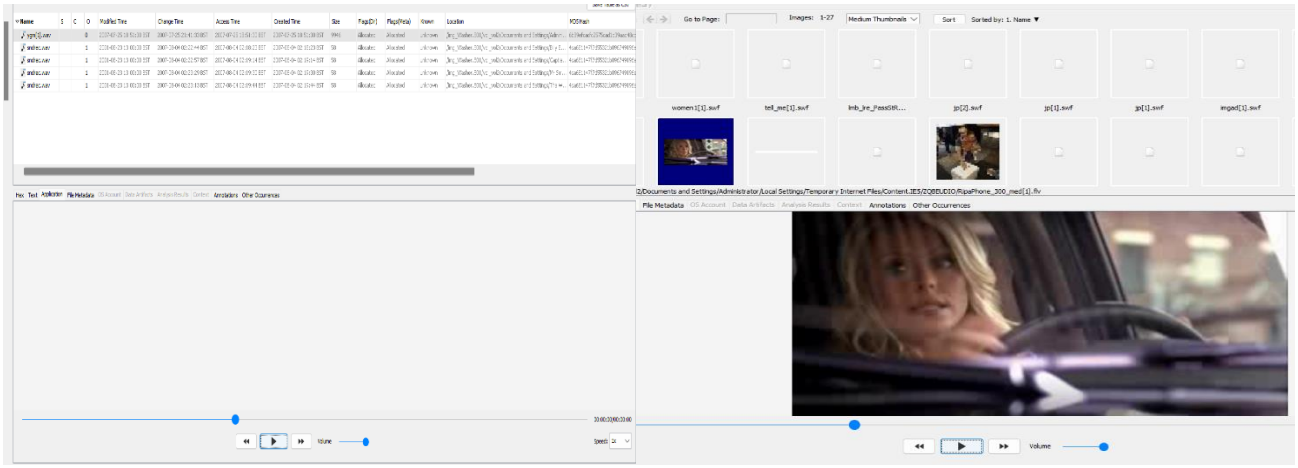


Figure 11: Audio and Video Files

6.8 Deleted Files

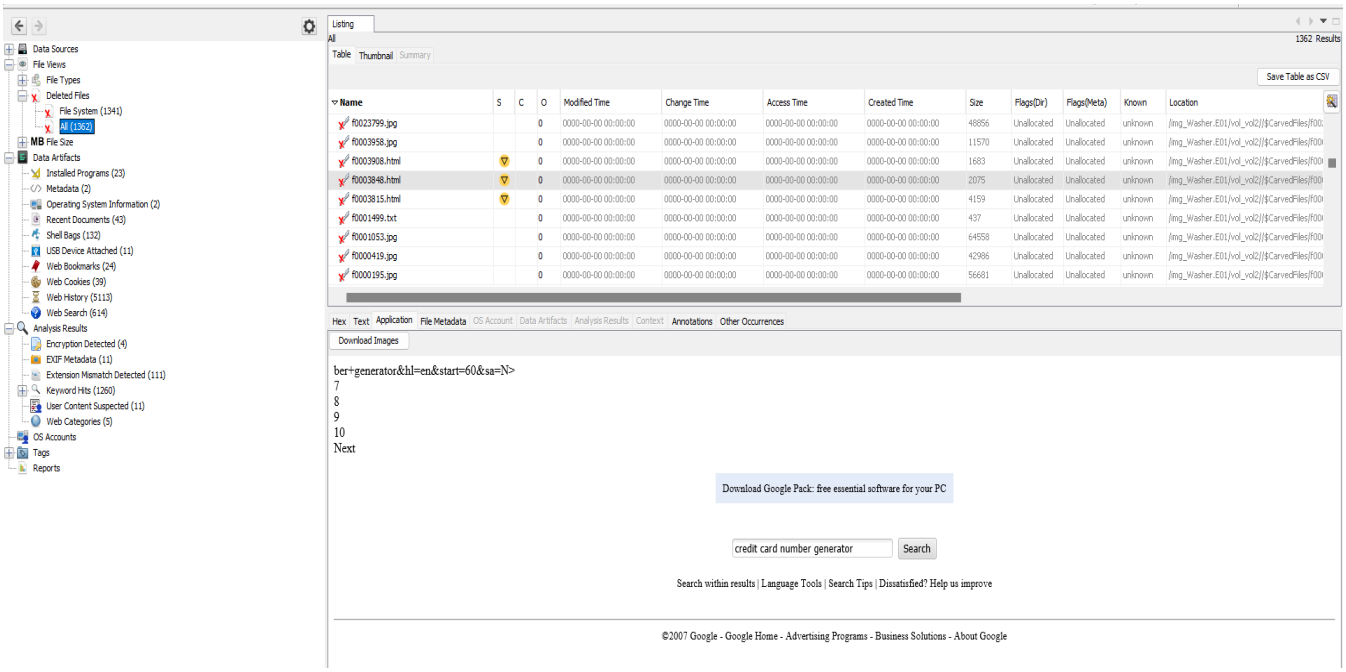


Figure 12: Deleted File

6.9 Connected Devices

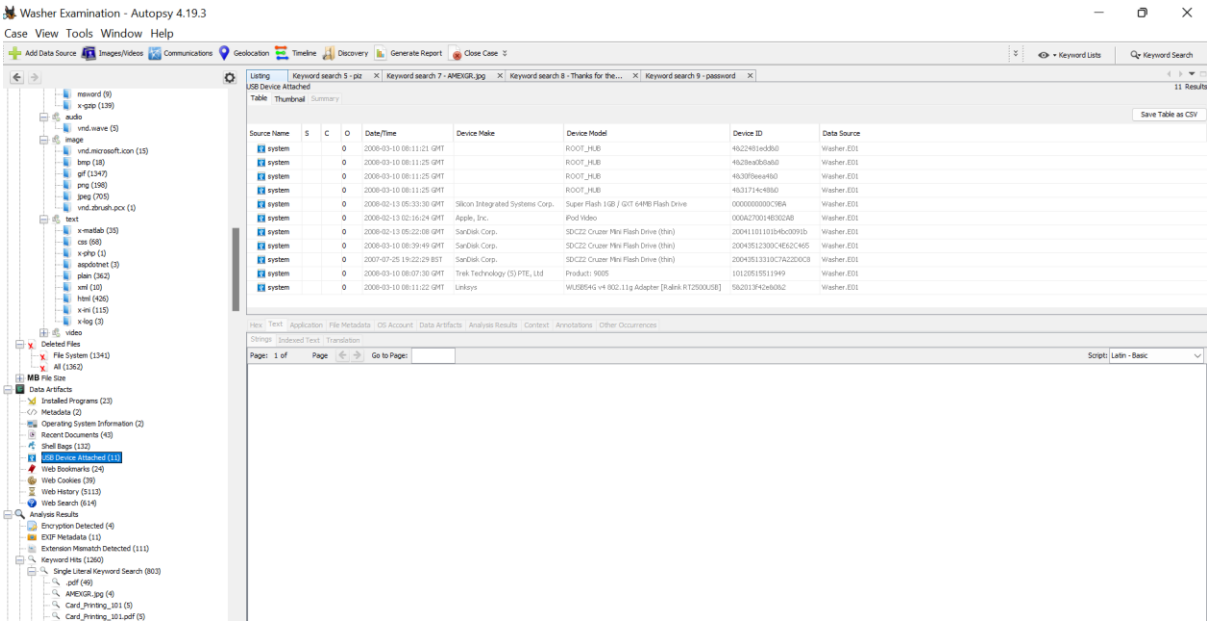


Figure 13: Attached USB Devices

The various USB gadgets that were connected to the machine are depicted above in figure 14.

6.10 Browser History

Below browser history was found on the suspect system. This is shown in Figure 15 below.

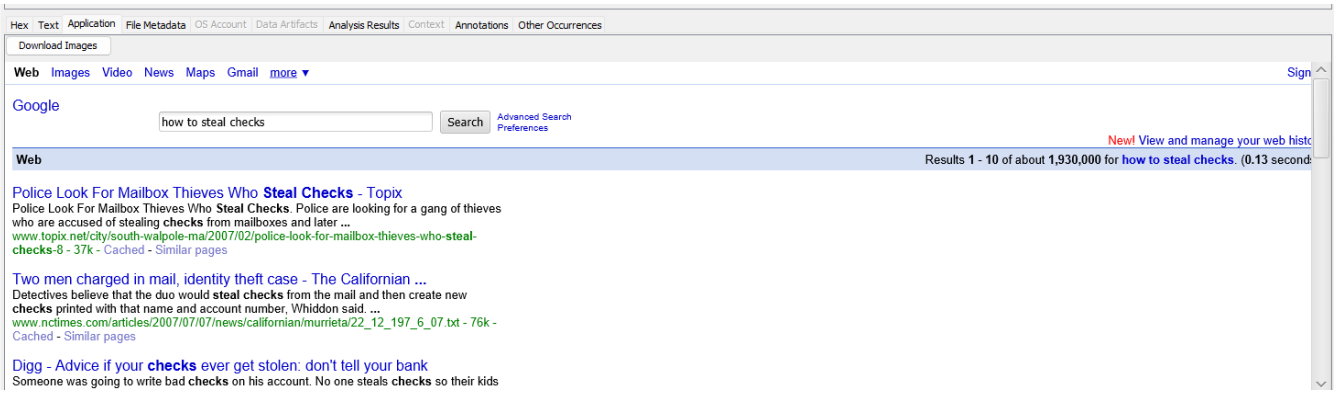


Figure 14: Browser History.

7.0 Evidence

This part contains some of the suspected criminal images and document extracted from the suspect's device.

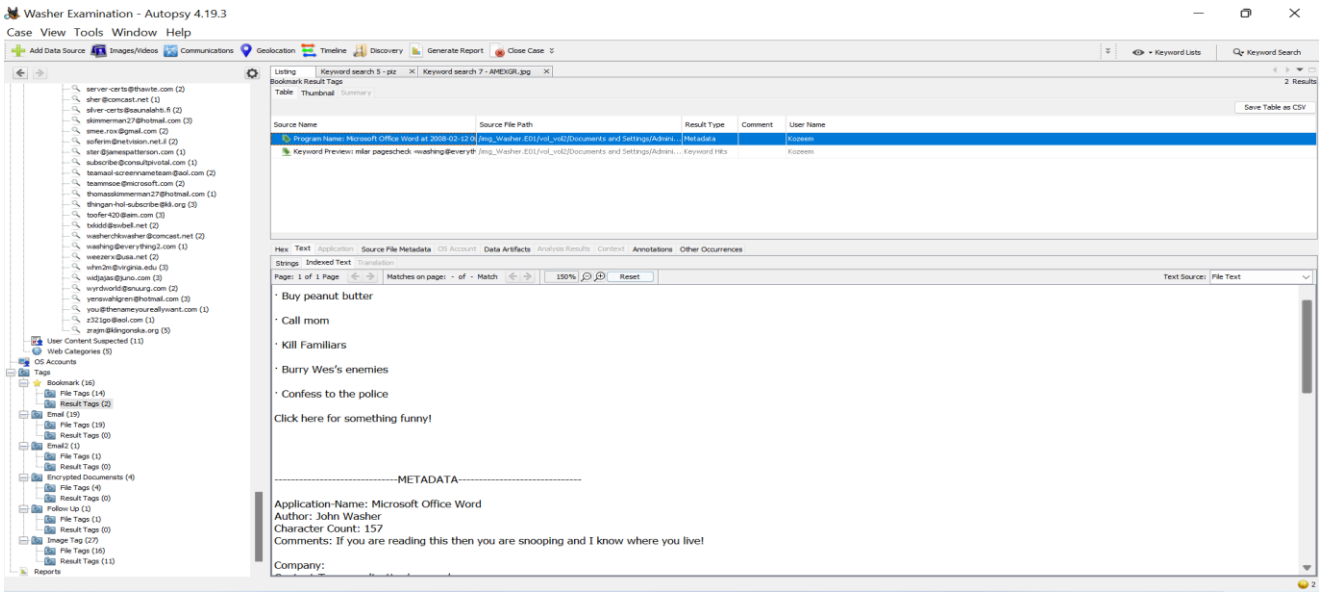


Figure 15: John Washer Todo List

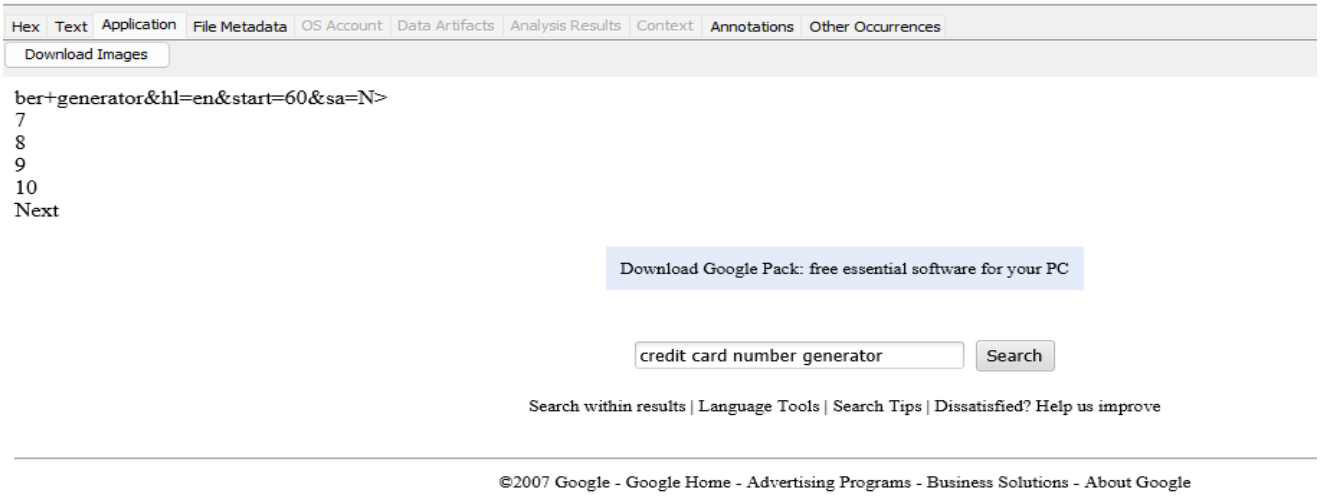


Figure 16: Web History of Credit Card Generator Search

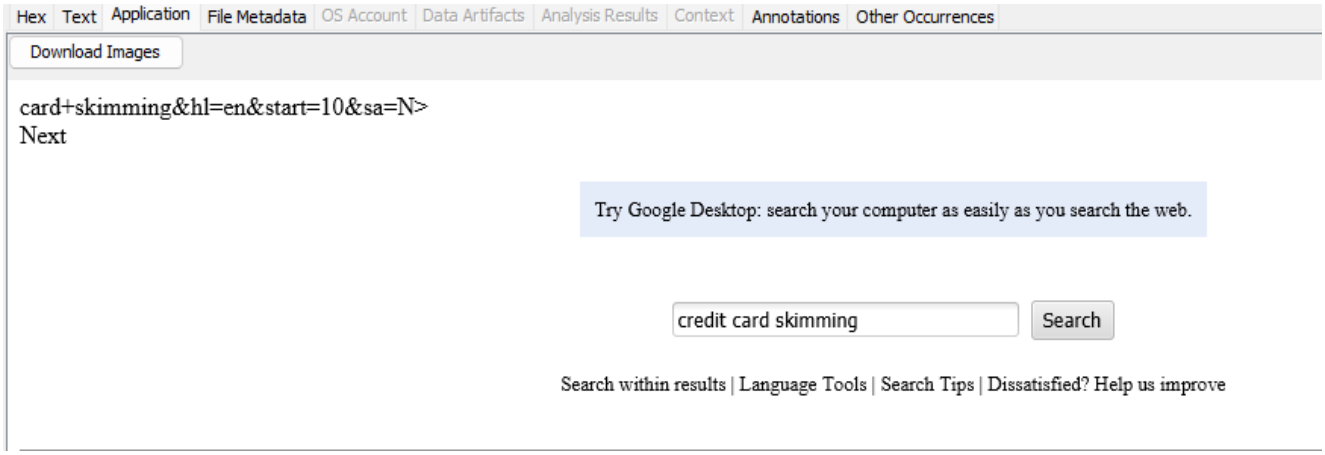


Figure 17: Web History of Credit Card Skimming Search

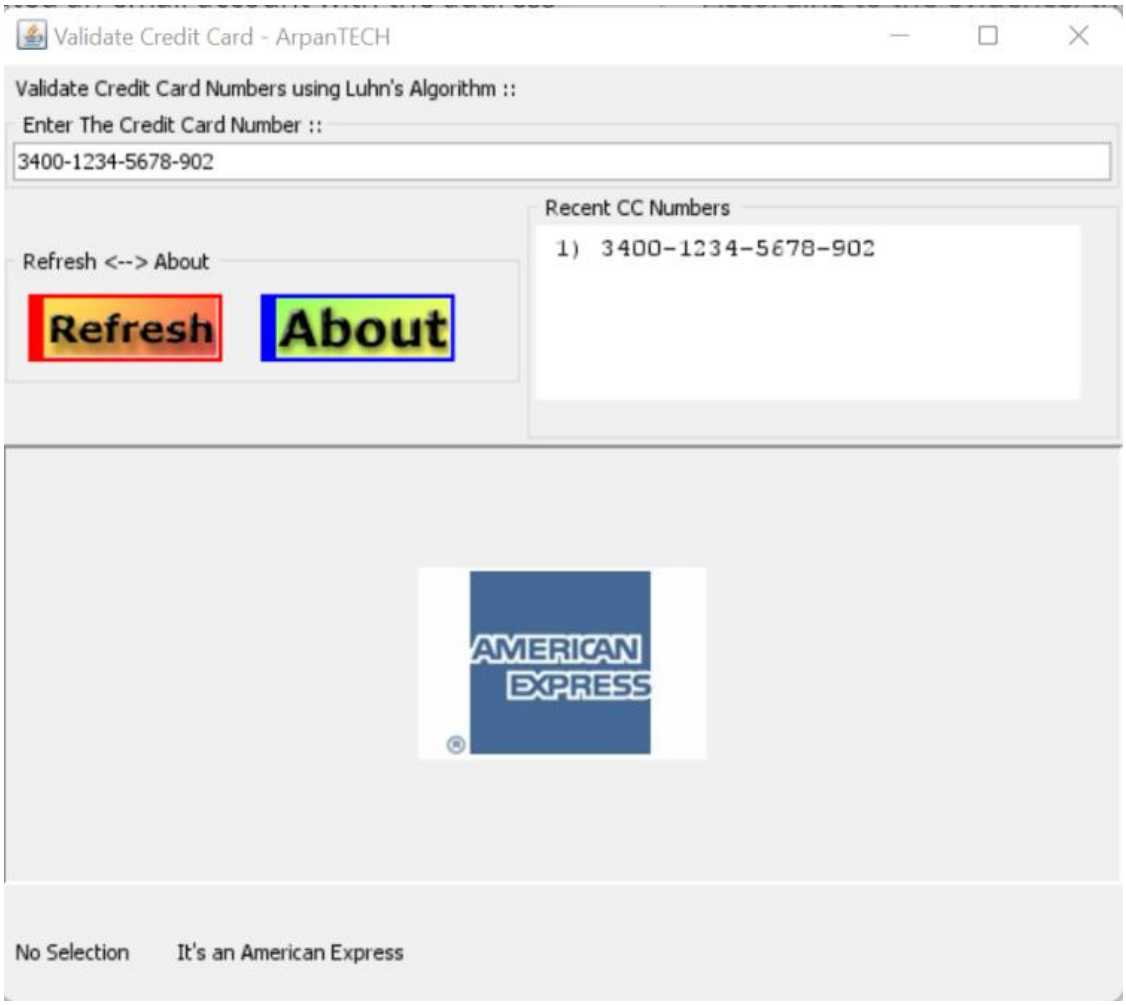


Figure 18: Credit Card Generator Application

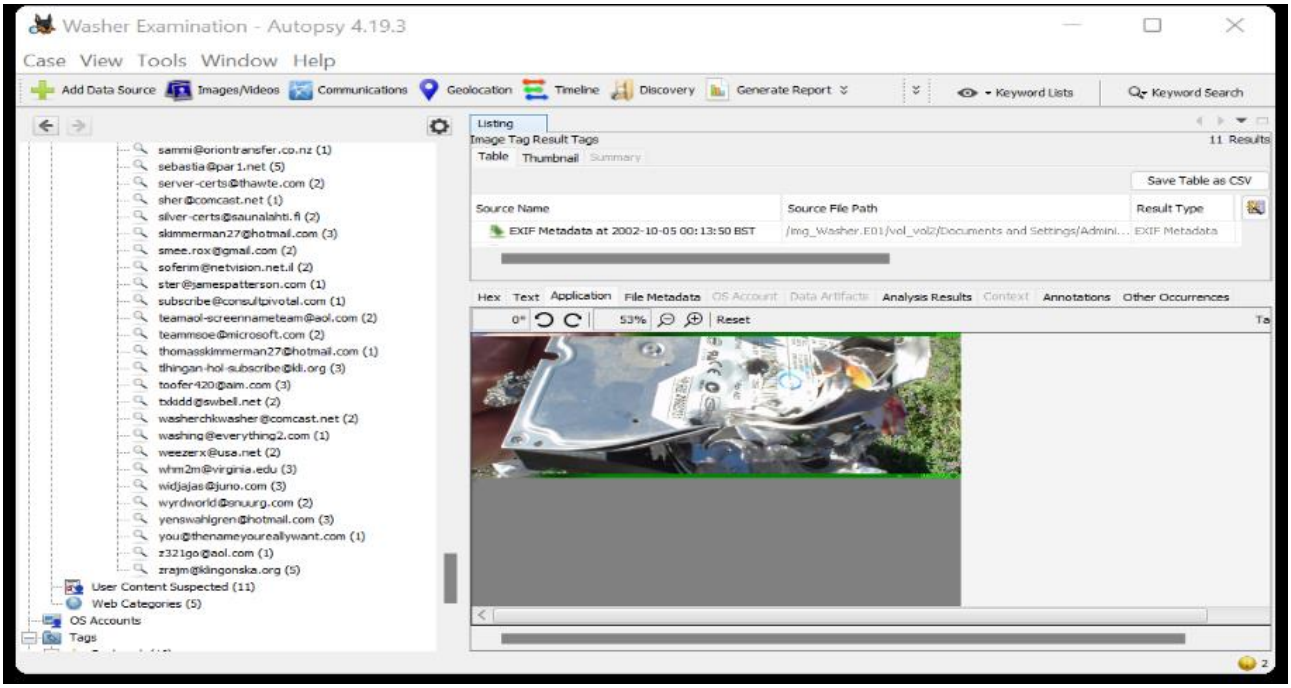


Figure 19: Damaged Hard Disk Drive

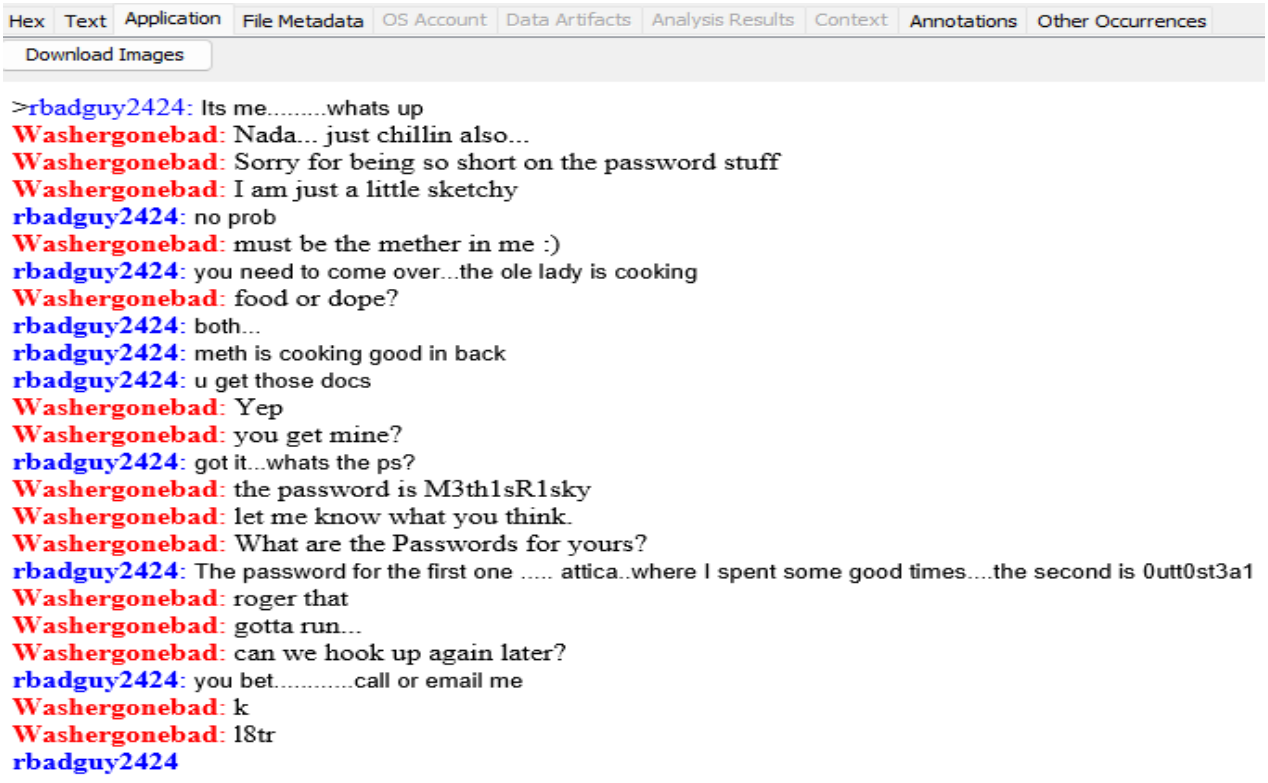


Figure 20: Conversation that reviewed the password for the protected document

7.1 Documents Evidence of Interest – Protected Documents

Four protected documents were found on the suspect computer which was further investigated. However, access to two of these documents was gained using the password "attica for SLIST.doc" and "0utt0st3a1 for How To Steal Credit Card Numbers.doc" as found in the message conversation between the suspect (John Washer) and Rbadguy2424(Rasco Badguy). As shown in Figure 10, this phenomenon can be seen to its full effect.

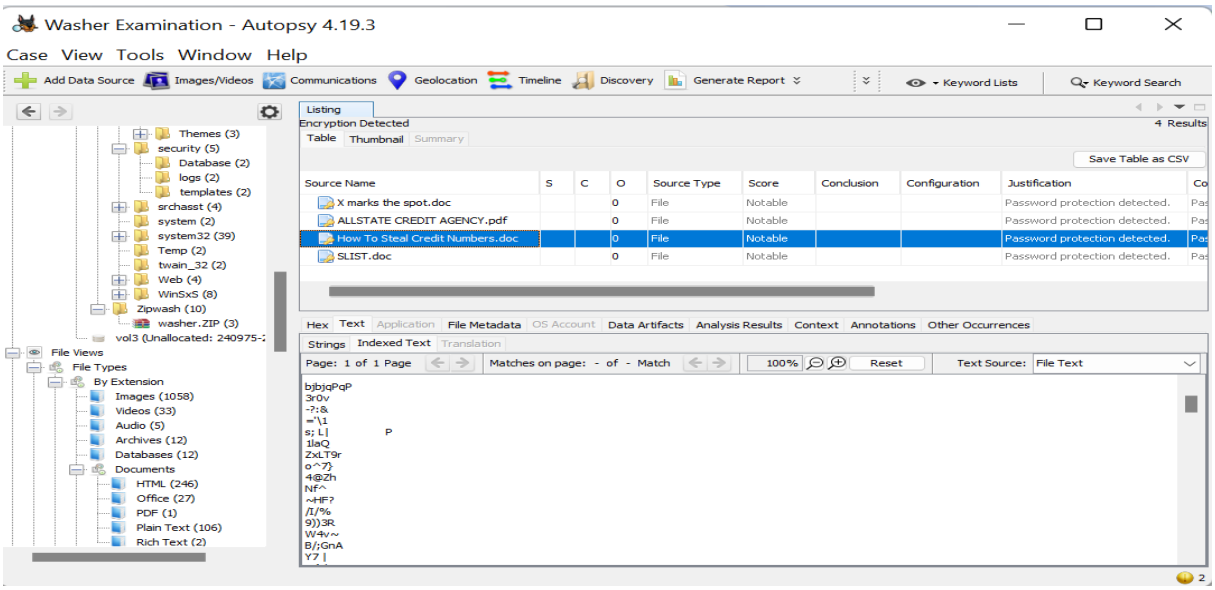
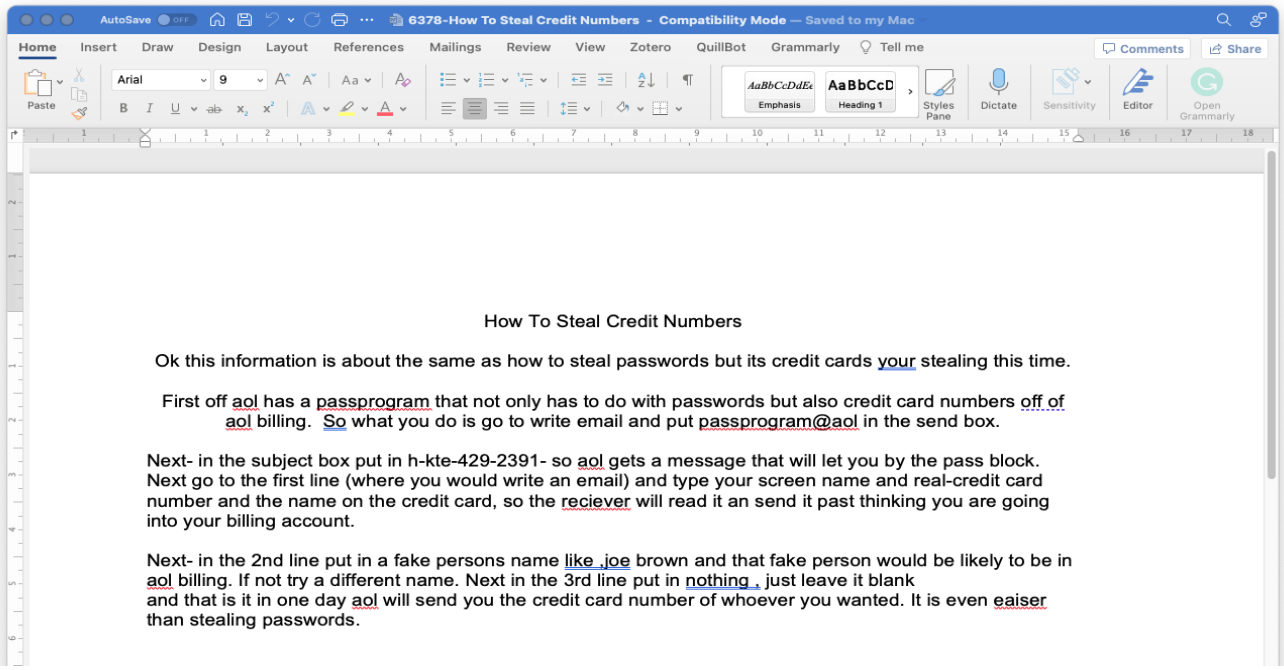


Figure 21: Protected Documents



How To Steal Credit Numbers

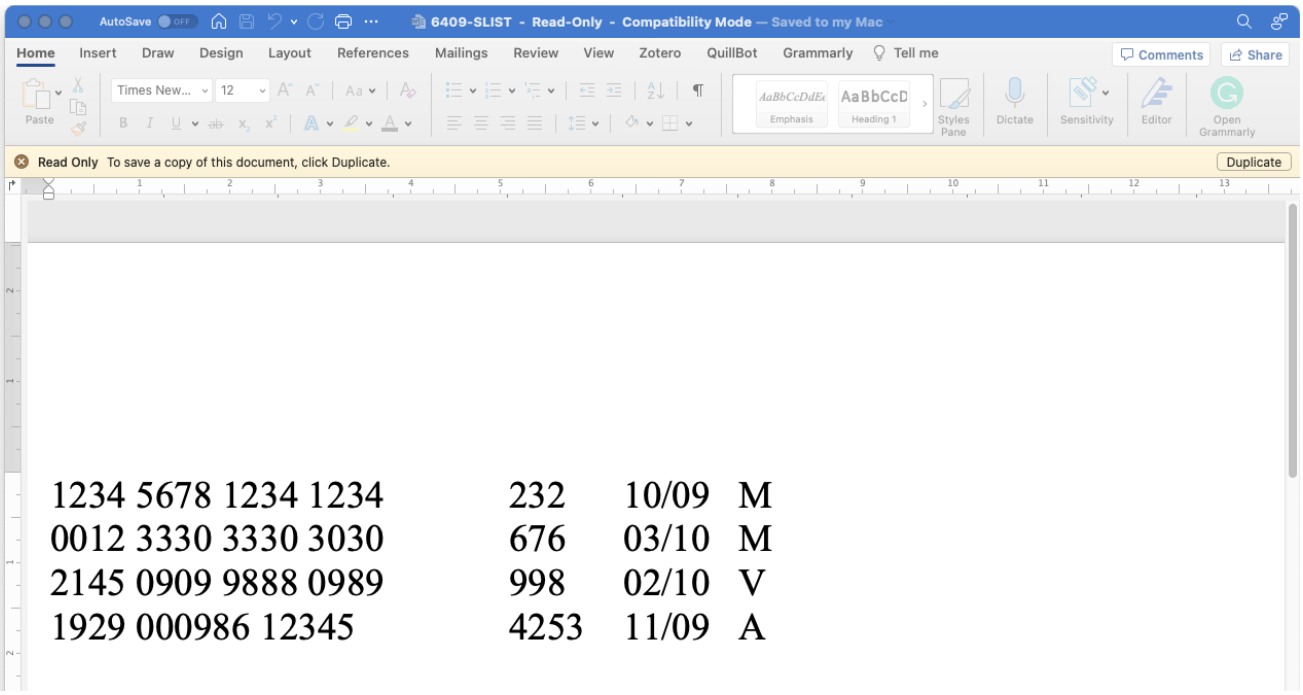
Ok this information is about the same as how to steal passwords but its credit cards your stealing this time.

First off aol has a passprogram that not only has to do with passwords but also credit card numbers off of aol billing. So what you do is go to write email and put passprogram@aol in the send box.

Next- in the subject box put in h-kte-429-2391- so aol gets a message that will let you by the pass block. Next go to the first line (where you would write an email) and type your screen name and real-credit card number and the name on the credit card, so the reciever will read it an send it past thinking you are going into your billing account.

Next- in the 2nd line put in a fake persons name like ,joe brown and that fake person would be likely to be in aol billing. If not try a different name. Next in the 3rd line put in nothing , just leave it blank
and that is it in one day aol will send you the credit card number of whoever you wanted. It is even eaiser than stealing passwords.

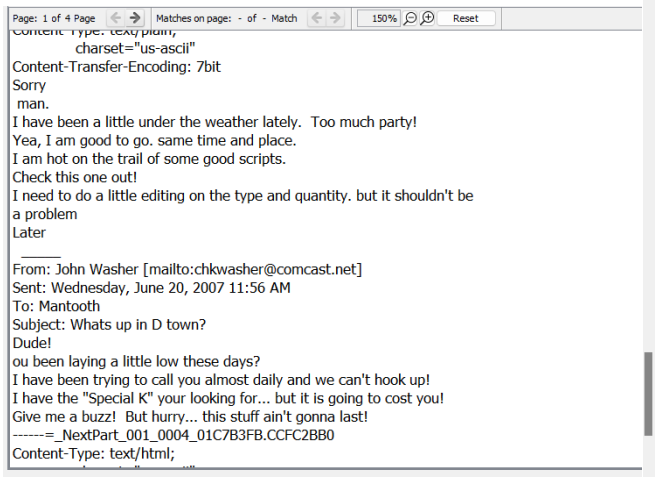
Figure 22: Stealing credit card document



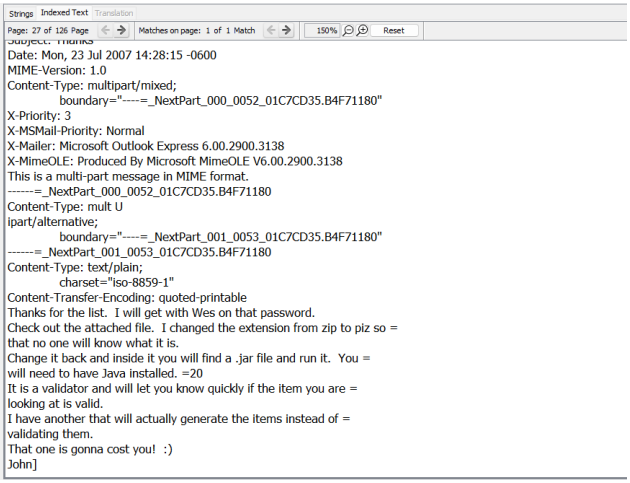
1234 5678 1234 1234	232	10/09	M
0012 3330 3330 3030	676	03/10	M
2145 0909 9888 0989	998	02/10	V
1929 000986 12345	4253	11/09	A

Figure 23: Credit Card Information Document

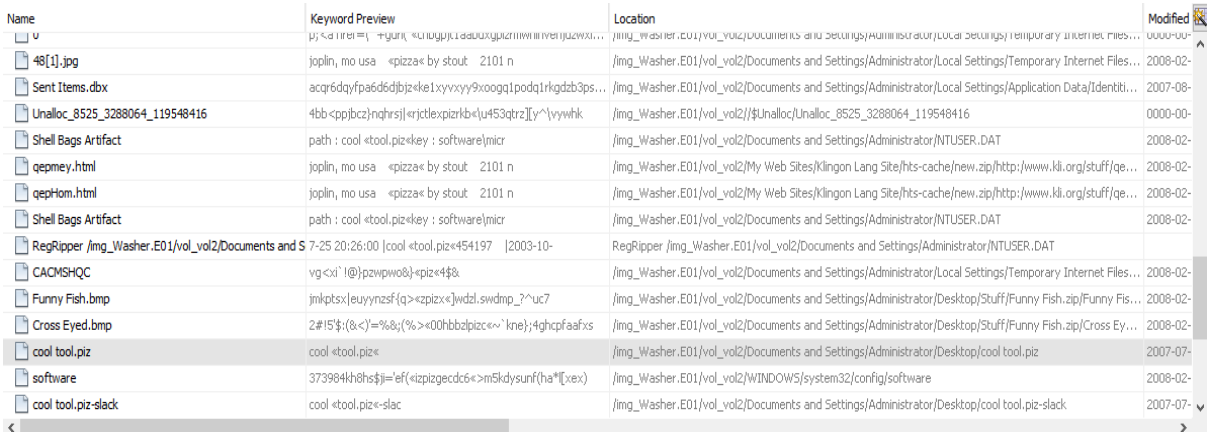
7.1.1 Email Evidence of Interest



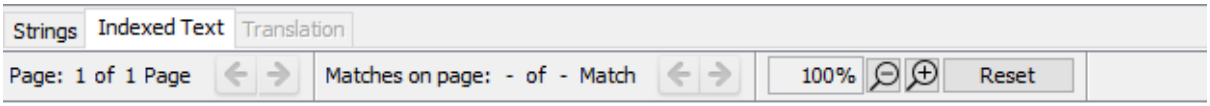
```
Page: 1 of 4 Page   Matches on page: - of - Match   150%   Reset
            charset="us-ascii"
Content-Transfer-Encoding: 7bit
Sorry
 man.
I have been a little under the weather lately.  Too much party!
Yea, I am good to go. same time and place.
I am hot on the trail of some good scripts.
Check this one out!
I need to do a little editing on the type and quantity. but it shouldn't be
a problem
Later
 _____
From: John Washer [mailto:chkwasher@comcast.net]
Sent: Wednesday, June 20, 2007 11:56 AM
To: Mantooth
Subject: Whats up in D town?
Dude!
ou been laying a little low these days?
I have been trying to call you almost daily and we can't hook up!
I have the "Special K" your looking for... but it is going to cost you!
Give me a buzz!  But hurry... this stuff ain't gonna last!
------=_NextPart_001_0004_01C7B3FB.CCFC2BB0
Content-Type: text/html;
```



```
Strings  Indexed Text  Translation
Page: 27 of 126 Page   Matches on page: 1 of 1 Match   150%   Reset
Date: Mon, 23 Jul 2007 14:28:15 -0600
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0052_01C7CD35.B4F71180"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.3138
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3138
This is a multi-part message in MIME format.
------=_NextPart_000_0052_01C7CD35.B4F71180
Content-Type: mult U
ipart/alternative;
        boundary="----=_NextPart_001_0053_01C7CD35.B4F71180"
------=_NextPart_001_0053_01C7CD35.B4F71180
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Thanks for the list.  I will get with Wes on that password.
Check out the attached file.  I changed the extension from zip to piz so =
that no one will know what it is.
Change it back and inside it you will find a .jar file and run it.  You =
will need to have Java installed. =20
It is a validator and will let you know quickly if the item you are =
looking at is valid.
I have another that will actually generate the items instead of =
validating them.
That one is gonna cost you!  :)
John]
```



Name	Keyword Preview	Location	Modified
48[1].jpg	joplin, mo usa «pizza« by stout 2101 n	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/Local Settings/Temporary Internet Files...	2008-02-
Sent Items.dbx	acqr6dqyfpa6d6djbjz«ke1xyvxyy9xoogq1podq1rkgdzb3ps...	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/Local Settings/Application Data/Identiti...	2007-08-
Unalloc_8525_3288064_119548416	4bb<ppjbcz}nqhrsj|«rjctlexpizrkb«\u453qtrz][y^\vywhk	/img_Washer.E01/vol_vol2//$Unalloc/Unalloc_8525_3288064_119548416	0000-00-
Shell Bags Artifact	path : cool «tool.piz«key : software\micr	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/NTUSER.DAT	2008-02-
qepmey.html	joplin, mo usa «pizza« by stout 2101 n	/img_Washer.E01/vol_vol2/My Web Sites/Klingon Lang Site/hts-cache/new.zip/http:/www.kli.org/stuff/qe...	2008-02-
qepHom.html	joplin, mo usa «pizza« by stout 2101 n	/img_Washer.E01/vol_vol2/My Web Sites/Klingon Lang Site/hts-cache/new.zip/http:/www.kli.org/stuff/qe...	2008-02-
Shell Bags Artifact	path : cool «tool.piz«key : software\micr	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/NTUSER.DAT	2008-02-
RegRipper /img_Washer.E01/vol_vol2/Documents and S	7-25 20:26:00 |cool «tool.piz«454197 |2003-10-	RegRipper /img_Washer.E01/vol_vol2/Documents and Settings/Administrator/NTUSER.DAT	
CACMSHQC	vg<xi`!@}pzwpwo8}«piz«4$&	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/Local Settings/Temporary Internet Files...	2008-02-
Funny Fish.bmp	jmkptsx|euyynzsf{q><pizx«]wdzl.swdmp_?^uc7	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/Desktop/Stuff/Funny Fish.zip/Funny Fis...	2008-02-
Cross Eyed.bmp	2#!5'$:(&<)'=%&;(%><00hbbzlpizc«~`kne};4ghcpfaafxs	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/Desktop/Stuff/Funny Fish.zip/Cross Ey...	2008-02-
cool tool.piz	cool «tool.piz«	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/Desktop/cool tool.piz	2007-07-
software	373984kh8hs$ji='ef(«izpizgecdc6«>mSkdysunf(ha*[xex)	/img_Washer.E01/vol_vol2/WINDOWS/system32/config/software	2008-02-
cool tool.piz-slack	cool «tool.piz«-slac	/img_Washer.E01/vol_vol2/Documents and Settings/Administrator/Desktop/cool tool.piz-slack	2007-07-



```
Strings  Indexed Text  Translation
Page: 1 of 1 Page   Matches on page: - of - Match   100%   Reset
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAy8my9gAAAEEANMeG6ytp8+fXaUHy/fFLMv3JLl0CDLA6heonMrBh7Twp2U0
ahyRhea3GT8TpRjtFhrYVgNUI8t9Y/Zj+e2njYHeZ5oTlM7/DQVp5sUAnMUi6Ygy
ABqge1VzSd4W43v9llUjpBdz0Smi2iQnJKdqkinUvu2CpCvlCiMiLUwbMW9pAAUR
tCxUaGUgS2xpbmdvbiBMYW5ndWFnZSBJbnN0aXR1dGUgPGtsaUBrbGkub3JnPokA
lQMFEDF2RQmEqSITH0YzbQEBcisEAKTFgtVkIZJZ9xpbbwczc+ip2+FlE6Xsm0o2
8AV+J94hdrzytDzNRBrqSR5gaG2WS6ckcaAxWV5WzSEOuQIR9dBHrQLsGr3k1+s7
By7mtE4Kzl0XCdKGfKvjFIfV2+tyOnVuszDaZPvmKpaZxGL0obEq8oui7HVNSngJ
Od1rl3XFiQCVAwUQL6uIACMiLUwbMW9pAQGsMgQAx3bP2zf+583PwfolBIpu/7GW
jwA4zQJs05phkthAiDXBeCRmNI8LoVOBsxoe/H24JXpXrrFfTNYJiFnAS/qMOOA/
nIAjwEJqYGdO9I08kkk4o5RjuD55HAXdIneb0pQDHgq848t5snmPRBdO136HsCeu
apDQ05iq20WisrNzqXGJAJUDBRAvdwttXhPpMM4AzmUBAWy6A/4raEUyGSvN+rER
u4pQlxgSPvkqZBf82Q1v0/kFseIhGzOwtWi5L/TO1sFawKFiXnM2Kcnd+PkReEDG
Z8ND9tBFrb4+r6oMzPuj32et1v0vvseTc/WFFukq6btTNHpfTRTYMOiUxPczpm+6
mnSrC/esy4jWnnQcKG6R5YCEVZ1jvYkAlQMFEC8m0A/YyHdxQpwH4QEBEqYD/jhW
m65f88bh6/f2IMClrpTeSezaJQ72x2DHN1k7dcOm5Ln3w6uJa/lD6hHUPB9M7F3j
kCLg9xrtfMIuHK4sNx0NN0P/E0g3ilxRpXzXr+/HiU/k5VDuT4OLjXaVmEHrPb+A
H+A7FZ9xRPg6eKzTcvWfmSFVaAcDx6IYOlYM8hgY
=WtvI
-----END PGP PUBLIC KEY BLOCK-----
```

----------METADATA----------

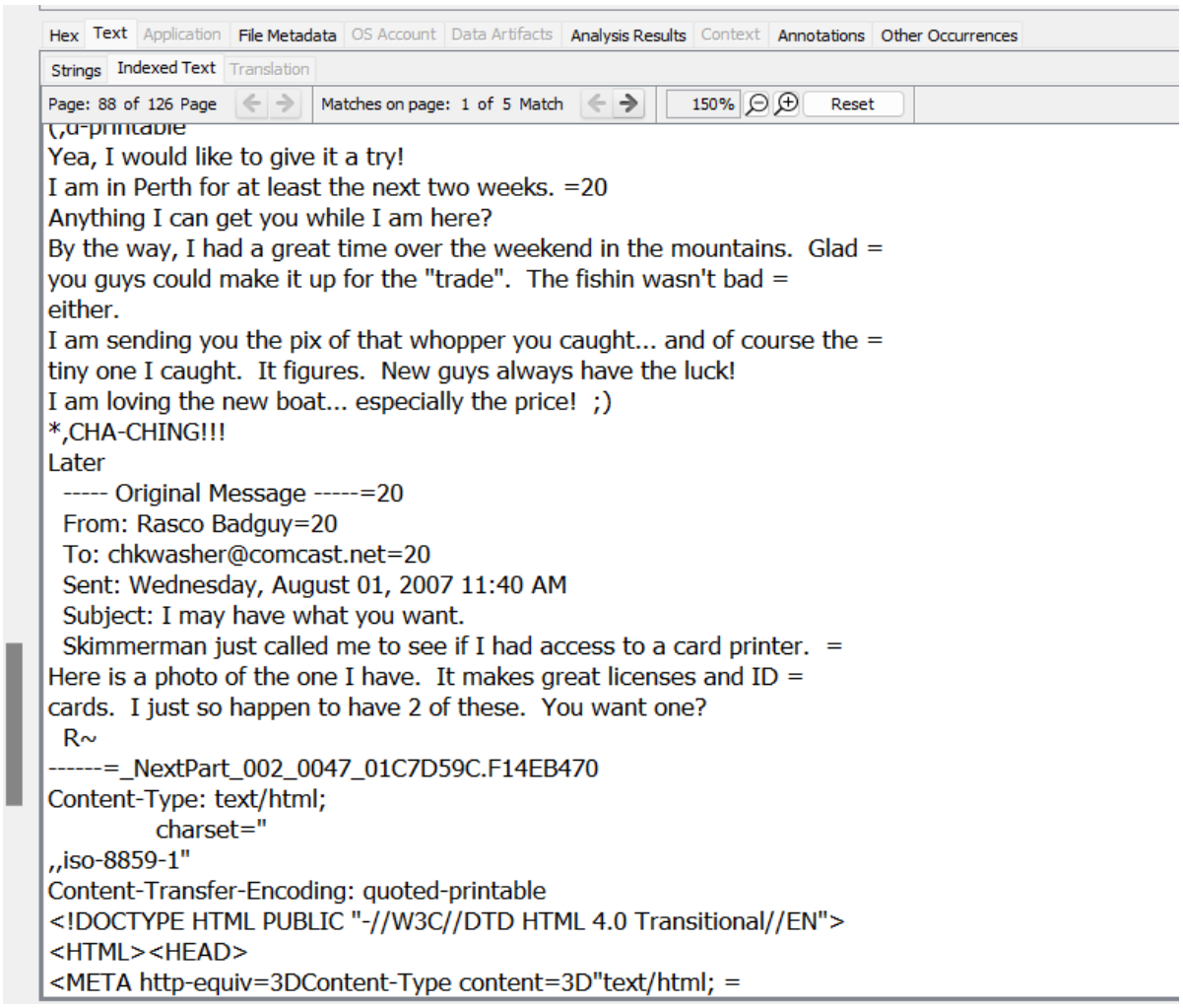


Figure 24: Email Conversations

7.2 **Autopsy Report**

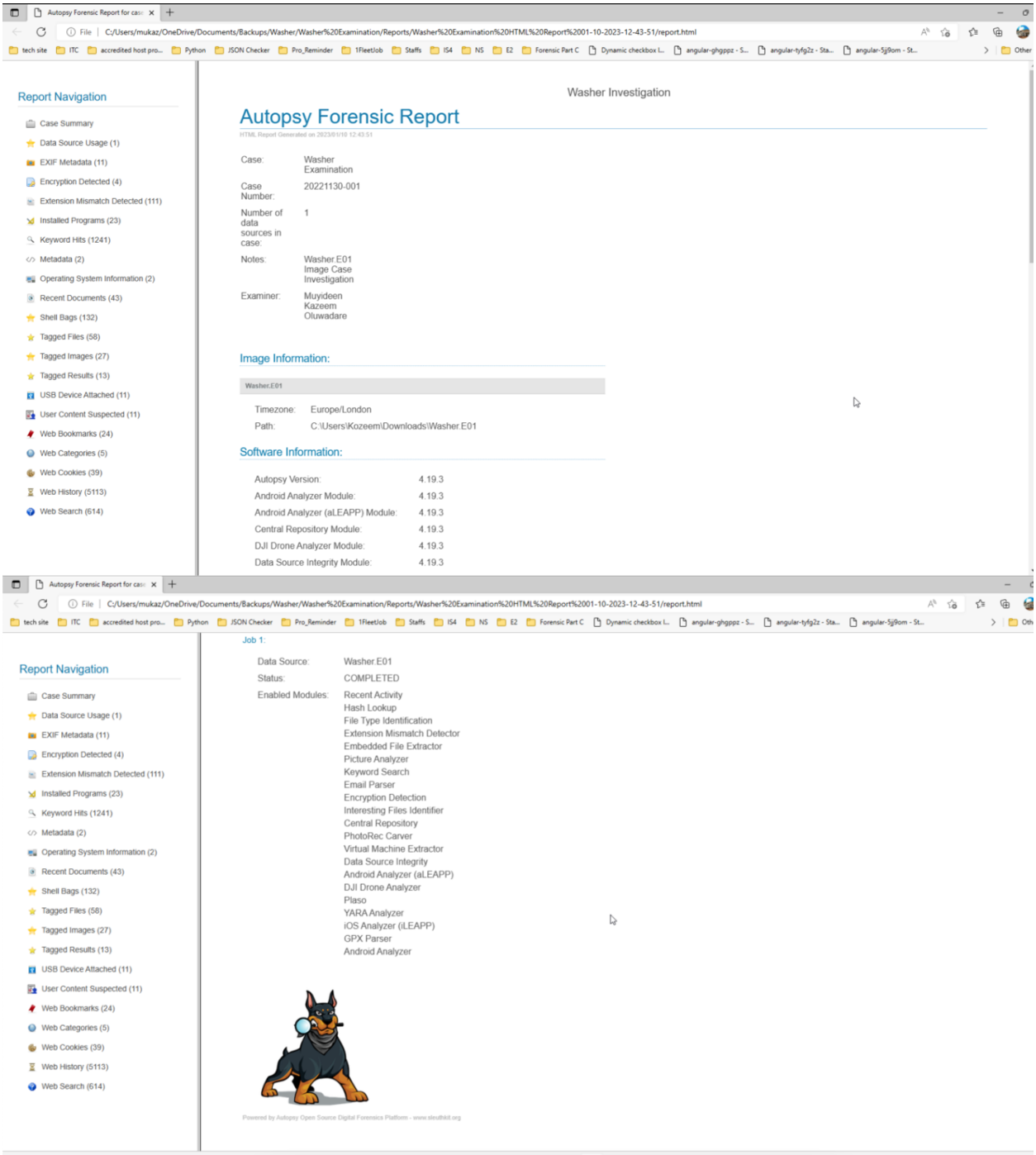


Figure 25: Autopsy Report

8.0 **Summary of Findings**

Table 4 is a summary of discovered activities with timestamps showing when the events were recorded with specific events. Furthermore, a document (see Figure 15) on the suspect system is uncovered stating that he wanted to confess to the police. The SOP step 8 discusses the important of this part which was followed for the presentation of this summary.

Table 5: Tale of Criminal Activity

Date/Time	Event / File name	Detail
10-03-2008 23:44:32	Time Zone	The suspect time zone is Europe/London
25-07-2007 02:16:06	OS installation	The first time the Operating System was installed was on the 25th July 2007 at 02:16:06. Under the Owner John Washer
25-07-2007 01:12:58	Suspicious Application Programme	Fontcore and MobileOptionPack are software application install, which are used to steal users' passwords and financial data.
01-08-2007 02:13:27 – 06:00	Email exchanges	The suspect's email address was chwasher@comcast.net, according to evidence. He emailed Mr. Smee and Rasco Badguy. The participants discussed writing script to create credit cards, validating the generated credit card information, and printing it on a card using a card printer.
25-07-2007 21:26:37	Documents	A password-protected document was found during the investigation which was open using the discovered password (see Figure 20) to unlock two of the documents where one contains the credit information(2 Mastercard, 1 VISA card and 1 AMEX) and the second document contain instructions of how to steal credit cards. In addition, the suspect must give his or her consent before the investigator can request the password. SLIST.doc, How to steal a credit number.doc, and X marks the spot.doc are the files in question.

(04-08-2007 02:18:00) (04-08-2008 02:15:03) (13-02-2008 01:13:46)	User Profile	The suspect's use of multiple user accounts for criminal purposes is also uncovered. Mr. Samee, The Wolf, and Artimus are just a few of the usernames used.

9.0 Conclusion

According to the evidence, a total number of 1,362 files are deleted files was discovered from the suspect machine, however, the suspect used the email address 'chwasher@comcast.net' in his or her criminal activities and has perform some email exchanges with Mr. Smee (smee.rox@gmail.com) and Rasco Badguy (txkidd@swbell.net) as shown if Figure 20 where several tidbits of their exchange are included and the analysis of these conversations revealed that the participants were talking about writing script to create credit cards, how to validate the generated credit card information, and discussing how to print the credit information generated on a card using a card printer. The figures 20 through figure 22 depict this discussion and the application created with the script. Conversely, the evidence extracted from the image shows that the machine user account “Mr. Smee” is associated with Mr. John Washer (the suspect). Pictures, emails, and browsing histories extracted from the file depict the users’ interests in various criminal activities such as credit card fraud, checks and stealing of credit cards, and producing fake credit cards. The suspect was also found to be exchanging encrypted messages with his co-conspirators. However, after critically analysis of all these acquire evidence, it is hereby recommended to report all these suspicious activities to the law enforcement agency for proper judgement in the court of law even though it was found out that he wanted to report himself (see figure 15) to the police after all his illegal activities.

References

ACPO (2011). *2 NOT PROTECTIVELY MARKED ACPO Good Practice Guide for Digital Evidence*. [Online]. Available from:https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf. [Accessed: 20 November 2022].

Aguilar, J., Barnes, T., Browne, J., Kennedy, A., Miranda, R., Williams, S., Burney, Y., Byrd, J., Carver, B., McClaren, J., McElroy, R., Denmark, A., Mount, M., Halla, S., Hartman, L., Mohr, K., Leben, D., Matheson, G., Sigel, S., Smither, J., Taylor, M. & Watts, A. (2013). *Forensic science laboratories : handbook for facility planning, design, construction, and relocation*. [Online]. Gaithersburg, MD. Available from: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7941.pdf.

Al-Dhaqm, A., Ikuesan, R.A., Kebande, V.R., Razak, S.A., Grispos, G., Choo, K.K.R., Al-Rimy, B.A.S. & Alsewari, A.A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE Access*. 9. p.pp. 152476–152502.

Balu, R. (2022). *Bangladesh Bank Cyber Heist: Incident Analysis*. [Online]. Available from: www.swift.com.

Centre for Responsible Business, M. (2013). *Myanmar ICT Sector Wide Impact Assessment: Chapter 4.5 - Cyber-Security*. [Online]. Available from: www.myanmar-responsiblebusiness.org.

FBI (2022). *DIGITAL FORENSIC EXAMINER An Inside Look*. [Online]. Available from: https://www.fbijobs.gov/sites/default/files/2022-05/Digital%20Forensic%20Examiner.pdf. [Accessed: 18 November 2022].

Institute of Electrical and Electronics Engineers & IEEE Communications Society (2017a). *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) : 22-24 March 2017, Chennai, India*.

Institute of Electrical and Electronics Engineers & IEEE Communications Society (2017b). *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) : 22-24 March 2017, Chennai, India*.

ISO/IEC (2021). *ISO/IEC Directives, Part 2 — Principles and rules for the structure and drafting of ISO and IEC documents*. [Online]. 1 October 2021. ISO/IEC. Available from:

https://www.iso.org/sites/directives/current/part2/index.xhtml. [Accessed: 14 January 2023].

Lin, A.C., Lin, I.L., Lan, T.H. & Wu, T.C. (2022). *Establishment of the Standard Operating Procedure (SOP) for gathering digital evidence*. [Online]. 2022. Proceedings - First International Workshop on Systematic Approaches to Digital Forensic Engineering. Available from: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=1592522&ref=. [Accessed: 26 November 2022].

Metropolitan Police Service (2022). *Digital Forensics Lab Manager - Police Careers (MET)*. [Online]. 2022. Metropolitan Police Service. Available from: https://policecareers.tal.net/vx/mobile-0/appcentre-External/brand-3/candidate/so/pm/6/pl/1/opp/5435-Digital-Forensics-Lab-Manager/en-GB. [Accessed: 18 November 2022].

National Institute of Standards and Technology (2022). *Digital evidence | NIST*. [Online]. 2022. National Institute of Standards and Technology (NIST). Available from: https://www.nist.gov/digital-evidence. [Accessed: 17 November 2022].

NCSC & NCA (2017). *The cyber threat to UK business*.

Nigel Jones, Victor Volzow, Andrea Bradley & Branko Stamenkovic (2016). *Digitak Forensics Laboratory Management and Procedures Guide*. [Online]. 26 October 2016. Council of Europe. Available from: https://rm.coe.int/16806b3058. [Accessed: 25 November 2022].

NIST (2022). *Standard Operating Procedures | NIST*. [Online]. 4 May 2022. National Institute of Standards and Technology. Available from: https://www.nist.gov/pml/owm/laboratory-metrology/standard-operating-procedures. [Accessed: 10 January 2023].

NPCC (2020). Digital Forensic Science Strategy 2020. *Digital Forensic Science Strategy*.

Office of Justice Programs & Institute of Justice, N. (2022). *Forensic Laboratories: Handbook for Facility Planning, Design, Construction, and Moving*. [Online]. Available from: http://www.ojp.usdoj.gov. [Accessed: 25 November 2022].

Ramadhani, S.S., Saragih, Y.M., Mh, S.H., Rahim, R., Tinggi, S., Putera, A., Siahaan, U. & Ramadhani, S. (2017). *Heuristic Function Influence to the Global Optimum Value in Shortest Path Problem View project Bit Error Detection and Correction with Hamming Code View project Post-Genesis Digital Forensics Investigation*. [Online]. 6 (3). p.pp. 164–166. Available from: https://www.researchgate.net/publication/318786117.

Rosselina, L., Suryanto, Y., Hermawan, T. & Alief, F. (2020). Framework design for the retrieval of instant messaging in social media as electronic evidence. In: *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*. 1 October 2020, Institute of Advanced Engineering and Science, pp. 209–215.

SalvationData Technology (2022). *Computer Forensics Lab: 7 Golden Design Rules for Optimal Working Conditions - Salvation DATA*. [Online]. 2022. Salvation Data Technology. Available from: https://www.salvationdata.com/work-tips/computer-forensics-lab-7-golden-design-rules-for-optimal-working-conditions/. [Accessed: 21 November 2022].

San Jose State University (2022). *Computer Forensic Analyst Job Description*. [Online]. 2022. San Jose State University - Computer Science Department. Available from: https://www.cs.sjsu.edu/jobs/eforinc.htm. [Accessed: 18 November 2022].

Study.com (2022). *Digital Forensic Imaging: Types & Examples - Video & Lesson Transcript | Study.com*. [Online]. 2022. Study.com. Available from: https://study.com/academy/lesson/digital-forensic-imaging-types-examples.html. [Accessed: 18 November 2022].

The Forensic Science Regulator (2020). *Codes of Practice and Conduct Appendix: Digital Forensic Services FSR-C-107 Issue 2*. [Online]. Available from: https://www.gov.uk/government/organisations/forensic-science-regulator. [Accessed: 20 November 2022].

Annex A – Chain of Custody

DESCRIPTION OF EVIDENCE				
Item #	**Quantity**	**Case Established By**	**Date/Time**	**Description of Item (Model, Serial #, Condition)**
1	1	Nick Drehel	10.03.1998 23:44:32	Washer.E01 and MD5 Hash Values

CHAIN OF CUSTODY				
Item #	**Date/Time**	**Released By** Signagture & ID #	**Received By** Signagture & ID #	**Comment/Location**
1	13.01.2023 - 23.59	Muyideen Kazeem Oluwdare - 21027842L	Digital Forensic Fundamental Staff COCS70704	For Examination and Analysis - Lab S520 Digital Forensic Fundamental Blackboard

(See SOP step 4)