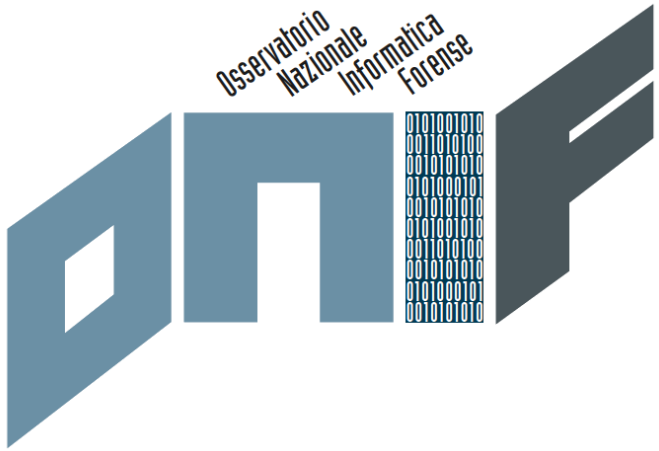


DFA Open Day 2016

Milano, 28 giugno 2016

Università degli Studi di Milano, via Festa del Perdono 7, Aula Malliani

ONIF Survey 2015

La figura dell'informatico forense in Italia

dott. Alessandro Borra

Introduzione

L'Osservatorio Nazionale per l'Informatica Forense (ONIF) nasce dall'idea di un gruppo di professionisti del settore e ha lo scopo di promuovere la figura dell'informatico forense

- ❑ definire metodologie condivise per l'identificazione, l'acquisizione e l'analisi dei dati digitali in ambito forense
- ❑ condividere modalità operative, tecnologia, prestazioni professionali
- ❑ predisporre ed aggiornare periodicamente la valutazione economica dei servizi di informatica forense su casi paradigmatici
- ❑ sensibilizzare, a tutti livelli, il riconoscimento della professionalità e una congrua valutazione economica della stessa
- ❑ diffondere la conoscenza dell'informatica forense e il suo riconoscimento ufficiale

www.onif.it

Obiettivi del ONIF Survay 2015

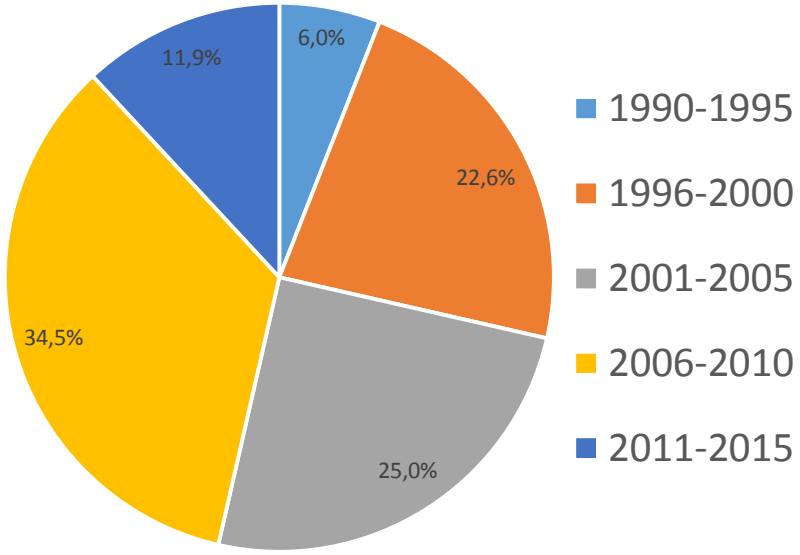
- ❑ interamente dedicato alla **figura professionale dell'Informatico Forense**
- ❑ delineare un quadro delle caratteristiche e delle criticità di questa attività professionale

- ❑ 84 domande suddivise in 6 aree tematiche:
  - **Formazione** personale e professionale
  - Modalità di svolgimento della **professione**
  - **Laboratorio** e attrezzature di lavoro
  - Composizione dei **compensi**
  - Attività di **divulgazione** della materia
  - Sviluppi e **sfide future**

- ❑ survey aperto dal 23 novembre al 31 dicembre 2015
- ❑ 127 questionari completati

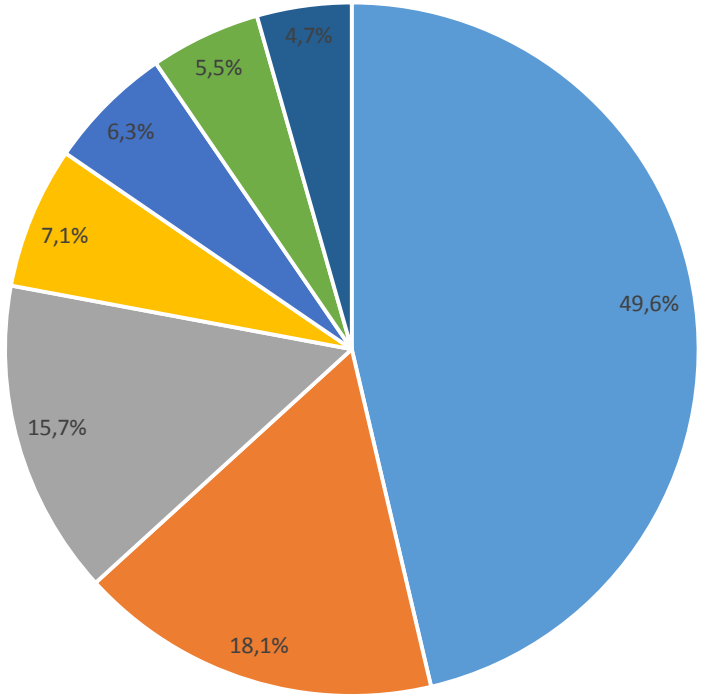
Profilazione 1/6 partecipanti

anno di inizio attività



(95 risposte)

come svolge l'attività professionale?



- Libero professionista autonomo
- Altro
- Titolare di azienda
- Dipendente di azienda che opera nell'ambito dell'informatica forense
- Dipendente di azienda che opera in altri settori
- Dipendente di azienda che opera nel settore ICT
- Studio Associato di liberi professionisti

(domanda con risposta multipla)

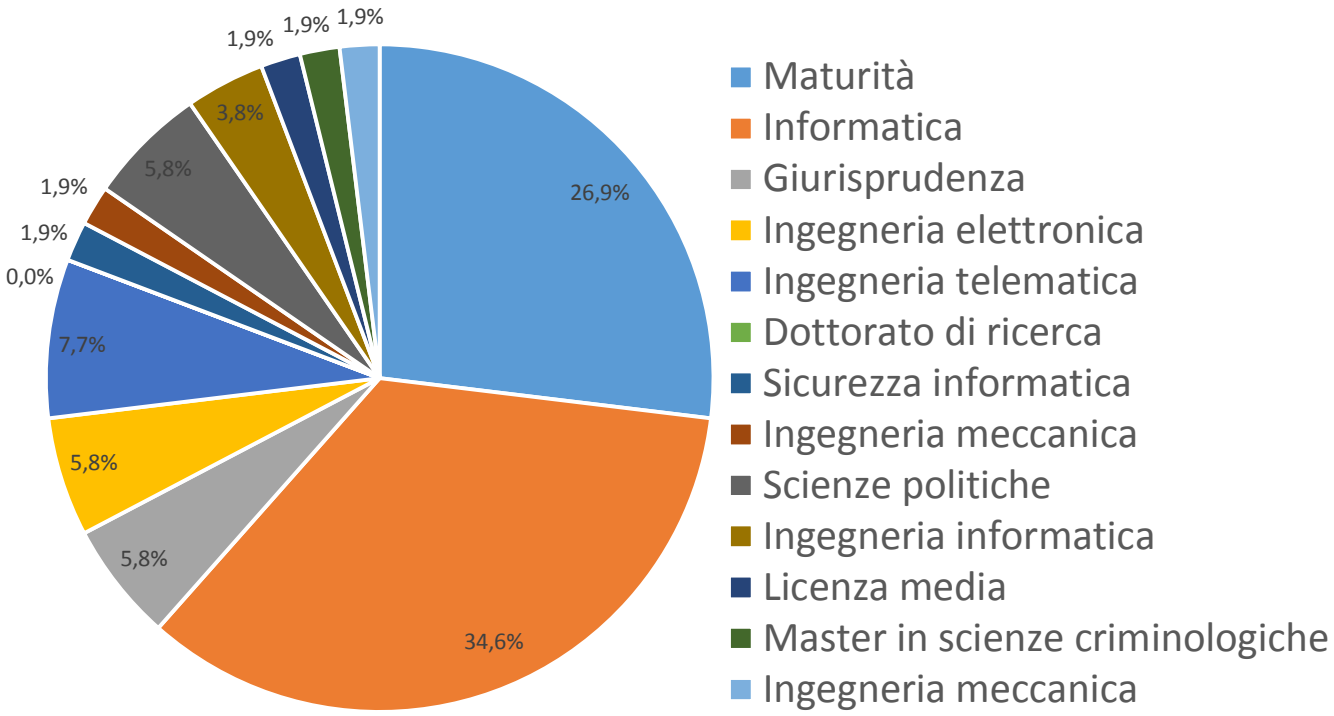
Profilazione 2/6
titolo di studio 1

- il **72,6% ha una laurea, ma solo il 40,3% ha una laurea attinente alla materia**
- il **19,2%** ha una laurea in materie non scientifiche (giurisprudenza, economia e commercio, scienze politiche, psicologia, …)

Licenza media	Ingegneria	Laurea (generico)
Maturità	Ingegneria civile	Psicologia
Master in scienze criminologiche	Ingegneria elettronica	Scienze delle comunicazioni
Dottorato di ricerca	Ingegneria elettrotecnica	Scienze giuridiche
Economia	Ingegneria informatica	Scienze politiche
Fisica	Ingegneria meccanica	Sicurezza informatica
Giurisprudenza	Ingegneria telematica	
Informatica		

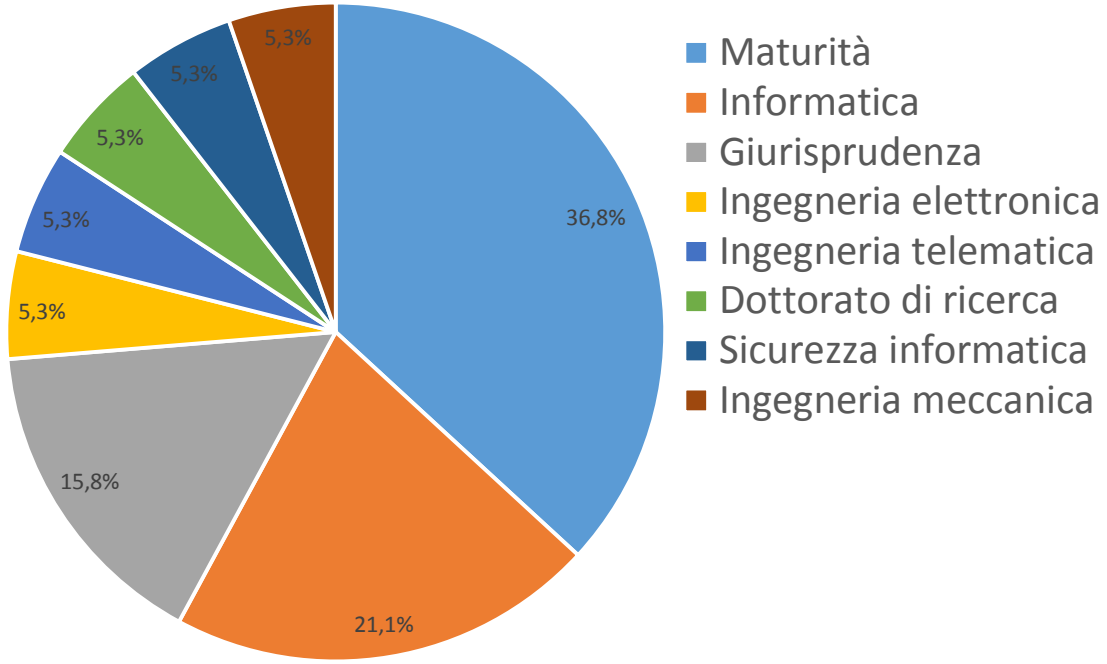
Profilazione 3/6
titolo di studio 2

CT dal 2005



(56 elementi)

CT dal 2010



(19 elementi)

Profilazione 4/6
formazione e aggiornamento professionale

- il **33%** ha seguito un **corso di formazione in materia** tra quelli offerti dalle principali associazioni e dai produttori di riferimento nel settore (prevalentemente SANS, IISFA, AccessData e Encase)

- il **22%** ha conseguito una **certificazione professionale**: CIFI (IISFA), ACE (AccessData) e GCFA (SANS)

- **aggiornamento professionale**:
  - avviene prevalentemente attraverso l'ausilio di **libri e pubblicazioni scientifiche**, la consultazione di **siti web** e l'accesso a **mailing list e social network** sull'argomento
  - il **43% investe meno di 500 €/anno**
  - solo il **12% più di 2.000 €/anno**

Profilazione 5/6
albi e assicurazioni professionali

- il **53% non è iscritto ad alcun albo professionale**, i restanti sono per lo più ingegneri

  Il motivo di non iscrizione è prevalentemente dovuto **all'assenza di un albo degli informatici** per chi non ha una laurea

- il **42% è iscritto all'albo dei Consulenti Tecnici e dei Periti** presso il proprio Tribunale di riferimento

- alcuni addirittura sono **iscritti a più Tribunali** (anche se teoricamente non è possibile…)

- solo il 30% ha una **assicurazione professionale**

Profilazione 6/6 divulgazione

- **il 25% ha avuto o ha tuttora un incarico di docenza presso una Università**, prevalentemente attraverso un incarico professionale all'interno di corsi universitari, di perfezionamento o master
- **il 36% svolge o ha svolto attività di docenza in corsi professionali**
- **il 50% partecipa o ha partecipato come relatore a seminari/workshop/conferenze in materia**
- gli argomenti più trattati in contesto formativo sono **Computer, Mobile e Network Forensics**
- il compenso medio per una attività di docenza professionale è pari a **120 €/h**

Lavoro 1/5
tipologie di clienti e di ambiti giuridici

- la maggior parte ha svolto consulenze in **ambito penale e/o civile**, con presenza di casi in ambito **giuslavoristico** e **stragiudiziale**

- i soggetti dai quali principalmente i consulenti ottengono incarichi sono **pubblici ministeri, avvocati penalisti, polizia giudiziaria** in qualità di ausiliario, **avvocati civilisti** e **aziende**

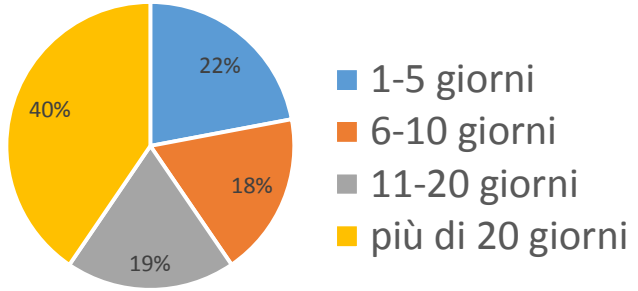
- il contatto con un nuovo cliente avviene prevalentemente attraverso il **passa parola** (di P.M./Giudici/A.G./Studio Legale/Azienda) e a seguito di **incontro personale** (es. convegno)

- quando si svolge un'**attività per una azienda**:
  - il **90% fa firmare una lettera di incarico e/o altra documentazione**
  - al termine dell'attività si mantengono i rapporti professionali con l'azienda (nel 40% dei casi) e con lo studio legale (nel 33% dei casi)

Lavoro 2/5
quantità, durata e area geografica

- il **37% ha svolto negli ultimi 3 anni da 1 a 10 consulenze**
- il 22% circa ne ha svolte più di 50

- nel **40% dei casi lo svolgimento di una consulenza richiede più di 20 giornate lavorative**, mentre nel 20% da 1 a 5, da 6 a 10 o da 11 a 20

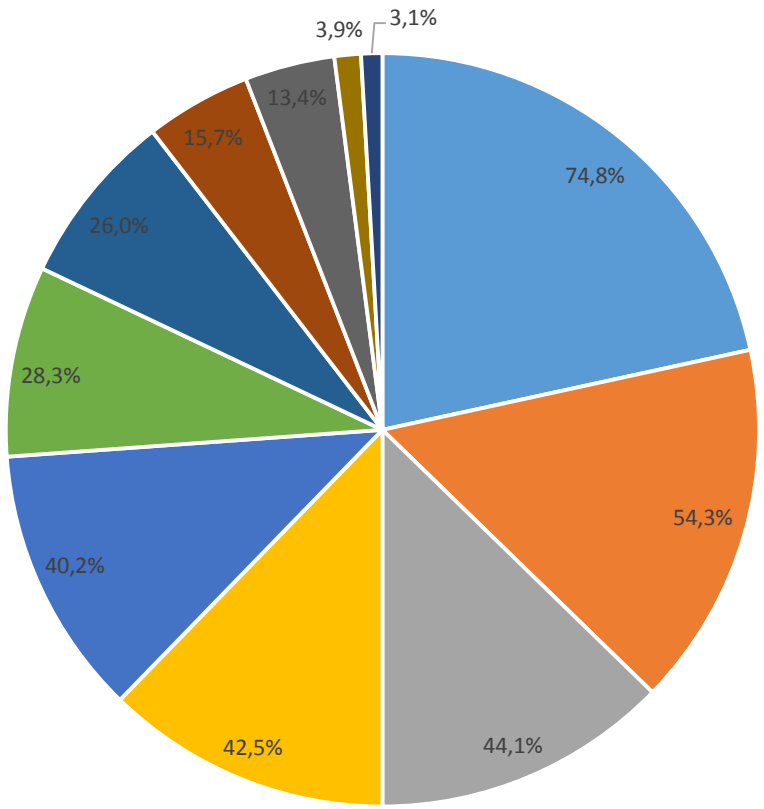


- le regioni italiane dove si opera maggiormente sono **Lombardia, Lazio, Emilia Romagna, Toscana, Veneto** e **Campania**

- il 18% degli intervistati ha svolto anche attività in Europa e l'8% Extra-Europa

Lavoro 3/5
requisiti minimi del consulente

36. [PROFESSIONE] A suo parere, quali tra i seguenti criteri/requisiti minimi deve soddisfare un consulente tecnico informatico forense?

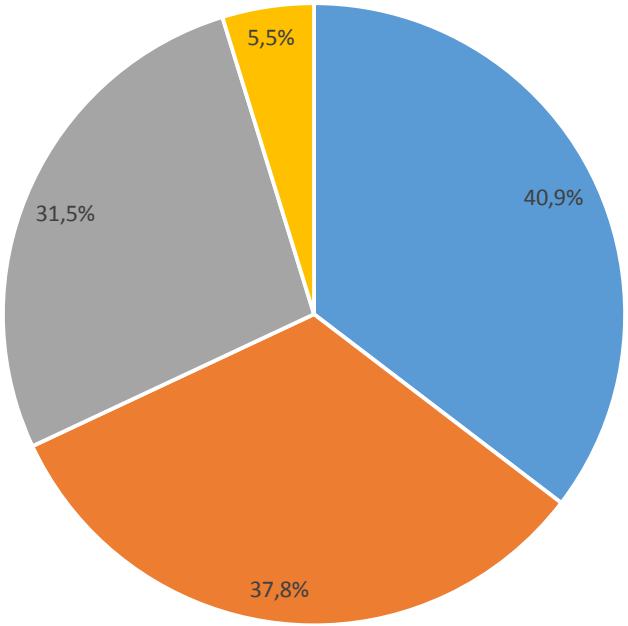


- Formazione continua
- Etica del consulente, anche rispetto al background professionale
- Anni minimi di esperienza (es. 3 o 5)
- Esperienza specifica del caso trattato
- Laurea e/o dottorato in materia di informatica (Informatica, Ingegneria Informatica, Elettronica, Telecomunicazioni)
- Possesso di certificazioni in materia di Digital Forensics
- Attività di ricerca in materia svolta personalmente o in collaborazione con enti/università
- Diploma di perito informatico/elettronico
- Sviluppo di software open per la comunità scientifica
- Altra laurea in ambito scientifico
- Altro

(domanda con risposta multipla)

Lavoro 4/5
criteri di selezione

38. [PROFESSIONE] Quale dei seguenti criteri dovrebbe a suo parere essere adottato per l'individuazione di un consulente tecnico che svolge attività per l'Autorità Giudiziaria?



- Attraverso la costituzione di un albo nazionale dei Consulenti Tecnici e dei Periti
- Attraverso gli albi dei Consulenti Tecnici e dei Periti delle procure e dei tribunali
- A libera discrezione del Giudice/Pubblico Ministero
- Altro

Lavoro 5/5
ambiti tecnologici di consulenza

- si analizzano prevalentemente **personal computer con sistema operativo Windows** e **server con sistema operativo Windows e Linux**

- nel mondo mobile principalmente si analizzano smartphone **Android** e **iOS**

- altri ambiti dove si riscontrano attività di consulenza sono:
  - tabulati e celle telefoniche
  - incident response
  - malware
  - sistemi di videosorveglianza
  - audio e video
  - network
  - analisi di software (es. valutazione delle specifiche rispetto al contratto)

Laboratorio 1/2

- impiegati **sia strumenti commerciali sia strumenti opensource**

- la prevalenza utilizza **distribuzioni Linux** per le attività di acquisizione (in particolare **DEFT** e **CAINE**). Una buona percentuale è dotata anche di strumenti hardware come **write blocker (45%)** e **duplicatori (38%)**

- il **35% non possiede strumenti per l'acquisizione di dispositivi mobile**

- **software commerciali** più utilizzati
  - X-Ways
  - EnCase
  - FTK
  - IEF
  - UFED Cellebrite
  - Oxygen Forensic
  - MobilEdit

- **software free/opensource** più utilizzati
  - FTK Imager
  - Autopsy
  - OS Forensics
  - RegRipper
  - The Sleuth Kit

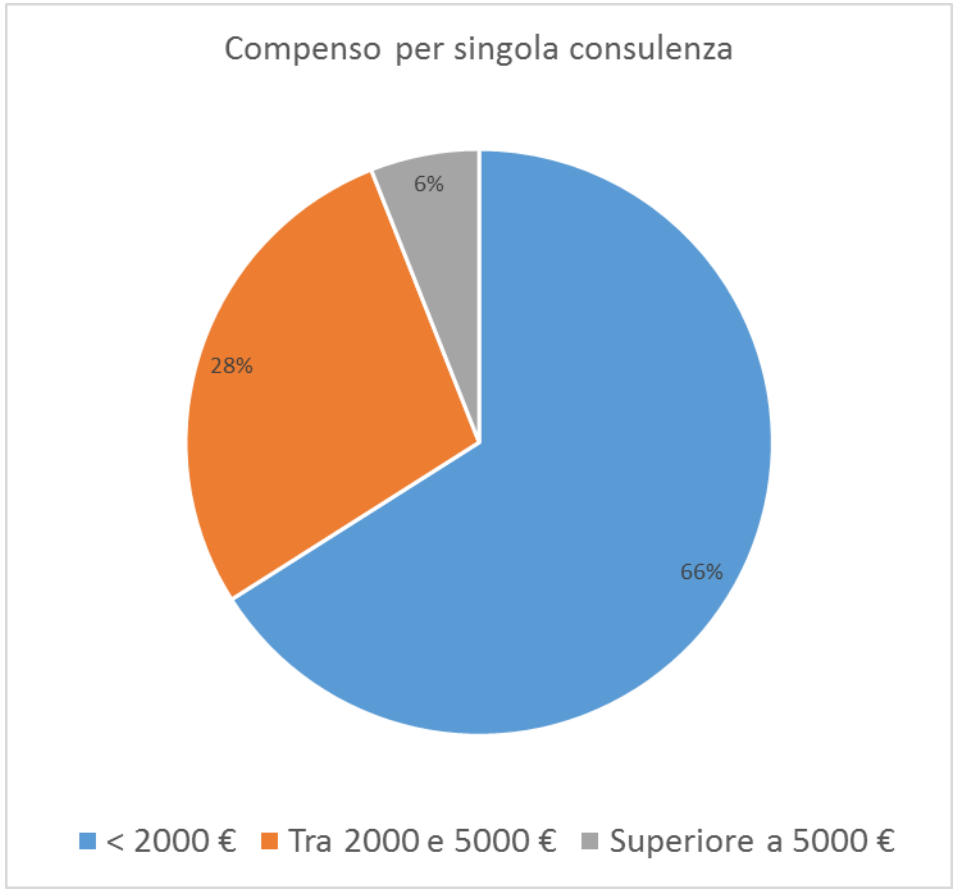
Laboratorio 2/2
costi e investimenti

- a seconda del numero di anni di attività e del tipo di realtà (es. singolo consulente o azienda) si registrano **diversi livelli di investimento sia complessivo sia annuale**

- alcune osservazioni generali di interesse:
  - il **50% ha sostenuto un investimento complessivo inferiore ai 20.000 €** per tutte le attrezzature di laboratorio (personal computer/workstation, notebook, sistemi di storage, duplicatori, write blocker, software/hardware per dispositivi mobile, software di analisi, ecc.)
  - l'**80% investe meno di 2.500 € all'anno per il mantenimento/upgrade hardware**
  - il **64% investe meno di 2.500 € all'anno per acquisto/rinnovo di licenze software**

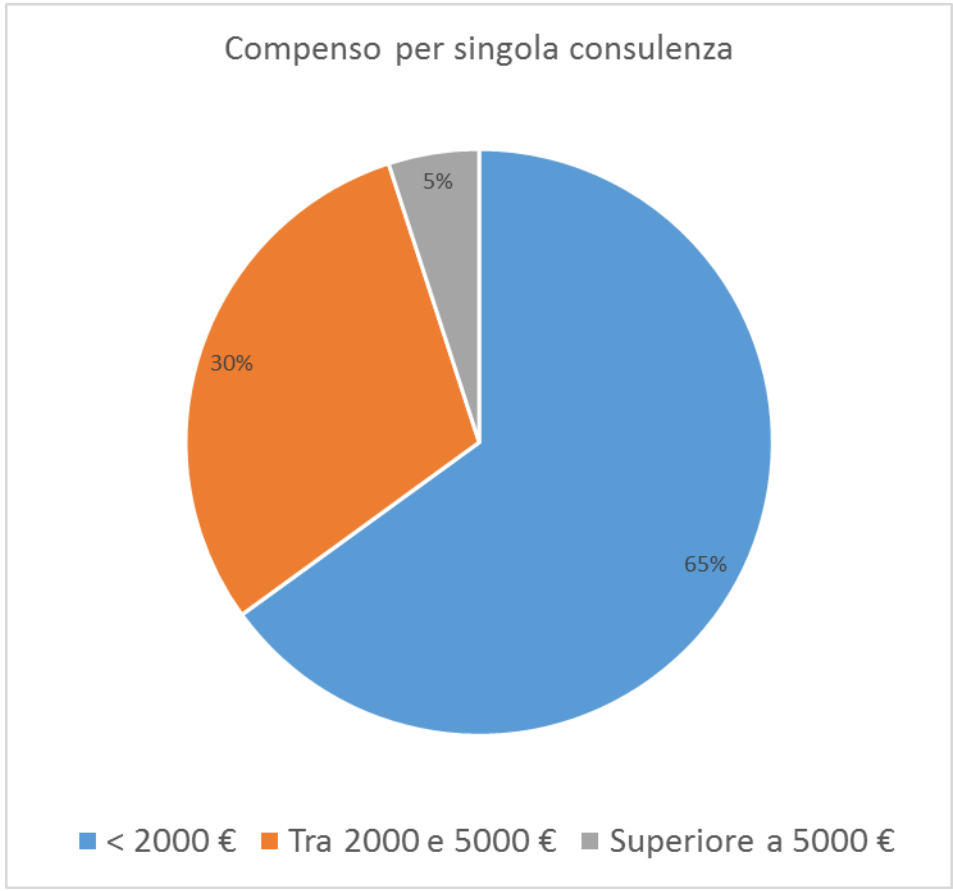
Clienti e compenso 1/6
Pubblico Ministero

- il **63%** svolge attività di consulenza per **Pubblici Ministeri**
- il pagamento avviene
  - a **vacazioni** (**90%** dei casi)
  - a seguito di **preventivo** (**10%**)



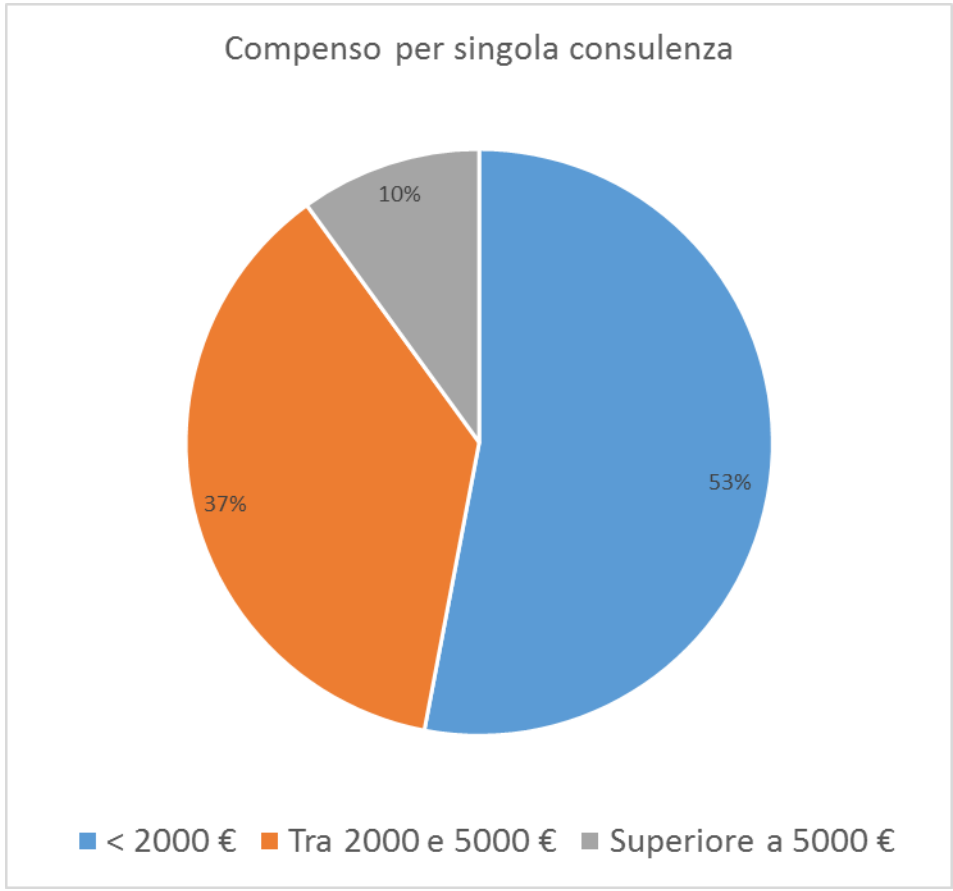
Clienti e compenso 2/6
Giudice Penale

- il **50%** svolge attività di consulenza per **Giudici Penali**
- il pagamento avviene
  - a **vacazioni** (**85%** dei casi)
  - a seguito di preventivo (**15%**)



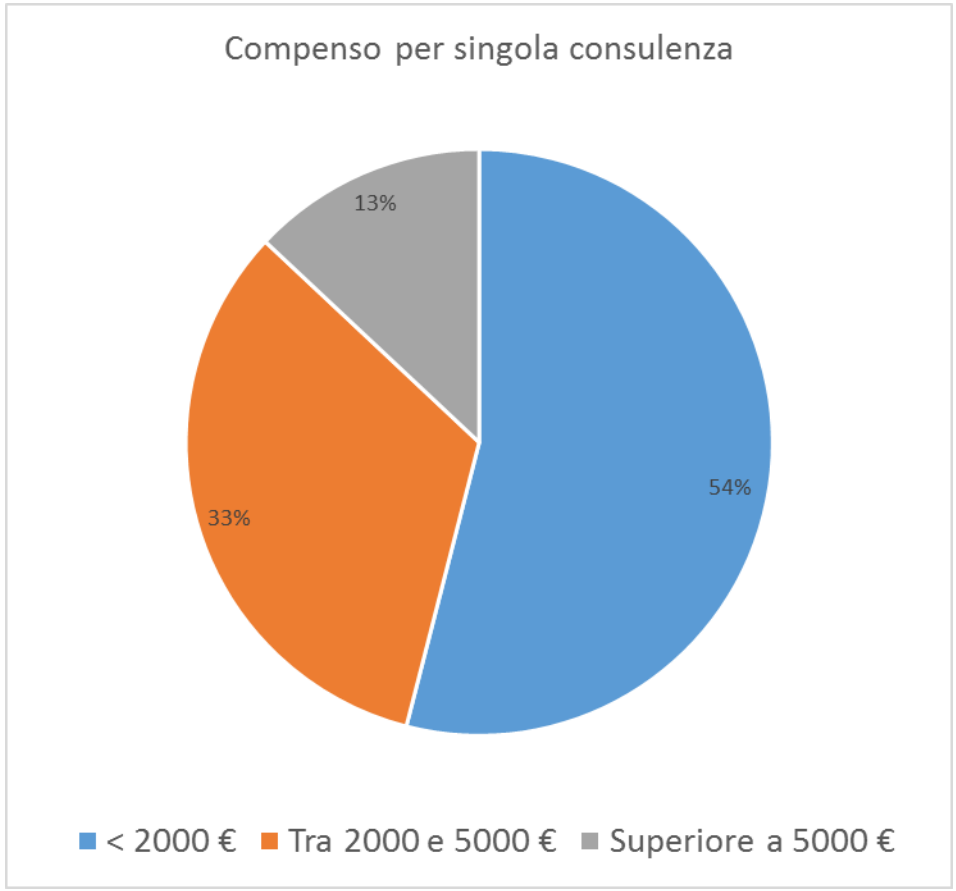
Clienti e compenso 3/6
Giudice Civile

- il **50%** svolge attività di consulenza per **Giudici Civili**
- il pagamento avviene
  - a **vacazioni** (**60%** dei casi)
  - sul **valore della causa** (**23%**)
  - a seguito di **preventivo** (**17%**)



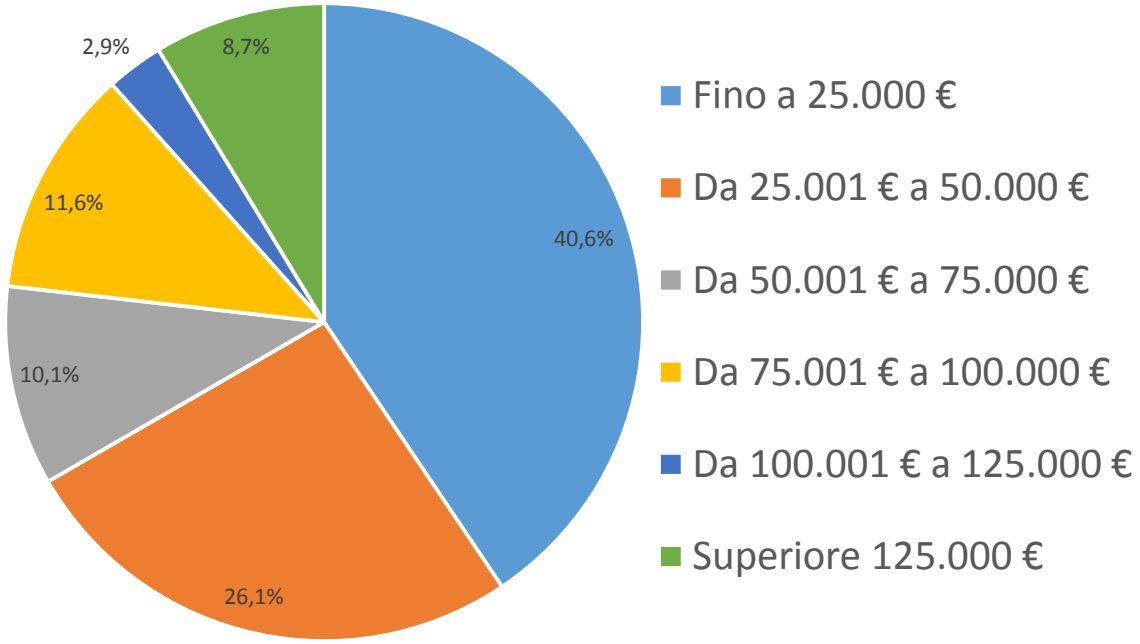
Clienti e compenso 4/6 aziende/studi legali

- più dell'**80%** svolge attività di **consulenza per aziende e studi legali**
- nel **90%** dei casi viene presentato un **preventivo prima delle attività**
- modalità di pagamento
  - nel **48%** è richiesto un acconto al momento dell'incarico
  - nel **41%** l'incasso è al termine della consulenza
- per chi applica **tariffe orarie**, il compenso medio richiesto è pari a circa **120 €**

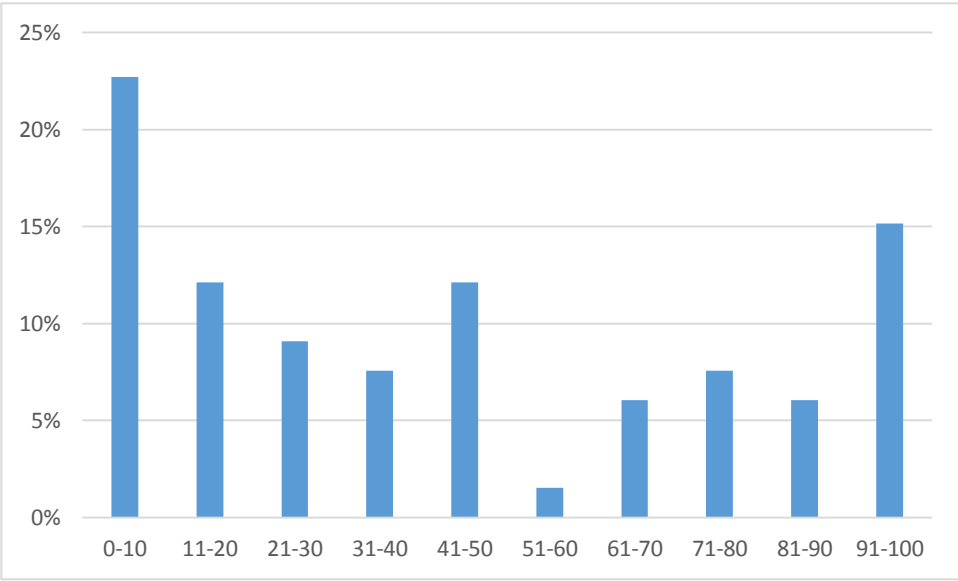


Clienti e compenso 5/6 fatturato

68. [COMPENSO] Quale è il fatturato medio annuo della sua attività professionale negli ultimi 3 anni? [Per i dipendenti non si intendono le consulenze tecniche svolte per il datore di lavoro, ma unicamente quelle svolte come attività professionale personale]

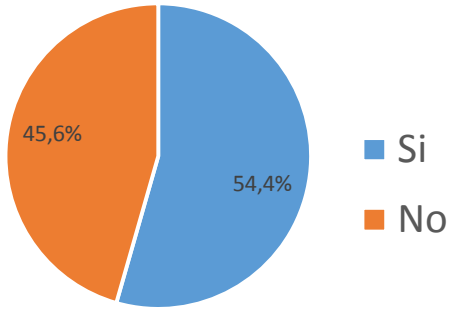


% di fatturato proveniente da D.F.

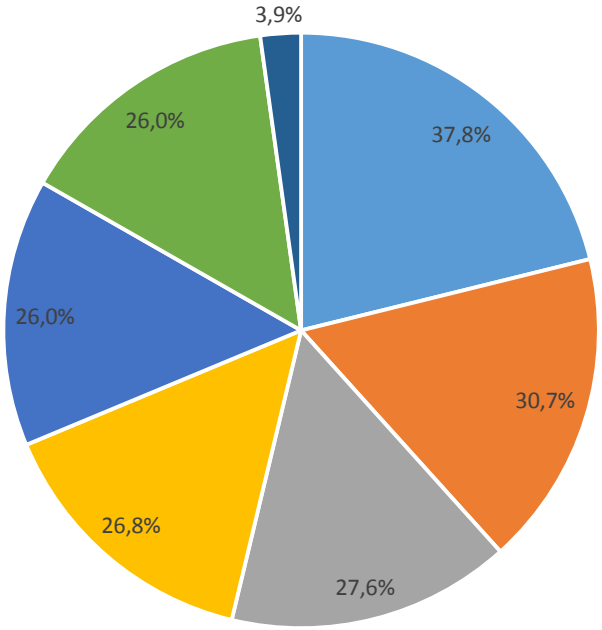


Clienti e compenso 6/6
andamento e prospettive

70. [COMPENSO] Negli ultimi 3 anni il reddito/fatturato personale in termini di consulenze tecniche informatico forensi è sempre stato in crescita?



72. [COMPENSO] Quali tra le seguenti iniziative ritiene che possano consentire un incremento del volume di attività?

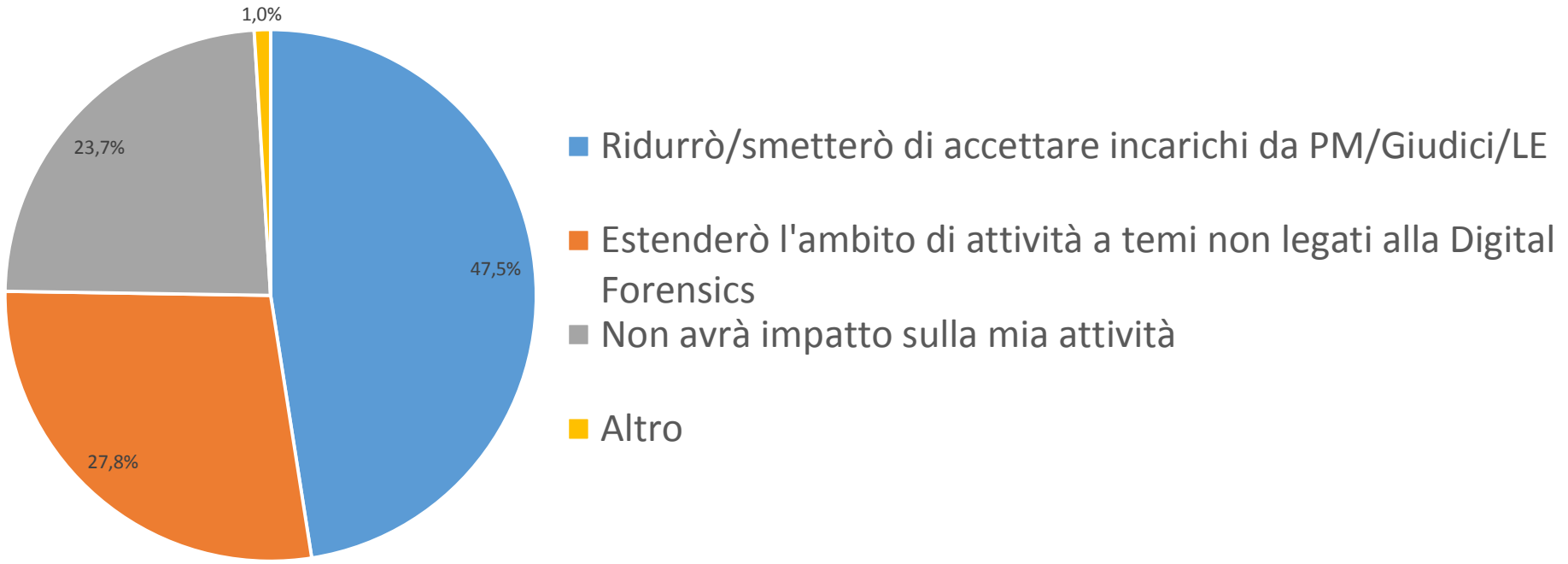


- Partecipazione ad attività di formazione (seminari, convegni, corsi, ecc.) in qualità di relatore/docente
- Marketing mirato
- Partecipazione ad attività di formazione (seminari, convegni, corsi, ecc.) in qualità di discente
- Conseguimento di certificazioni
- Pubblicità online/offline
- Investimenti hardware e software
- Altro

(domanda con risposta multipla)

Sviluppi 1/2
attività per il pubblico

73. [COMPENSO] Se il contesto normativo alla base del compenso pubblico non verrà adeguato nei prossimi anni, ritiene che:



Sviluppi 2/2
sfide future

- necessità di **linee guida, metodologie e tool per l'acquisizione di dati remoti/su cloud**
- tecniche di **acquisizione di dispositivi mobile** e superamento di codici di protezione e/o sistemi di cifratura
- analisi delle **applicazioni mobile**
- acquisizione e analisi di **dispositivi non convenzionali** (es. smartwatch, glasses, smart tv, domotica, robotica, automotive)
- **valute elettroniche**
- investigazioni nel **deep web**
- sistemi **SCADA**
- **droni**

Conclusioni

- **Professione:**
  - **variegata**, composta da una elevata percentuale di persone la cui preparazione non appare idonea al ruolo
  - **complessa**, poiché richiede costante studio e aggiornamento
  - **costosa**, poiché per farla al meglio è inevitabilmente necessario dotarsi di strumenti e di formazione adeguata. E i software e la formazione costano!
  - **a basso profitto**, come si evince sia dai numeri sulle singole consulenza sia dal fatturato complessivo

Proposte

- **definizione di linee guida** tecniche e procedurali riconosciute in Italia
- **divulgazione e studio della materia**, anche attraverso una più ampia diffusione nelle università di corsi di Informatica Forense nei curriculum legati alla Sicurezza Informatica
- **riconoscimento professionale**, ad esempio mediante l'istituzione di un registro nazionale degli esperti forensi
- **valorizzazione economica** per chi opera a supporto di Procure e Tribunali mediante l'adeguamento dei criteri di liquidazione dei compensi a Consulenti Tecnici così come previsto dal T.U. Spese di Giustizia

DFA Open Day 2016

Milano, 28 giugno 2016

Università degli Studi di Milano, via Festa del Perdono 7, Aula Malliani

Grazie per l'attenzione!

www.onif.it

info@onif.it