Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea in Informatica

Cancellazione Sicura dei Dati: Analisi di Normative e Tecnologie per lo Sviluppo di una Procedura Operativa

Tesi di Laurea Triennale

Relatore

Prof. Marco Zanella

Laureando

Giovanni Moretti

Matricola 1217655

Anno Accademico 2023-2024

© Giovanni Moretti, Dicembre 2024. Tutti i diritti riservati. Tesi di Laurea Triennale: "*Cancellazione Sicura dei Dati: Analisi di Normative e Tecnologie per lo Sviluppo di una Procedura Operativa*", Università degli Studi di Padova, Dipartimento di Matematica "Tullio Levi-Civita".

Ringraziamenti

Desidero esprimere la mia gratitudine al professor Marco Zanella, mio relatore, per l'aiuto e il sostegno che mi ha dato durante la stesura dell'elaborato.

Vorrei anche ringraziare i miei genitori per il loro sostegno durante gli anni di studio.

Padova, Dicembre 2024 *Giovanni Moretti*

Sommario

Questa tesi rappresenta la relazione del progetto di tirocinio svolto presso SIES, avente come obiettivo lo sviluppo di una procedura per la cancellazione sicura dei dati. L'importanza della protezione dei dati sensibili, unita all'esigenza di conformità alle normative vigenti e agli standard internazionali di sicurezza, rende cruciale l'implementazione di soluzioni che garantiscano l'eliminazione definitiva dei dati. Il progetto si articola in diverse fasi. In primo luogo, è stata condotta un'analisi approfondita delle normative rilevanti, e delle best practices per la protezione dei dati. Successivamente, sono state valutate le tecnologie esistenti per la cancellazione sicura dei dati, confrontando soluzioni commerciali e open source in termini di efficacia, costi e conformità. A partire da queste analisi, è stata sviluppata una procedura operativa, finalizzata a fornire un servizio sicuro e conforme alle normative per l'eliminazione definitiva dei dati aziendali.

Indice

1 Introduzione **1**

1.1 L'azienda 1

1.2 L'offerta di stage 2

1.3 Organizzazione del testo 2

2 Descrizione dello stage **3**

2.1 Introduzione al progetto 3

2.2 Contenuti formativi previsti 3

2.3 Prodotti attesi 4

2.4 Pianificazione 5

3 Analisi di Normative, Standard e Best Practices, nell'ambito della Cancellazione Sicura **7**

3.1 La necessità della cancellazione dei dati 7

3.2 Classificazione delle tecniche di cancellazione 8

3.3 Supporti e relative tecniche di cancellazione proposte nel NIST SP 800-88 9

3.4 L'efficacia degli algoritmi di sovrascrittura 11

3.4.1 Sovrascrittura dei dispositivi magnetici (HDD) 11

3.4.2 Sovrascrittura dei dispositivi a stato solido (SSD) 12

4 Analisi delle Tecnologie **14**

4.1 Criteri di selezione 14

4.1.1 Compatibilità del sistema operativo 14

4.1.2 Supporto hardware 15

4.1.3 Usabilità e funzionalità aggiuntive 15
4.1.4 Costi e licenze 15
4.2 Metodologia di test 15
4.2.1 Tecnologie utilizzate per il processo di test 16
4.2.2 Processo sperimentale 16
4.3 Prodotti software presi in analisi 17
4.3.1 Remo Drive Wipe 17
4.3.2 Active KillDisk 18
4.3.3 ShredOS (nwipe) 18
4.3.4 PartedMagic 19
4.3.5 BleachBit 20
4.4 Tabella comparativa 22
4.5 Conclusioni e scelta 22

5 Descrizione della Procedura 23
5.1 Tecnologie utilizzate 23
5.1.1 ShredOS 23
5.1.2 Nwipe 24
5.1.3 Hdparm 24
5.1.4 Nvme-cli 24
5.2 Preparazione della live USB 25
5.2.1 Download e configurazione 25
5.2.2 Montaggio dell'immagine sul supporto 26
5.3 Procedura di cancellazione 27
5.3.1 Cancellazione dei dischi rigidi 27
5.3.2 Cancellazione dei dischi a stato solido 28
5.3.2.1 Dischi SSD ATA 28
5.3.2.2 Dischi SSD NVMe 29
5.4 Certificato di cancellazione 30

6 Verifica della procedura 31
6.1 Processo sperimentale 31
6.1.1 Selezione dei dispositivi e loro preparazione 31

6.1.2 Esecuzione della procedura 31
6.1.3 Creazione dell'immagine del disco 32
6.1.4 Verifica con WinHex 32
6.1.5 Verifica con Autopsy 32
6.2 Risultati dei test 33

7 Conclusioni **34**
7.1 Consuntivo finale 34
7.2 Raggiungimento degli obiettivi 36
7.3 Conoscenze acquisite e valutazione personale 36

Glossario **i**

Bibliografia **iii**

Elenco delle figure

1.1 Logo di SIES 1

4.1 Logo di USB Write Blocker, WinHex Hex Editor, Autopsy e OSForensics 16

5.1 Schermata di creazione del supporto avviabile con Rufus 27

5.2 Schermata iniziale di nwipe 28

Elenco delle tabelle

4.1 Tabella comparativa delle tecnologie analizzate 22

7.1 Consuntivo finale 35

Capitolo 1

Introduzione

Il presente documento è relativo al lavoro di tirocinio curricolare svolto presso l'azienda SIES. In questo capitolo introduttivo vengono presentati il contesto aziendale, l'offerta di stage e l'organizzazione del testo.

1.1 L'azienda

SIES è un'azienda operante nel settore *ICT* $_G$, specializzata nella progettazione e gestione di infrastrutture IT per clienti aziendali.
Si occupa di infrastrutture di rete, gestione dati, sicurezza informatica e servizi di hosting, con una particolare attenzione alla continuità operativa e alla protezione delle informazioni aziendali.
L'azienda supporta i propri clienti con soluzioni di gestione server, dispositivi, servizi di sicurezza e tecnologie di *backup* e *disaster recovery*.

Figura 1.1: Logo di SIES

1.2 L'offerta di stage

SIES offre già da tempo diversi servizi nell'ambito della gestione dei dati personali e della conformità al regolamento europeo sulla protezione dei dati. L'idea dello stage nasce dalla volontà di integrare e ampliare questo tipo di offerta, sviluppando un servizio per la cancellazione sicura dei dati.

1.3 Organizzazione del testo

Il documento, organizzato in sette capitoli, è strutturato come segue:

Il secondo capitolo descrive il progetto di stage, i suoi obiettivi e la sua pianificazione.

Il terzo capitolo riguarda l'analisi di norme, standard e documenti tecnici, in materia di cancellazione dei dati.

Il quarto capitolo analizza le tecnologie proprietarie e open source per la cancellazione dei dati.

Il quinto capitolo descrive la procedura realizzata.

Il sesto capitolo delinea i processi di verifica e validazione, e presenta i risultati di test riguardanti la procedura.

Nel settimo capitolo vengono tratte le conclusioni del progetto di stage.

Riguardo la stesura del testo, relativamente al documento sono state adottate le seguenti convenzioni tipografiche:

- gli acronimi, le abbreviazioni e i termini ambigui o di uso non comune menzionati vengono definiti nel glossario, situato alla fine del presente documento;
- i termini in lingua straniera o facenti parti del gergo tecnico sono evidenziati con il carattere *corsivo*.

Capitolo 2

Descrizione dello stage

2.1 Introduzione al progetto

SIES gestisce la fornitura di computer e postazioni per vari clienti. Fornisce anche servizi sicurezza informatica, e soluzioni di privacy, supportando i propri clienti nel proteggere e gestire i dati sensibili.
SIES ha deciso di integrare questi servizi sviluppando una procedura da offrire ai propri clienti per la rimozione sicura dei dati personali.
Per definire una procedura conforme alle normative vigenti e adeguatamente sicura, il progetto prevede anche uno studio delle normative stesse e un'analisi della letteratura inerente.

2.2 Contenuti formativi previsti

Il principale contenuto formativo del progetto di stage è approfondire l'ambito della sicurezza informatica, con particolare focus sulla cancellazione sicura dei dati. Saranno affrontati temi come le tecnologie per la cancellazione sicura di supporti di memorizzazione, sia commerciali che *open source*, e le principali normative di riferimento, tra cui la ISO/IEC 27001 [1]. Verranno acquisite competenze nella progettazione di procedure operative, nella gestione di un progetto IT e nell'esecuzione di test per valutare l'efficacia delle soluzioni adottate.

2.3 Prodotti attesi

I prodotti attesi, definiti nel piano di lavoro, sono:

1. **Documento di obiettivi del progetto**
   Un documento che descriva gli obiettivi principali del progetto, includendo le esigenze e le richieste emerse durante le fasi preliminari di analisi e confronto con i referenti interni.

2. **Documento di scelta delle tecnologie**
   Relazione tecnica che documenti il processo di selezione delle tecnologie utilizzate per la cancellazione sicura dei dati. Dovrà includere una valutazione comparativa delle soluzioni analizzate, sia commerciali che *open-source*, e giustificare la scelta finale in base a criteri di efficacia, conformità alle normative e costi. Inoltre, sarà necessario includere evidenze sull'efficacia delle soluzioni scelte attraverso test documentati.

3. **Procedura operativa**
   Un documento interno che descriva in dettaglio la procedura di cancellazione sicura definita durante il progetto. Questo documento dovrà essere completo di tutte le fasi operative, dalla preparazione dei supporti di memorizzazione alla verifica finale dell'effettiva cancellazione, con riferimenti alle *best practices* e alle normative ISO/IEC 27001.

4. **Certificazione di cancellazione**
   Template per la certificazione di avvenuta cancellazione sicura dei dati. Questo documento servirà a garantire e attestare che il processo di eliminazione dei dati è stato eseguito in conformità alle procedure stabilite e alle normative vigenti.

5. **Scheda di servizio**
   Un documento esterno destinato a descrivere e presentare il servizio al cliente. Oltre alle caratteristiche del servizio, potrà descrivere le eventuali esclusioni, il livello di servizio che il cliente può attendersi, la durata (per i servizi ricorrenti) e le informazioni di fatturazione e pagamento.

2.4 Pianificazione

Il lavoro di stage è stato pianificato per una durata complessiva di 304 ore, e organizzato settimanalmente come segue:

- **Prima Settimana (24 ore)**
  - Lettura della documentazione interna relativa ai collaboratori
  - Lettura della documentazione interna relativa all'applicazione della norma ISO/IEC 27001
  - Presa visione dell'infrastruttura esistente
- **Seconda Settimana - Studio obiettivi (40 ore)**
  - Incontro con persone coinvolte nel progetto per discutere i requisiti e le richieste relativamente alla soluzione da implementare
  - Individuazione delle tecnologie esistenti, commerciali ed open source
  - Studio delle normative vigenti
  - Stesura documento obiettivi del progetto
- **Terza Settimana - Analisi delle tecnologie (40 ore)**
  - Analisi degli strumenti di cancellazione sicura dei dati individuati
  - Test preliminari di cancellazione su supporti di prova
  - Valutazione delle tecnologie in termini di efficacia, conformità e costi
- **Quarta Settimana - Sviluppo della procedura (40 ore)**
  - Definizione delle fasi operative della procedura di cancellazione sicura
  - Scelta delle tecnologie che verranno utilizzate
  - Sviluppo della procedura
  - Integrazione delle *best practices* e delle normative ISO/IEC 27001
- **Quinta Settimana - Sviluppo procedura e Analisi (40 ore)**

  - Conclusione dello sviluppo della procedura
  - Esecuzione di test su supporti di memorizzazione reali
  - Raccolta dati e risultati dai test effettuati
  - Aggiornamento e perfezionamento della procedura in base ai risultati

- **Sesta Settimana - Collaudo finale e dimostrazione interna (40 ore)**
  - Verifica finale della procedura di cancellazione sicura
  - Presentazione e dimostrazione interna dei risultati e delle soluzioni proposte
  - Raccolta feedback e proposte di miglioramento, e eventuale implementazione

- **Settima Settimana - Stesura documentazione (40 ore)**
  - Redazione della documentazione completa della procedura di cancellazione sicura
  - Creazione della scheda di servizio per l'uso delle soluzioni selezionate
  - Sviluppo del *template* per il documento di certificazione della cancellazione

- **Ottava Settimana - Conclusione e obiettivi facoltativi (40 ore)**
  - Revisione finale e consegna della documentazione
  - Eventuali ottimizzazioni e ulteriori test facoltativi

Capitolo 3

Analisi di Normative, Standard e Best Practices, nell'ambito della Cancellazione Sicura

Al fine di poter definire dei criteri di selezione per la tecnologia che verrà impiegata nella procedura, è stata individuata la necessità di analizzare le normative, gli standard, e i documenti tecnici pubblicati in materia di cancellazione sicura dei dati.
In questo capitolo viene compiuta questa analisi, con una particolare attenzione alla necessità normativa della cancellazione sicura, alla classificazione delle tecniche e alla loro efficacia applicata ai supporti di memorizzazione di interesse.

3.1 La necessità della cancellazione dei dati

È possibile identificare la necessità della cancellazione dei dati all'interno di normative e regolamenti giuridici.
All'interno della norma ISO/IEC 27001:2022 [1], viene definito come le informazioni memorizzate nei sistemi informativi, debbano essere eliminate, quando

non sono più necessarie.[1] È quindi presente la necessità per le aziende di aver un processo adeguato di cancellazione dei dati, da applicare quando necessario.

La stessa necessità è presente anche da un punto di vista legale, in particolare all'interno del *Regolamento generale sulla protezione dei dati* [2]. L'Articolo 5(1)(e) stabilisce che i dati personali devono essere *"conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati"*. Una volta esaurite tali finalità, i dati devono essere cancellati o resi anonimi, salvo che siano richiesti per ulteriori trattamenti compatibili con le finalità originali.
Inoltre l'Articolo 32(1) richiede ai titolari e responsabili del trattamento di adottare *"misure tecniche e organizzative adeguate"* per garantire un livello di sicurezza adeguato al rischio.

All'interno di queste norme e regolamenti non viene però definito come effettuare la cancellazione, o che standard di sicurezza è necessario seguire. Per questo si farà riferimento ad altre pubblicazioni tecniche.

3.2 Classificazione delle tecniche di cancellazione

Una volta identificata la necessità per la cancellazione dei dati, è opportuno definire una classificazione delle tecniche di sicurezza. Per questo, si farà riferimento al documento *NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization* [3].
Questo documento rappresenta una linea guida In questo vengono definite tre categorie di cancellazione:

- ***Clear***: Applicazione di tecniche logiche di eliminazione per sanificare i

[1] ISO/IEC 27001:2022 1, *"Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization."*, Tabella A.1, sezione 8.3.

dati in tutte le aree di memoria accessibili all'utente, proteggendoli da tecniche semplici di recupero non invasivo.

- ***Purge***: Applicazione di tecniche fisiche o logiche, che rendono impossibile il recupero dei dati tramite l'utilizzo di tecniche allo stato dell'arte.
- ***Destroy***: Applicazione di tecniche fisiche o logiche, che rendono impossibile il recupero dei dati tramite l'utilizzo di tecniche allo stato dell'arte, e rendono inutilizzabile il dispositivo.

In particolare in un approfondimento all'interno della sezione 5 dello stesso documento, vediamo che viene definito come una tecnica di cancellazione rientra nella definizione di *Clear* se l'interfaccia utente non permette il recupero di tale informazione.[2]
Clear non interessa quindi l'eliminazione a basso livello, infatti anche il ripristino alle impostazioni di fabbrica, che tipicamente opera semplicemente cancellando i puntatori ai file, rappresenta una tecnica accettabile.
Per questo *Clear* non definisce un'operazione adeguata ai requisiti della procedura che si vuole definire, in quanto tramite strumenti software sarebbe possibile recuperare (in parte o totalmente) i dati cancellati.
Anche *Destroy* non sarà una tecnica appropriata, in quanto i dispositivi da cancellare sono destinati ad essere riutilizzati.
Purge invece presenta le caratteristiche opportune, in quanto rende "impossibile" il recupero dei dati e non rende inutilizzabile il dispositivo.

3.3 Supporti e relative tecniche di cancellazione proposte nel NIST SP 800-88

Esistono varie operazioni che rientrano nelle descrizioni delle tre classificazione discusse nella sezione precedente, e necessariamente diverse a seconda del supporto di memorizzazione di interesse, delle sue caratteristiche e del suo fun-

[2]NIST SP 800-88 3, *" [...] still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data".*

zionamento interno.

Abbiamo già identificato che, tra le tecniche definiste nel *NIST SP 800-88*, *Purge* è quella che corrisponde ai requisiti della procedura che si vuole definire. Di seguito vengono discusse le tecniche conformi alle sue caratteristiche, per le varie categorie di supporti di memorizzazione.

Ai fini della procedura, i supporti di interesse sono **dischi rigidi** (HDD_G) e **unità di memoria a stato solido** (SSD_G)

Dischi rigidi

Per i dischi rigidi (in particolare ATA HDD), vengono proposte quattro opzioni:

1. Il comando ***ATA Sanitize Device***:
   Questo è un comando definito nello standard ATA, che permette di eliminare i dati da un dispositivo in modo sicuro tramite firmware, utilizzando una delle tre opzioni: sovrascrittura, cancellazione a blocchi o eliminazione crittografica. Queste operazioni, più rapide rispetto alla riscrittura tradizionale, agiscono su tutte le aree dati, comprese quelle non più allocate o inaccessibili, e sulle cache. Il risultato varia in base al metodo scelto: la sovrascrittura applica un modello specificato dall'utente, la cancellazione a blocchi solitamente produce solo 0 o 1, mentre l'eliminazione crittografica mescola i dati con un metodo definito dal produttore.

2. Il comando ***ATA Secure Erase***:
   È un'operazione di sovrascrittura, definita nello standard ATA, basata su firmware, più veloce rispetto alla riscrittura tradizionale. Può essere eseguito in modalità *normal erase*, che sovrascrive i dati con 0 o 1 limitatamente a determinate aree, o *enhanced erase,* che sovrascrive tutti i dati utente, inclusi i settori riassegnati. Il risultato di *enhanced erase* varia in base al produttore e al modello.

3. La **Eliminazione Crittografica o *Cryptographic Erase***:
   È un metodo di sanitizzazione che elimina la chiave di crittografia del

supporto (MEK) o la chiave di crittografia della chiave (KEK), rendendo impossibile recuperare i dati decifrati.

4. La **Demagnetizzazione o *Degaussing***: questa tecnica consiste nel ridurre a zero il flusso magnetico applicando un campo magnetico inverso. Questo processo rende inutilizzabili i dischi rigidi moderni, come IDE, EIDE, ATA e SCSI, poiché cancella anche le informazioni di localizzazione delle tracce memorizzate sul disco.

Unità di memoria a stato solido (SSD)

Le le unità di memoria a stato solido, considereremo ATA SSD (SATA, eSATA, ecc...) e NVM Express (NVMe) SSD.
Per le prime (ATA SSD) vengono presentate due opzioni:

1. Il comando ***ATA Secure Erase***, già descritto.

2. La **Eliminazione Crittografica o *Cryptographic Erase*** anch'essa già descritta.

Per i dispositivi NVMe invece le operazioni presentate sono:

1. Il comando ***NVM Express Format***:
   Offre due opzioni: *User Data Erase*, per cancellare i dati utente, e *Cryptographic Erase*, se il dispositivo supporta la crittografia. Dopo l'applicazione di *Cryptographic Erase*, è possibile utilizzare *User Data Erase* per completare l'eliminazione dei dati o, in assenza di supporto per questo comando, applicare una procedura di *Clear*.

2. La **Eliminazione Crittografica o *Cryptographic Erase***

3.4 L'efficacia degli algoritmi di sovrascrittura

3.4.1 Sovrascrittura dei dispositivi magnetici (HDD)

Nel *NIST SP 800-88 Rev.1* viene esposto come, nel caso di dischi magnetici, un singolo passaggio di sovrascrittura rende impossibile il recupero dei dati,

anche tramite l'utilizzo di tecniche di laboratorio allo stato dell'arte.[3]
Possiamo quindi affermare che per il contesto di questo progetto, anche l' *"overwriting"* con un solo passaggio, è sufficientemente sicuro nel caso di dischi magnetici.
L'uso di tali comandi porta a un compromesso: è necessario assicurarsi che tali comandi siano implementati correttamente dal produttore.[4]
Sarà quindi opportuno verificare l'implementazione (o comunque il corretto funzionamento) di tali metodi, nel caso vengano impiegati nella procedura prodotti che li utilizzano.

3.4.2 Sovrascrittura dei dispositivi a stato solido (SSD)

La stessa cosa non vale per gli SSD, a causa del loro funzionamento interno. Nell'articolo *"Advances in SSD Erasure Solutions: A Risk Based Approach"* [4], parlando del metodo di sovrascrittura viene descritto come questo non sia efficace su questo tpo di supporti, a causa del funzionamento del *firmware*.[5]
Possiamo attribuire questo a quattro principali cause:

- Gli **algoritmi di *wear-leveling***:
  Gli SSD utilizzano algoritmi di *wear-leveling* per distribuire i dati su diverse posizioni fisiche, prolungando la vita della memoria flash. Questo significa che la sovrascrittura dei dati logici non corrisponde necessariamente alla sovrascrittura dello stesso spazio fisico che conteneva i dati originali.

- Il **Flash Translation Layer (FTL)**:
  Il livello di traduzione flash mappa gli indirizzi logici (LBA_G) a posizioni

[3] NIST SP 800-88, sezione 2.4: Trends in Sanitization 3, *"For storage devices containing magnetic media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data."*

[4] NIST SP 800-88 3, *"The use of such commands results in a tradeoff because although they should more thoroughly address all areas of the media, using these commands also requires trust and assurance from the vendor that the commands have been implemented as expected."*

[5] Advances in SSD Erasure Solutions: A Risk Based Approach 4, *"However, this method will not effectively clear all digital locations in the SSD that reside beneath the firmware or flash transition layer. But, due to the characteristics of the SSD firmware, a multiple overwrite solution will populate this blank data to the digital spaces below the firmware level at the discretion of the SSD firmware code."*

fisiche. Quando si sovrascrivono i dati, l'SSD potrebbe scriverli in una nuova posizione, mantenendo i vecchi dati come "remanenze digitali" fino a quando non vengono fisicamente cancellati.

- L'**impossibilità di sovrascrittura diretta**:
  A differenza degli hard disk tradizionali, gli SSD non supportano la sovrascrittura diretta per la natura della memoria *flash*. La sovrascrittura garantisce solo una sanitizzazione logica, non una sanitizzazione fisica.

- La **copertura incompleta**:
  Anche con molteplici passaggi di sovrascrittura, i dati possono persistere in parti dell'SSD a causa della gestione a livello di firmware o di aree fuori dal controllo dell'utente.

Per questi dispositivi è quindi opportuno utilizzare funzionalità che operano a livello *firmware*, come *Secure Erase*.

Capitolo 4

Analisi delle Tecnologie

In questo capitolo, vengono esposti i criteri di selezione e le modalità di test, utilizzati per l'analisi delle tecnologie prese in esame, e per la selezione di una di queste ai fini del suo utilizzo nella procedura.

4.1 Criteri di selezione

Sulla base dei requisiti tecnici evidenziati nello scorso capitolo, e di quelli richiesti dal proponente, sono stati identificati i seguenti criteri di selezione:

4.1.1 Compatibilità del sistema operativo

Al fine di poter sviluppare un'unica procedura è fortemente preferita la scelta di un prodotto che presenti una versione Linux. In questo modo sarà possibile creare un supporto avviabile, dalla quale si possa effettuare la cancellazione di un'intera macchina.
È considerato a sua volta più desiderabile, la presenza di una versione apposita per creare un supporto avviabile, in quanto facilita il processo di creazione del supporto, sia inizialmente che ogni qual volta sia necessario aggiornare ad una nuova versione.

4.1.2 Supporto hardware

Come da requisito definito dal proponente, è necessario che il prodotto software che verrà selezionato fornisca funzionalità adeguate alla cancellazione sicura dei seguenti dispositivi di memorizzazione:

- Unità disco rigido ATA
- Unità SSD ATA
- Unità SSD NVM Express (NVMe)

4.1.3 Usabilità e funzionalità aggiuntive

Verranno considerate anche soluzioni che non forniscono un'interfaccia grafica, e che possono richiedere delle competenze tecniche (programmi a riga di comando). Questo è possibile perché la procedura verrà effettuata da personale tecnico.
È comunque considerata positivamente la presenza di un'interfaccia che renda più intuitivo e rapido l'utilizzo del prodotto.
Un ulteriore aspetto desiderabile è la presenza di una funzionalità di generazione di un certificato di cancellazione.

4.1.4 Costi e licenze

A parità di funzionalità offerte e soddisfacimento dei requisiti, sono preferiti programmi gratuiti.
Allo stesso modo vengono preferiti prodotti *open source*.

4.2 Metodologia di test

La metodologia di test è stata progettata basandosi su quella utilizzata in *An Evaluation Of Data Erasing Tools* [5].
Di seguito vengono esposti gli strumenti utilizzati ed il processo di *testing* seguito.

4.2.1 Tecnologie utilizzate per il processo di test

- ***USB Write Blocker*** è stato impiegato per impedire scritture del disco non volute nella fase di creazione e analisi dell'immagine del disco.
- ***WinHex Hex Editor*** è stato utilizzato per l'analisi e la visualizzazione dell'immagine del disco.
- ***Autopsy*** è stato utilizzato per analizzare l'immagine del disco, ed individuare eventuali frammenti di informazioni residui.
- ***OSForensics*** è stato utilizzato per creare l'immagine del disco.

Figura 4.1: Logo di USB Write Blocker, WinHex Hex Editor, Autopsy e OSForensics

4.2.2 Processo sperimentale

1. Il disco viene popolato con dei dati
2. Viene eseguito il processo di cancellazione
3. Il disco viene scollegato
4. Il disco viene ricollegato, utilizzando *USB Write Blocker* per impedire qualsiasi scrittura
5. Viene creata un immagine del disco cancellato con *OSForensics*
6. L'immagine viene importata e analizzata con *WinHex Editor* e *Autopsy*

4.3 Prodotti software presi in analisi

Di seguito vengono presentate le tecnologie prese in analisi.

4.3.1 Remo Drive Wipe

Descrizione e sistemi operativi supportati

Remo Drive Wipe[6], è uno strumento di *drive wiping* per Windows. Offre nove algoritmi per la sovrascrittura dei dischi nella versione completa, e due nella versione gratuita.

Supporto Hardware

In quanto il prodotto presenta solo funzionalità di sovrascrittura, presenta un supporto adeguato per dispositivi a disco rigido, ma non supporta funzionalità appropriate alla cancellazione di supporti SSD.

Usabilità e funzionalità aggiuntive

L'interfaccia si presenta chiara e intuitiva, non è presente una funzionalità di generazione di un certificato di cancellazione.

Costi e licenze

Esistono varie licenze, tra le quali una gratuita che è l'oggetto di questa analisi.

Risultati dei test e considerazioni

Remo Drive Wipe è risultato efficace su unità disco rigido, infatti nessun residuo di dati è stato identificato. La mancata presenza di funzionalità per dischi a stato solido e di una versione Linux lo rendono inadatto all'impiego nella procedura.

4.3.2 Active KillDisk

Descrizione e sistemi operativi supportati

Active KillDisk[7] è un'applicazione per la rimozione dei dati e presenta versioni per sistemi Windows, Mac e Linux. È anche disponibile una versione per creare supporti avviabili.
Nella versione gratuita è inclusa l'applicazione per Windows e quella per creare un supporto avviabile.

Supporto Hardware

Active KillDisk offre sia funzionalità di sovrascrittura, che funzionalità per dischi a stato solido (come ATA Secure Erase).

Usabilità e funzionalità aggiuntive

È presente un'interfaccia grafica funzionale ed intuitiva. Non viene offerta la possibilità di generare un certificato di avvenuta cancellazione.

Costi e licenze

Esistono varie versioni, quella gratuita è quella presa in analisi.

Risultati dei test e considerazioni

Nell'analisi con *WinHex Editor* è stato evidenziato come nel processo di sovrascrittura, *Active KillDisk* non elimini il settore di boot dei dischi.

4.3.3 ShredOS (nwipe)

Descrizione e sistemi operativi supportati

ShredOs[8] è una distribuzione linux avviabile da USB, finalizzata alla funzionalità di eliminare l'intero contenuto di un disco, utilizzando ***nwipe***[9].
Può operare sia a riga di comando, che con una GUI. Essendo una distribuzione

Linux portatile, un supporto contenente *ShredOS* può essere avviato su qualsiasi macchina ed opera indipendentemente dal sistema operativo installato.

Supporto Hardware

Nwipe offre funzionalità di cancellazione per supporti a disco rigido, e gli altri programmi inclusi (*hdparm* e *nvme-cli*) offrono supporto per dispositivi a stato solido.

Usabilità e funzionalità aggiuntive

Nwipe offre una GUI intuitiva e facilmete utilizzabile, mentre per la cancellazione di SSD, è necessario utilizzare programmi a riga di comando.
È presente anche una funzionalità per la generazione di un certificato di cancellazione, che può essere configurato con i dati dell'operatore e dell'organizzazione che effettua la rimozione dei dati.

Costi e licenze

È distribuito con licenza *GNU General Public Licence Version 2* [10].

Risultati dei test e considerazioni

La procedura di verifica non ha identificato nessun residuo di informazioni.

4.3.4 PartedMagic

Descrizione e sistemi operativi supportati

Parted Magic[11] è un software basato su Linux progettato per la gestione delle partizioni, il recupero dati e la clonazione di dischi. Offre funzionalità per la cancellazione sicura e il ripristino di sistemi operativi.
Parted Magic offre una versione per la creazione di un supporto avviabile. È quindi utilizzabile indipendentemente dal sistema operativo della macchina.

Supporto Hardware

Offre funzionalità che rispettano i requisiti sia per HDD che SSD. Per dischi rigidi utilizza algoritmi si sovrascrittura, mentre per i supporti a stato solido utilizza ATA secure erase e NVMe secure erase.

Usabilità e funzionalità aggiuntive

Non è stato possibile verificare l'usabilità del prodotto a causa della mancanza di una versione di prova o gratuita.

Costi e licenze

Offre solo versioni a pagamento.

Risultati dei test e considerazioni

In quanto non è disponibile una versione di prova, non è stato possibile verificare le funzionalità di *Parted Magic*.

4.3.5 BleachBit

Descrizione e sistemi operativi supportati

BleachBit[12] è un software open source per Linux e Windows progettato per liberare spazio su disco e proteggere la privacy. Offre funzionalità come la pulizia di cache, cookie, cronologia Internet, file temporanei, log e altri dati da migliaia di applicazioni, tra cui Firefox, Google Chrome, Adobe Flash e Opera. Oltre all'eliminazione dei file, include strumenti per la sovrascrittura sicura dei dati e la pulizia dello spazio libero
Sebbene offra funzionalità di rimozione sicura dei file, è principalmente progettato per la gestione della memoria, e la pulizia dello spazio libero.

Supporto Hardware

BleachBit non presenta funzionalità adeguate alla cancellazione di dati su SSD.

Usabilità e funzionalità aggiuntive

Non essendo principalmente progettato per la cancellazione completa dei dischi, BleachBit risulta più complicato da utilizzare per questa funzione rispetto ad altri *software*.

Costi e licenze

BleachBit è gratuito e distribuito con licenza *GNU General Public Licence Version 3* [13].

Risultati dei test e considerazioni

La mancata presenza di metodi adeguati ai dischi SSD, e la natura non ottimizzata dell'interfaccia e delle procedure disponibili per la cancellazione sicura, rendono il processo poco intuitivo e più complicato.

4.4 Tabella comparativa

La tabella 4.1 riassume le principali caratteristiche emerse dall'analisi dei vari prodotti.

Prodotto	**Sistema Operativo**	**Supporto Hardware**	**Costi e licenze**	**Risultati**
Remo Drive Wipe	Windows	HDD	Gratuito	Soddisfacenti per HDD
Active KillDisk	Supporto avviabile	HDD e SSD	Gratuito	Non elimina il settore di boot
ShredOS	Supporto avviabile	HDD e SSD	Gratuito e *Open Source*	Soddisfacenti
Parted Magic	Supporto avviabile	HDD e SSD	Solo a pagamento	Non testato
BleachBit	Linux, Windows	HDD	Gratuito e *Open Source*	Soddisfacenti per HDD

Tabella 4.1: Tabella comparativa delle tecnologie analizzate

4.5 Conclusioni e scelta

La scelta della tecnologia per il suo utilizzo nella procedura, è ricaduta su ***ShredOS***. Questo perché oltre a rispettare tutti i requisiti, presenta anche la funzionalità di creazione di un certificato di avvenuta eliminazione.

Capitolo 5

Descrizione della Procedura

In questo capitolo viene descritta la procedura di cancellazione sicura, progettata sulla base delle caratteristiche emerse dall'analisi del terzo capitolo e utilizzando la tecnologia selezionata nel quarto capitolo.
Dopo una presentazione delle tecnologie utilizzate, viene illustrato il processo di creazione e configurazione del supporto avviabile contenente ShredOS. Successivamente vengono elencati i passi da seguire per la cancellazione sicura dei vari supporti di interesse.

5.1 Tecnologie utilizzate

Come esposto nel capitolo precedente, la tecnologia scelta per effettuare la procedura di cancellazione sicura è ***ShredOS***. Di seguito vengono descritti ShredOS e i programmi contenuti al suo interno.

5.1.1 ShredOS

ShredOS è una distribuzione Linux leggera e avviabile tramite USB o CD/DVD, progettata per la cancellazione sicura dei dischi utilizzando nwipe. Quest'ultimo è un *fork*$_G$ del comando dwipe di *DBAN*$_G$, creato per superare i limiti di DBAN, non più aggiornato dal 2015, offrendo compatibilità con hardware moderno e miglioramenti continui.
ShredOS opera indipendentemente dal sistema operativo presente sul dispositi-

vo, eliminando completamente dati, directory e sistemi operativi dai dischi selezionati. Supporta sia architetture a 32 che a 64 bit, con file immagine dedicate (.img per USB e .iso per CD/DVD)[8].

5.1.2 Nwipe

Nwipe è uno strumento open source concepito per la cancellazione sicura di dati dai dischi rigidi, come già detto, è nato come fork di dwipe. La sua indipendenza dal progetto DBAN, non più mantenuto dal 2015, consente a Nwipe di offrire un supporto più aggiornato per l'hardware moderno e una maggiore compatibilità con varie distribuzioni Linux.
Il programma permette di eliminare i dati utilizzando algoritmi di sovrascrittura, offrendo sia soluzioni rapide a singolo passaggio sia procedure più approfondite.
L'interfaccia di Nwipe è disponibile sia in modalità testuale che tramite un'interfaccia grafica *ncurses*.
Un'altra caratteristica rilevante di Nwipe è la capacità di gestire la cancellazione di più dischi simultaneamente, sfruttando un'architettura software *multi-thread*[9].

5.1.3 Hdparm

Hdparm è un programma da linea di comando per Linux utilizzato per impostare e visualizzare i parametri hardware dei dischi ATA e per testare le loro prestazioni. Consente di configurare una varietà di impostazioni, come la gestione della cache dei dischi, la modalità di sospensione, la gestione dell'energia, la gestione acustica e le impostazioni *DMA*$_G$.
Di particolare importanza per questo contesto è l'utilità di accesso al comando *secure erase* del *firmware* ATA.

5.1.4 Nvme-cli

Il programma nvme-cli è un'*utility open-source* per la gestione e il controllo dei dispositivi NVMe attraverso la linea di comando. Progettato per amministratori di sistema e utenti avanzati, consente di eseguire una vasta gamma di

operazioni, tra cui il monitoraggio delle prestazioni, la configurazione avanzata, e funzioni di diagnostica sui dispositivi NVMe. Fornisce accesso diretto ai comandi NVMe definiti dallo standard, consentendo operazioni come la lettura e scrittura di *namespace*, gestione delle informazioni sul dispositivo, e aggiornamenti del firmware[14].
Allo stesso modo di hdparm, viene utilizzato in questo contesto per l'accesso ai comandi di cancellazione sicura definiti nel *firmware* dei dispositivi NVMe.

5.2 Preparazione della live USB

Il primo passaggio della procedura è preparare il supporto avviabile (chiamato anche *"live USB"* o *"dispositivo di boot"*).
Questo passaggio oltre ad essere eseguito alla prima creazione della *live USB*, andrà ripetuto quando sarà necessario effettuare l'aggiornamento di ShredOS.

5.2.1 Download e configurazione

In primo luogo è necessario scaricare l'ultima versione dell'immagine di SHredOS dalla pagina *GitHub* https://github.com/PartialVolume/shredos.x86_64.
In seguito, si vuole sfruttare il programma ***loadkeys*** presente in ShredOS, al fine di avviare il sistema con *layout* di tastiera italiano. Per fare questo, viene modificato il file `grub.cfg` situato in `/boot/grub`, come segue:

```
set default="0"
set timeout="0"

menuentry "shredos" {
        linux /boot/shredos console=tty3 loglevel=3
}
```

Codice 5.1: File grub.cfg originale

```
set default="0"
set timeout="0"

menuentry "shredos" {
        linux /boot/shredos console=tty3 loglevel=3 loadkeys=it
}
```

Codice 5.2: File grub.cfg modificato

5.2.2 Montaggio dell'immagine sul supporto

Il passaggio successivo è quello di montare l'immagine su un dispositivo *USB*$_G$.
Per *"montare"* (o *"mount"* in inglese) si intende il processo attraverso il quale si rende accessibile un *file system*, un *file*, una *directory*, un dispositivo o un file speciale, associandolo a una specifica posizione nel sistema operativo, detta punto di montaggio (*"mount point"*)[15].

Per fare questo si è deciso di utilizzare *Rufus*.
Rufus è un software gratuito e *open-source* progettato per creare unità USB avviabili. È particolarmente utile per installare sistemi operativi (come Windows o Linux), lavorare su sistemi senza un sistema operativo installato, aggiornare BIOS o firmware, o eseguire operazioni di formattazione a basso livello. Non richiede installazione e supporta una vasta gamma di formati ISO. Rufus è compatibile con le versioni di Windows a partire dalla 8. È sviluppato in modo trasparente e distribuito sotto licenza GPLv3[13].[1]

Per ottenere un supporto avviabile, è sufficiente selezionare il file, il dispositivo USB, mantenere tutte le impostazioni di default e premere il bottone *avvia*, come mostrato nell'immagine.

[1] 16, Dal sito ufficiale di Rufus.

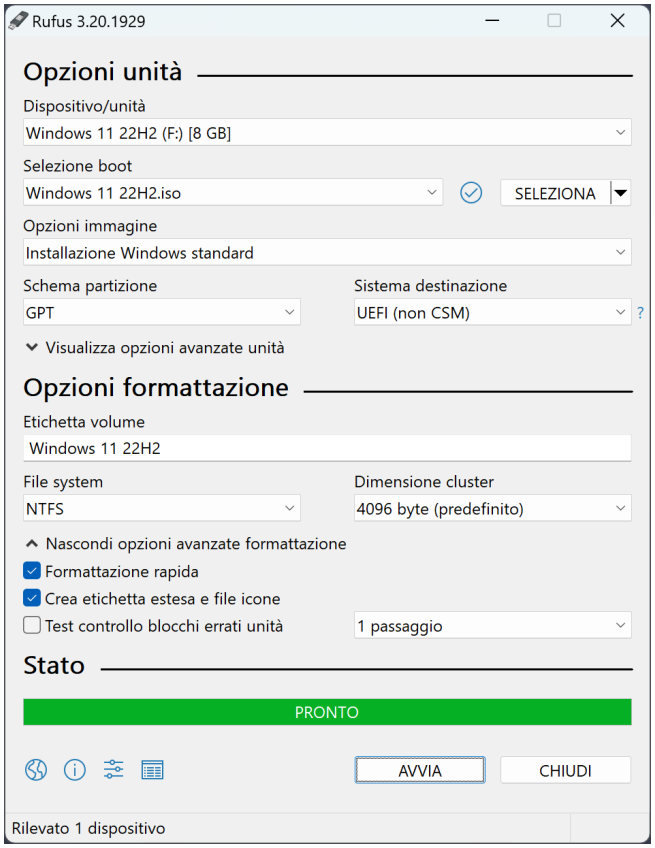

Figura 5.1: Schermata di creazione del supporto avviabile con Rufus

5.3 Procedura di cancellazione

Di seguito viene presentato il processo di cancellazione dei dispositivi di memorizzazione.

Viene innanzitutto inserita la *live USB* nel computer contenente i dischi da cancellare. A questo punto viene fatto il boot dalla USB e all'avvio del sistema operativo verrà eseguito automaticamente nwipe.

Nei passaggi successivi la procedura differisce a seconda della tipologia di supporto di memorizzazione.

5.3.1 Cancellazione dei dischi rigidi

Per la cancellazione dei dischi rigidi viene utilizzato esclusivamente nwipe. Come è stato discusso nei capitoli precedenti, è sufficientemente sicuro utilizzare un algoritmo di sovrascrittura a un solo passaggio. Il metodo viene quindi cambiato a *"Zero Fill"*. Sarà sufficiente premere "M", accedendo in questo

modo al menù dei metodi, e scegliere il metodo voluto dalla lista.
Tornarti alla schermata principale di nwipe, è possibile selezionare i dischi da cancellare, e successivamente avviare la cancellazione premendo spazio.

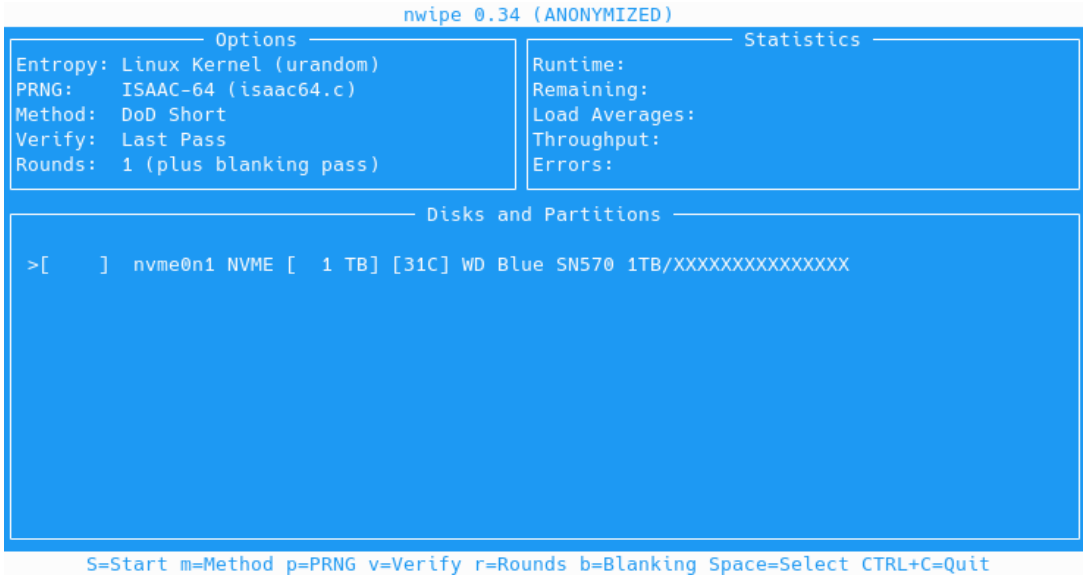

Figura 5.2: Schermata iniziale di nwipe

5.3.2 Cancellazione dei dischi a stato solido

Come discusso in precedenza, per gli SSD verranno usati ***hdparm*** e *NVMe - CLI*, rispettivamente per i dispositivi ATA e NVMe.
Prima di poter eseguire i comandi opportuni, è necessario uscire da nwipe premendo `Ctrl + C` e accedere ad un terminale premendo `Ctrl + Alt + F2`.

5.3.2.1 Dischi SSD ATA

La cancellazione di un disco SSD ATA tramite hdparm può essere eseguita seguendo i passi qui riportati:

- Elencare i dischi presenti nel sistema con il comando `fdisk -l`.
- Identificare il disco da cancellare (ad esempio, supponiamo che il disco sia `/dev/sda`).
- Verificare lo stato del disco con il comando `hdparm -I /dev/sda`. Controllare che lo stato non sia indicato come *frozen*.

- **Se lo stato è *frozen***:
  - Eseguire il comando `echo -n mem > /sys/power/state` per mettere il sistema in modalità sospensione.
  - Riattivare il sistema e ripetere il controllo con `hdparm -I /dev/sda` fino a quando lo stato non risulta sbloccato.
- Impostare una password temporanea per abilitare la modalità di sicurezza sul disco con il comando `hdparm -user-master u -security-set-pass p /dev/sda`.
- Verificare che il livello di sicurezza del disco sia stato impostato su *high* utilizzando `hdparm -I /dev/sda`.
- Avviare la procedura di cancellazione sicura utilizzando la modalità avanzata (se supportata) con il comando `hdparm -user-master u -security-erase-enhanced p /dev/sda`. **Nota**: Se la modalità *enhanced* non è disponibile, utilizzare il comando alternativo `hdparm -security-erase p /dev/sda`.
- Attendere il tempo necessario per il completamento della procedura.
- Verificare che la password sia stata rimossa e che la sicurezza sia tornata allo stato predefinito con `hdparm -I /dev/sda`.
- Effettuare un controllo a campione per verificare che i dati siano stati cancellati con il comando `dd if=/dev/sda bs=1M count=5`.

5.3.2.2 Dischi SSD NVMe

La cancellazione di un disco SSD NVMe tramite nvme-cli può essere eseguita seguendo i passi qui riportati:

- Identificare l'unità NVMe da cancellare con il comando `nvme list`, che elenca tutte le unità NVMe collegate al sistema.

- Verificare il supporto per la cancellazione sicura con il comando `nvme id-ctrl /dev/nvmeXn1`, sostituendo `nvmeXn1` con l'identificatore corretto dell'unità. Controllare i campi relativi ai comandi di cancellazione.
- Eseguire una cancellazione sicura standard con il comando `nvme format /dev/nvmeXn1 -ses=1`, dove `-ses=1` specifica la cancellazione sicura.
- Attendere il completamento della procedura.
- Verificare il successo dell'operazione controllando lo stato del disco con il comando `nvme list`. Assicurarsi che l'unità sia pronta per un nuovo utilizzo.

5.4 Certificato di cancellazione

Per la generazione del certificato di cancellazione viene sfruttata la funzionalità di nwipe.
Nwipe compie automaticamente una verifica dell'avvenuta cancellazione, e genera un certificato in formato PDF, al termine della cancellazione di un dispositivo.
Per salvare il certificato sarà sufficiente uscire da nwipe, collegare un dispositivo USB e premere il tasto spazio per salvarlo.
Nel caso dei dispositivi SSD, per i quali la cancellazione non è stata effettuata con nwipe, è possibile effettuare con nwipe un passaggio di verifica, che genererà il certificato.

Capitolo 6

Verifica della procedura

Nel presente capitolo viene presentato in dettaglio il processo sperimentale atto a verificare l'efficacia e la congruenza ai requisiti della procedura.

6.1 Processo sperimentale

Il processo sperimentale per la verifica della procedura è lo stesso descritto nella sezione 4.2. Di seguito vengono presentate nel dettaglio le fasi che lo compongono.

6.1.1 Selezione dei dispositivi e loro preparazione

Per la procedura di test sono stati selezionate due tipologie di supporti di memoria: un disco rigido ed un disco a stato solido. Questo permette di verificare tutti gli aspetti della procedura.
L'intero processo sperimentale è stato eseguito prima su dischi contenenti varie tipologie di file, e successivamente sugli stessi dischi, sui quali era stata installata una copia di *Windows 10*.

6.1.2 Esecuzione della procedura

La procedura è stata eseguita seguendo le istruzioni illustrate nel capitolo 5. Per i due dischi selezionati, sono stati seguiti rispettivamente i passaggi per

i dischi rigidi (HDD) e per i dischi a stato solido (SSD), in particolare ATA-SSD.

6.1.3 Creazione dell'immagine del disco

Una volta eseguita la procedura, i dischi sono stati scollegati. Successivamente è stato attivato il blocco della scrittura di *USB Write Blocker*, in modo da prevenire scritture involontarie da parte del sistema operativo.
I dischi sono stati ricollegati, ed è stata creata e memorizzata una loro immagine tramite *OSForensics*.

6.1.4 Verifica con WinHex

L'immagine dei dischi è stata importata ed analizzata con *WinHex Hex Editor*. Si sono esaminati tutti i settori del disco, in formato esadecimale, verificando che nessun dato residuo persistesse. È possibile evidenziare l'eventuale residuo di dati tramite questo processo in quanto per la cancellazione è stato utilizzato un algoritmo che sovrascrive con valore *"0"*. In questo modo è facile identificare valori che non sono zero, e che quindi rappresentano frammenti di dati non cancellati.

6.1.5 Verifica con Autopsy

Successivamente le immagini dei dischi sono state analizzate con *Autopsy*. *Autopsy* è un software di *digital forensics* che consente di esaminare immagini di dischi rigidi e dispositivi di memoria per analizzare e recuperare dati. In particolare le funzionalità utilizzate che permettono di verificare eventuali residui di informazioni sono:

- **Analisi del filesystem**:
  Viene eseguita un'analisi del *filesystem* per identificare eventuali file e cartelle presenti. Nel caso di un disco cancellato, il programma può rilevare i settori che non sono più collegati a nessuna voce di *directory*, ma che

potrebbero contenere ancora dati recuperabili (ad esempio, dati che non sono stati sovrascritti).

- **Recupero di file cancellati**:
  Questa funzionalità permette di cercare e recuperare file che sono stati cancellati ma non sovrascritti. Questi file possono essere identificati grazie alla loro "testa" e "coda" (*header* e *footer*) all'interno dei settori del disco. L'analisi dei settori liberi può rivelare file parzialmente recuperabili.

- **Ricerca di residui nei settori non allocati**:
  Il *software* esplora anche i settori non allocati e i settori liberi del disco per cercare dati residui che potrebbero non essere visibili nel *filesystem*, ma che sono ancora fisicamente presenti sul disco.

6.2 Risultati dei test

In tutti i test eseguiti, non è stato individuato nessun residuo di dato.
In particolare dall'analisi con *WinHex* è stato evidenziato come tutti i settori del disco fossero stati sovrascritti, e *Autopsy* non ha rilevato nessun residuo di informazione.
Questo risultato garantisce che la procedura sviluppata soddisfa i requisiti di sicurezza desiderati.

Capitolo 7

Conclusioni

7.1 Consuntivo finale

La tabella 7.1 rappresenta il consuntivo finale del lavoro di stage.

Ore totali	**Settimana**	**Descrizione**
24	1	• Studio della documentazione interna
40	2	• studio di norme e best practice dell'ambito • definizione degli obiettivi e dei requisiti del progetto
60	3, 4	• Individuazione delle tecnologie • Studio delle tecnologie • Test preliminari

80	4, 5, 6	• Definizione delle fasi della procedura • Scelta delle tecnologie • Sviluppo della procedura
60	6, 7	• Esecuzione dei test • Raccolta dei dati
40	8	• Presentazione della procedura • Stesura della documentazione
Totale ore:		**304**

Tabella 7.1: Consuntivo finale

7.2 Raggiungimento degli obiettivi

Al termine del progetto di stage sono stati raggiunti tutti gli obiettivi obbligatori.
Nel complesso il tempo pianificato è risultato sufficiente. È stato impiegato più tempo del previsto per lo studio delle normative e dei vari documenti analizzati, e lo stesso anche per lo studio delle tecnologie.
Invece è stato impiegato meno tempo di quello pianificato per lo sviluppo della procedura.

7.3 Conoscenze acquisite e valutazione personale

Durante il periodo di stage ho avuto modo di studiare e approfondire l'ambito della cancellazione sicura e degli argomenti che lo circondano.
In particolare lo studio delle normative, dei documenti tecnici e delle tecniche di cancellazione sicura, si è rivelato interessante e arricchente.
Inoltre poter lavorare all'interno di un contesto aziendale, mi ha permesso di sviluppare e affinare varie *soft-skills*, come la gestione e la programmazione delle attività.
In complesso valuto positivamente il progetto di stage, sia in termini di obiettivi raggiunti che di conoscenze e competenze acquisite.

Glossario

DMA (Direct Memory Access) tecnologia che consente a dispositivi hardware di accedere direttamente alla memoria del sistema, bypassando il coinvolgimento diretto della CPU. Questo meccanismo ottimizza il trasferimento di dati, riducendo il carico sul processore e migliorando l'efficienza in operazioni come I/O ad alta velocità. 24

Fork processo che crea una copia di un repository o di un progetto software, permettendo lo sviluppo indipendente rispetto all'originale. In ambienti collaborativi, come i sistemi di controllo versione distribuiti (ad esempio Git), il fork consente di modificare, testare o ampliare il codice senza influenzare direttamente il progetto originale. 23

HDD (Hard Disk Drive) sono dispositivi di archiviazione dati che utilizzano piatti magnetici rotanti e testine mobili per leggere e scrivere informazioni. Basati su tecnologia magnetica, offrono capacità elevate e sono utilizzati in una vasta gamma di applicazioni, dai computer personali ai sistemi di archiviazione su larga scala. 10

ICT (Information and Communication Technology) comprende l'insieme delle tecnologie e infrastrutture utilizzate per la gestione, il trattamento, la trasmissione e la condivisione delle informazioni, combinando informatica, telecomunicazioni e sistemi digitali per supportare processi comunicativi e operativi in diversi contesti. 1

DBAN (Darik's Boot and Nuke) software open-source progettato per la cancellazione sicura dei dati su unità di archiviazione. Avviato da supporti

esterni come CD, DVD o USB, utilizza algoritmi di sovrascrittura per eliminare irreversibilmente i dati, garantendo la conformità a standard di sicurezza per la protezione delle informazioni sensibili. 23

LBA (Logical Block Addressing) metodo per identificare e accedere ai blocchi di dati su dispositivi di archiviazione, utilizzando indirizzi logici sequenziali anziché una mappatura fisica di cilindri, testine e settori. Introdotto per superare le limitazioni dei vecchi schemi CHS, LBA è ampiamente adottato in dischi rigidi, SSD e altri dispositivi moderni. 12

SSD (Solid State Drive) sono dispositivi di archiviazione dati basati su memoria flash o DRAM, privi di parti mobili, che utilizzano celle di memoria per immagazzinare informazioni in modo elettronico, garantendo tempi di accesso rapidi, bassa latenza e maggiore affidabilità meccanica rispetto ai dispositivi tradizionali basati su tecnologia magnetica. 10

USB (Universal Serial Bus) sono un'interfaccia standard per la connessione, il trasferimento di dati e l'alimentazione tra dispositivi elettronici. Basate su un protocollo seriale, supportano diverse versioni con velocità crescenti (da USB 1.0 a USB4) e connettori standardizzati, garantendo interoperabilità tra una vasta gamma di dispositivi. 26

Bibliografia

Standard, Linee Guida Tecniche, Regolamenti

[1] *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. standard. Geneva, CH: International Organization for Standardization, 2022 (cit. alle pp. 3, 7, 8).

[2] *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati*. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679. Regolamento Generale sulla Protezione dei Dati (GDPR). 2016 (cit. a p. 8).

[3] Richard Kissel, Andrew Regenscheid, Matthew Scholl e Kevin Stine. *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*. Rapp. tecn. SP 800-88 Rev. 1. Gaithersburg, MD: National Institute of Standards e Technology, 2014. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf (cit. alle pp. 8, 9, 12).

Articoli

[4] David Dykes Joe Mount Daniel Dyer. «Advances in SSD Erasure Solutions: A Risk Based Approach». In: *Lifespan Technology* (2022) (cit. a p. 12).

[5] Isaac Afrifa Andrew Jones. «An Evaluation Of Data Erasing Tools». In: *Journal of Digital Forensics, Security and Law* 15.1 (2020). URL: https://commons.erau.edu/cgi/viewcontent.cgi?article=1615&context=jdfsl (cit. a p. 15).

Sitografia

[6] *Sito ufficiale di Remo Drive Wipe*. URL: https://www.remosoftware.com/remo-drive-wipe (visitato il giorno 24/11/2024) (cit. a p. 17).

[7] *Sito ufficiale di Active Kill Disk*. URL: https://www.killdisk.com/eraser.html (visitato il giorno 24/11/2024) (cit. a p. 18).

[8] *Repository e sito ufficiale di ShredOS*. URL: https://github.com/PartialVolume/shredos.x86_64 (visitato il giorno 29/11/2024) (cit. alle pp. 18, 24).

[9] *Repository e sito ufficiale di Nwipe*. URL: https://github.com/martijnvanbrummelen/nwipe (visitato il giorno 29/11/2024) (cit. alle pp. 18, 24).

[10] *GNU General Public License, version 2*. URL: https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html (visitato il giorno 23/11/2024) (cit. a p. 19).

[11] *Sito ufficiale di Parted Magic*. URL: https://partedmagic.com/ (visitato il giorno 24/11/2024) (cit. a p. 19).

[12] *Sito ufficiale di BleachBit*. URL: https://www.bleachbit.org/ (visitato il giorno 24/11/2024) (cit. a p. 20).

[13] *GNU General Public License, version 3*. URL: GNU%20General%20Public%20License,%20version%202 (visitato il giorno 23/11/2024) (cit. alle pp. 21, 26).

[14] *Sito ufficiale di NVMe - CLI*. URL: https://nvmexpress.org/open-source-nvme-management-utility-nvme-command-line-interface-nvme-cli/ (visitato il giorno 29/11/2024) (cit. a p. 25).

[15] *Mounting - IBM Documentation*. URL: https://www.ibm.com/docs/en/aix/7.2?topic=systems-mounting (visitato il giorno 29/11/2024) (cit. a p. 26).

[16] *Sito ufficiale di Rufus*. URL: https://rufus.ie/en/ (visitato il giorno 28/11/2024) (cit. a p. 26).