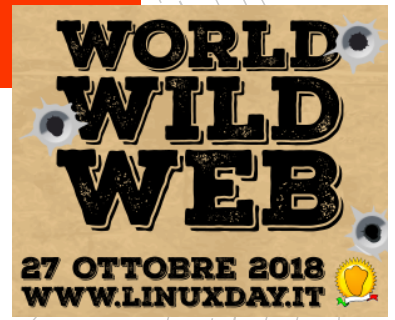
27 ottobre 2018: XVIII giornata nazionale per il software libero

Linux Day a Pisa - 27 ottobre 2018

Analisi e interpretazione degli elementi di prova digitali:

Standard ISO 27042:2016



DirICTo
Diritto & Information and Communication Technology

ICT4Law & Forensics

DirICTo
Diritto & Information and Communication Technology

Linux Day a Pisa

Chi siamo

- DirICTo è un network che raggruppa esperti e studiosi, di tutta l'Italia, in materia di Diritto dell'Informatica e dell'Informatica Giuridica con il fine di sviluppare attività di studio, ricerca e approfondimento nell'ambito delle tematiche di interesse comune per il mondo giuridico e informatico

Web site: **www.diricto.it**

Maria Letizia Perugini
Marco Carlo Spada

ICT4Law & Forensics

Linux Day a Pisa

Chi siamo

Maria Letizia Perugini
Marco Carlo Spada

- ICT for Law and Forensics è il laboratorio di Informatica Forense del Dipartimento di Ingegneria Elettrica e Elettronica dell'Università di Cagliari.
- Aree di interesse: e-commerce e contrattazione telematica, la tutela giuridica dei domain names, privacy e protezione dei dati personali nel mondo telematico, cyber crimes, digital forensics

Web site: **ict4forensics.diee.unica.it**

Linux Day a Pisa

Il team

Maria Letizia Perugini
Marco Carlo Spada

il talk viene presentato contemporaneamente in due sedi

- Smau Milano, relatori
  - Massimo Farina, ricercatore UniCa, Docente di Diritto dell'Informatica
  - Alessandro Bonu, Systems Infrastructure Engineer
- LINUX DAY PISA, relatori
  - Maria Letizia Perugini, blockchain postdoctoral researcher
  - Marco Carlo Spada, Network Security Engineer

Linux Day a Pisa

Il progetto

Maria Letizia Perugini
Marco Carlo Spada

- La presentazione fa parte del progetto di ricerca sugli standard ISO in materia di sicurezza informatica (serie 27000) coordinato dal laboratorio ICT4Law and Forensics
- Nel mondo globalizzato, gli scambi e le comunicazioni si svolgono normalmente in via digitale. I Tribunali italiani si trovano quotidianamente di fronte all'analisi e interpretazione di questi possibili elementi di prova. Quale metodo viene applicato? Come vengono verificati i risultati? Lo Standard ISO 27042 stabilisce le linee guida per questa delicata e importante attività, offrendo un modello di riferimento uniforme

Linux Day a Pisa

Lo standard 27042:2016

Maria Letizia Perugini
Marco Carlo Spada

- È importante che i metodi e i processi utilizzati durante un'indagine siano appropriati
- Lo standard internazionale ISO 27042:2016 fornisce indicazioni su metodi e processi dell'indagine richiamando le altre norme ISO della famiglia 27000 per le prescrizioni di dettaglio
- Le linee guida per le attività specifiche nella gestione degli elementi di prova digitale (identificazione, raccolta, acquisizione e conservazione degli elementi digitali che possono rivestire valore probatorio) sono contenute nello standard ISO 27037:2012

Linux Day a Pisa

Incidenti informatici

Maria Letizia Perugini
Marco Carlo Spada

- Lo scopo principale di un'indagine è quello di acquisire informazioni su un incidente informatico
- Le indagini possono portare a misure correttive, miglioramenti delle misure di sicurezza e dei controlli futuri, azioni disciplinari contro il personale o procedimenti giudiziari civili o penali contro i responsabili dell'incidente
- È fondamentale che l'indagine sia condotta in modo intrinsecamente affidabile e che produca elementi di prova con provenienza affidabile
- Questo risultato richiede investigatori competenti e processi analitici convalidati in modo che ogni elemento di prova digitale possa essere ricondotto alla fonte da cui è derivato

Linux Day a Pisa

Quesito e rapporto di indagine

Maria Letizia Perugini
Marco Carlo Spada

- Prima di avviare l'indagine, la natura e lo scopo della relazione finale devono essere verificati dall'organo inquirente
- Il quesito guida il processo investigativo e può consistere in una serie di domande a cui rispondere, un'indicazione dei probabili destinatari della relazione e dettagli su eventuali vincoli e limitazioni che si applicano all'indagine
- Il responsabile dell'indagine deve preparare una strategia o un piano investigativo documentato al fine di contribuire alla determinazione delle risorse, alla selezione dei processi e degli strumenti e di fornire indicazioni al gruppo investigativo
- Le relazioni devono includere tutte le informazioni richieste dalla normativa locale applicabile

Linux Day a Pisa

Catena di custodia

Maria Letizia Perugini
Marco Carlo Spada

- Una corretta registrazione della catena di custodia e dei processi applicati agli elementi di prova digitale consente di prevenire eventuali problemi di manomissione

- La registrazione deve essere rigorosa e completa riguardo tutti i processi applicati

Linux Day a Pisa

Ripetibilità e riproducibilità

- Gli elementi di prova devono essere raccolti con metodi ripetibili e riproducibili
- Può essere necessario elaborare nuovi metodi durante un'indagine, al fine di rispondere a nuove tecnologie o ad un'esigenza investigativa precedentemente sconosciuta
- L'applicazione di un procedimento convalidato (ISO/IEC 27041) contribuisce a dimostrare che i risultati ottenuti sono affidabili e riproducibili e che soddisfano un'esigenza investigativa

Maria Letizia Perugini
Marco Carlo Spada

Linux Day a Pisa

Approccio strutturato

Maria Letizia Perugini
Marco Carlo Spada

- Gli inquirenti devono garantire che le loro conclusioni siano comunicate nel modo più completo e imparziale possibile
- L'indagine, deve essere condotta da investigatori con competenze accertata e certificata da precorsi di aggiornamento professionale documentabili
- Gli elementi di prova digitale devono essere esaminati secondo prodedure di analisi adeguate ai dispositivi e ai dati oggetto dell'indagine

Linux Day a Pisa

Incertezza

Maria Letizia Perugini
Marco Carlo Spada

- Gli investigatori devono essere consapevoli delle aree di incertezza nei risultati
- In alcune situazioni la presenza di un unico elemento di prova digitale può essere sufficiente ai fini dell'indagine mentre in altre circostanze può essere necessario un corpus di prove più ampio per corroborare l'ipotesi degli investigatori
- Gli investigatori possono richiedere ulteriori indicazioni alla persona o all'organizzazione per conto della quale deve essere effettuata l'indagine

Linux Day a Pisa

Analisi

Maria Letizia Perugini
Marco Carlo Spada

- L'analisi è necessaria in quanto molti elementi di prova digitale vengono reperiti in forma latente
  - tracce di un file cancellato
  - ricostruzione della timeline tramite esame dei metadati
- l'analisi deve fare uso di processi convalidati (come definiti dalla ISO/IEC 27041), deve essere eseguita da personale competente ed essere scrupolosamente documentata per stabilire una provenienza delle informazioni tracciabile e difendibile

Linux Day a Pisa

Interpretazione

Maria Letizia Perugini
Marco Carlo Spada

- L'obiettivo dell'interpretazione è quello di ricavare un significato dagli elementi di prova digitale effettuando una valutazione dei dati e analizzandoli nel contesto delle circostanze
- L'interpretazione porta all'individuazione dei fatti e in alcuni casi al rafforzamento dei fatti con la formulazione di un'ipotesi
- A seconda dei risultati dell'interpretazione può essere necessario reiterare l'analisi o procedere alla rilevazione di ulteriori elementi di prova digitale
- Il team investigativo deve sempre ricordare che la responsabilità primaria di cui è investito è quella di fornire un'interpretazione corretta e accurata dei fatti così come sono stati accertati

Linux Day a Pisa

Competenza

Maria Letizia Perugini
Marco Carlo Spada

- Tutte le fasi dell'inchiesta su un incidente devono essere eseguite da persone di provata competenza
- I componenti del Team devono avere familiarità ed esperienza con gli strumenti, i metodi e le tecniche che utilizzano per poterli eseguire e devono anche essere in grado di riconoscere i limiti delle proprie capacità
- Nel caso in cui un investigatore riconosca i propri limiti, la questione deve essere sottoposta a un individuo più anziano o maggiormente competente per stabilire le azioni appropriate da intraprendere
- Il coinvolgimento di una persona non competente in un'indagine può influire negativamente sui risultati dell'indagine, con conseguenti ritardi nel completamento o conclusioni errate

Linux Day a Pisa

Strumenti informatici

Maria Letizia Perugini
Marco Carlo Spada

- Gli strumenti informatici (combinazioni di software, hardware e firmware) possono essere di grande aiuto nel processo di analisi
- La selezione degli strumenti deve essere basata sui requisiti concordati e sui processi convalidati di analisi (ISO/IEC 27041)
- Gli investigatori devono essere in grado di utilizzare gli strumenti nel contesto del processo di analisi
- I processi che richiedono nuovi strumenti di indagine devono essere convalidati prima dell'implementazione secondo la procedura specificata nella norma ISO/IEC 27041

Linux Day a Pisa

Licenza CC

Attribuzione Non Commerciale Condividi allo stesso modo 4.0 (CC BY-NC-SA 4.0) Internazionale

creative commons

COMMONS DEED

Maria Letizia Perugini
Marco Carlo Spada

- **Tu sei libero di:**

Condividere - riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare questo materiale con qualsiasi mezzo e formato;

Modificare - remixare, trasformare il materiale e basarti su di esso per le tue opere;

Il licenziante non può revocare questi diritti fintanto che tu rispetti i termini della licenza

Alle seguenti condizioni:

Attribuzione. Devi riconoscere una menzione di paternità adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma non con modalità tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.

Non commerciale. Non puoi usare il materiale per fini commerciali.

Stessa Licenza. Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

Divieto di restrizioni aggiuntive — Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare.

Non sei tenuto a rispettare i termini della licenza per quelle componenti del materiale che siano in pubblico dominio o nei casi in cui il tuo utilizzo sia consentito da una eccezione o limitazione prevista dalla legge

Non sono fornite garanzie. La licenza può non conferirti tutte le autorizzazioni necessarie per l'utilizzo che ti prefiggi. Ad esempio, diritti di terzi come i diritti all'immagine, alla riservatezza e i diritti morali potrebbero restringere gli usi che ti prefiggi sul materiale.