



Roma, 10 giugno 2010

SECURITY SUMMIT 2010

by IISFA Italia

www.iisfa.it

IISFA Survey 2010

Lo stato dell'arte della computer forensics in Italia

Gerardo Costabile - presidente@iisfa.it



Intervistati e finalità d'indagine

Lo scopo dell'indagine e della conseguente attività di rielaborazione e studio dei dati raccolti è stato quello di raccogliere un volume significativo di informazioni che riguardano la "comunità" dei soggetti coinvolti nelle attività di computer forensics.

Le opinioni raccolte hanno consentito di delineare a tutto tondo la disciplina dell'analisi forense in relazione soprattutto alle sue criticità: sono infatti emersi problemi concreti e bisogni nonché differenze comportamentali tra categorie.

L'originalità dell'indagine è data dal fatto che è il primo studio basato su metodologia di self-assessment in Italia e che anche sul piano internazionale non sembrano al momento sussistere analisi strutturate di questo tipo.



All'indagine hanno partecipato in 178, ristretti al territorio italiano.



Metodologia seguita

La raccolta di opinioni e dati è stata svolta per mezzo di un questionario strutturato, distinto per categorie e articolato per aree omogenee, con una sola area comune. Le domande prevedevano una sola risposta, salvo in alcuni casi la possibilità di fornire risposte libere o anche più di una risposta, in modo da trattare successivamente i dati raccolti in modo automatizzato (tramite applicazione software web-based).

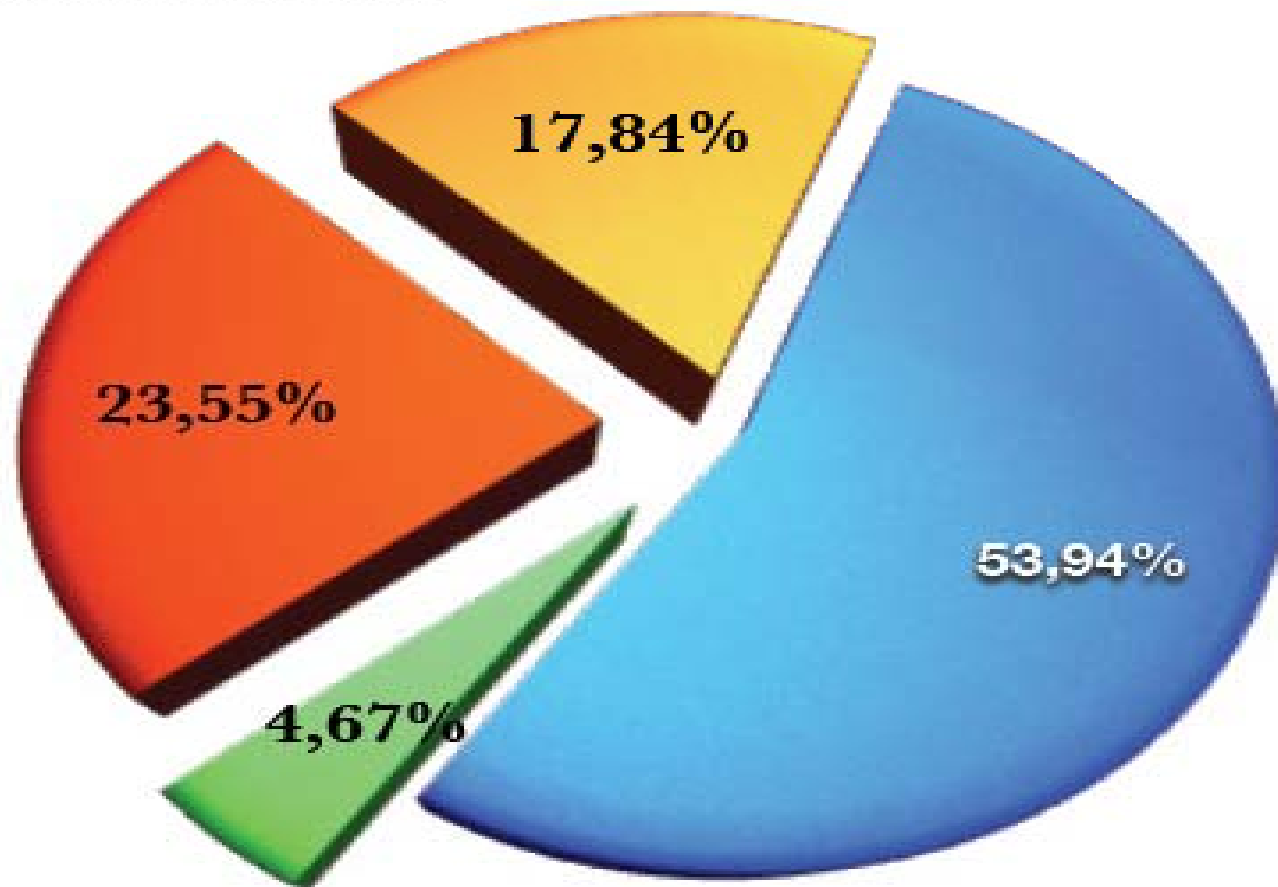
Le categorie individuate ed oggetto di analisi sono le seguenti:

- **Consulente o Azienda che fa consulenze**
- **Azienda che commissiona consulenze**
- **Pubblico Ministero**
- **Avvocato**
- **Investigatore ordinario**
- **Investigatore che fa computer forensics**
- **Giudice**



Gli intervistati

- Consulente e investigatore che fa computer forensics
- Azienda che commissiona consulenze
- Giudice, Pubblico Ministero e investigatori classici
- Avvocato





Sezione Comune a tutti gli intervistati: Introduzione in Italia della Convenzione di Budapest – Legge n. 48 del 2008

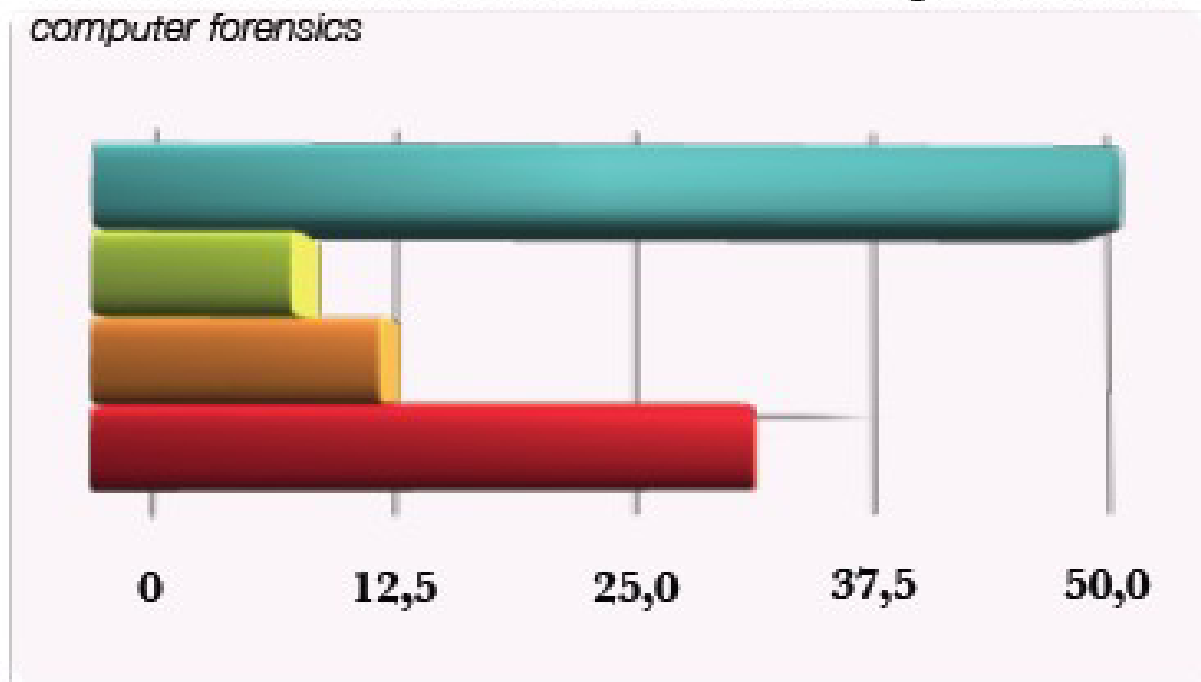
- Secondo il 77% degli intervistati le innovazioni introdotte nel codice di procedura penale italiano sono importanti.
- Il 23% invece ha espresso una posizione problematica: è stato detto che la legge 48, per taluni aspetti, comporta ulteriore confusione in termini procedurali, rendendo difficoltosa l'applicazione della perquisizione d'iniziativa da parte della polizia giudiziaria non specializzata.
- E' stato rilevato che le innovazioni normative introdotte dovrebbero integrarsi con dei rimandi ad un disciplinare tecnico (almeno per la CF), come avviene per il codice della privacy.
- Secondo il 95% degli intervistati è necessario disporre di linee guida per l'informatica forense: tuttavia per il 58% degli intervistati le linee guida per l'informatica forense devono essere procedure molto puntuali e precise, mentre per il 39% devono limitarsi a enunciare principi di massima.
- Quanto al soggetto che dovrebbe emettere le linee guida, il 34% affida questo ruolo a norme internazionali, a seguire il 25% che pensa a associazioni nazionali e internazionali, il 20% che fa riferimento a norme nazionali, il 16% le università.
- Il campione si divide nettamente su questo punto: il 50% propende per una codificazione normativa tradizionale con preferenza per la codificazione internazionale, mentre l'altro 50% ha espresso una preferenza per una codificazione non avente valore e forza di legge, come è quella delle associazioni.



Le motivazioni che spingono alla computer forensics: consulenti e investigatori

Il 47% dei consulenti/investigatori di c.f. svolge l'attività per passione: molto bassa la percentuale di quelli che dichiarano di svolgerla come unica attività: appena il 30%. Tale dato trova riscontro in quanto rilevato dagli avvocati per cui il 60% delle attività di computer forensics vengono effettuate/richieste come lavoro occasionale (35%) o per hobby (25%) e solo per il 35% come lavoro principale.

Motivazione dell'attività svolta dai consulenti/investigatori che fanno computer forensics

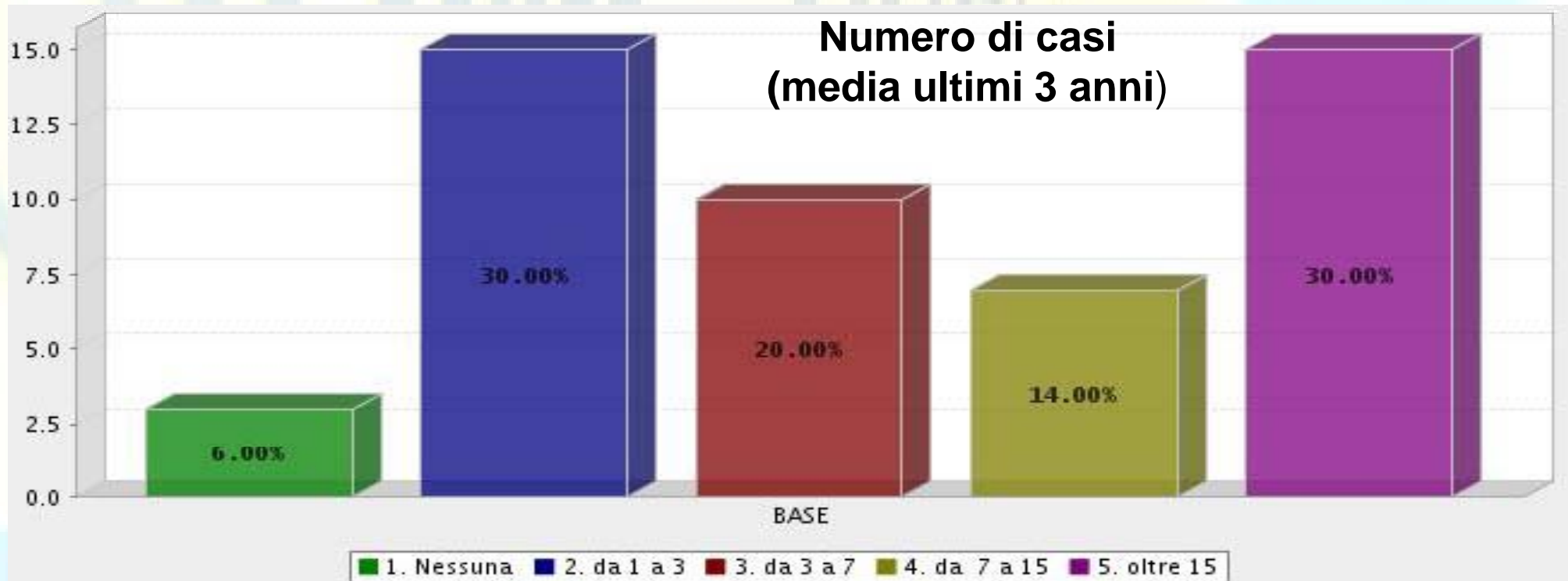


- Per passione**
- Per incrementare i guadagni**
- Come secondo lavoro, durante il tempo libero**
- Come unica attività o comunque come attività principale**



Il *computer forensics expert* “tipo”

Il consulente/investigatore di computer forensics medio che emerge dalla survey svolge l'attività per lo più come dipendente all'interno di società/pubblica amministrazione, con una esperienza media da 3 a 8 anni. L'attività di computer forensics è svolta più per passione che come secondo lavoro o come fonte di incremento guadagni.





Il *computer forensics* expert “tipo” (segue)

- Il peso consistente della motivazione di svolgimento dell'attività “per passione” è rivelatore del fatto che la materia non ha una maturità tale da spingere il consulente a staccarsi dall'hobbistica e vivere come un professionista del settore. Il dato “per passione” si collega con il dato “dipendente” probabilmente in considerazione del fatto che la computer forensics non è “core” delle attività come dipendente.
- Il consulente tipo lavora per lo più per clienti istituzionali e nel settore penale. Le consulenze di computer forensics riguardano per lo più casi in cui il computer è mero contenitore e la tipologia di reato più seguita è il P2P/pedopornografia. In materia di illecito civile, l'infedeltà aziendale ha costituito materia maggiore per consulenza di computer forensics.



Computer forensics expert: guadagni

- **Se effettuata per clienti istituzionali, una consulenza tecnica in Italia è pagata da €500 a €1.500, con una tempistica per i pagamenti di oltre 150 gg;**
- **Se effettuata per clienti privati, da € 1.000 a € 3.000 ed è pagata entro 30 gg.**
- **La preferenza accordata al cliente istituzionale, nonostante l'enorme divario rispetto al cliente privato in termini di entità del corrispettivo e di tempi di pagamento si spiega con la considerazione che il cliente istituzionale (si pensi alla qualità e quantità delle casistiche oltre che alla qualificata esperienza, con innegabili effetti curriculari).**

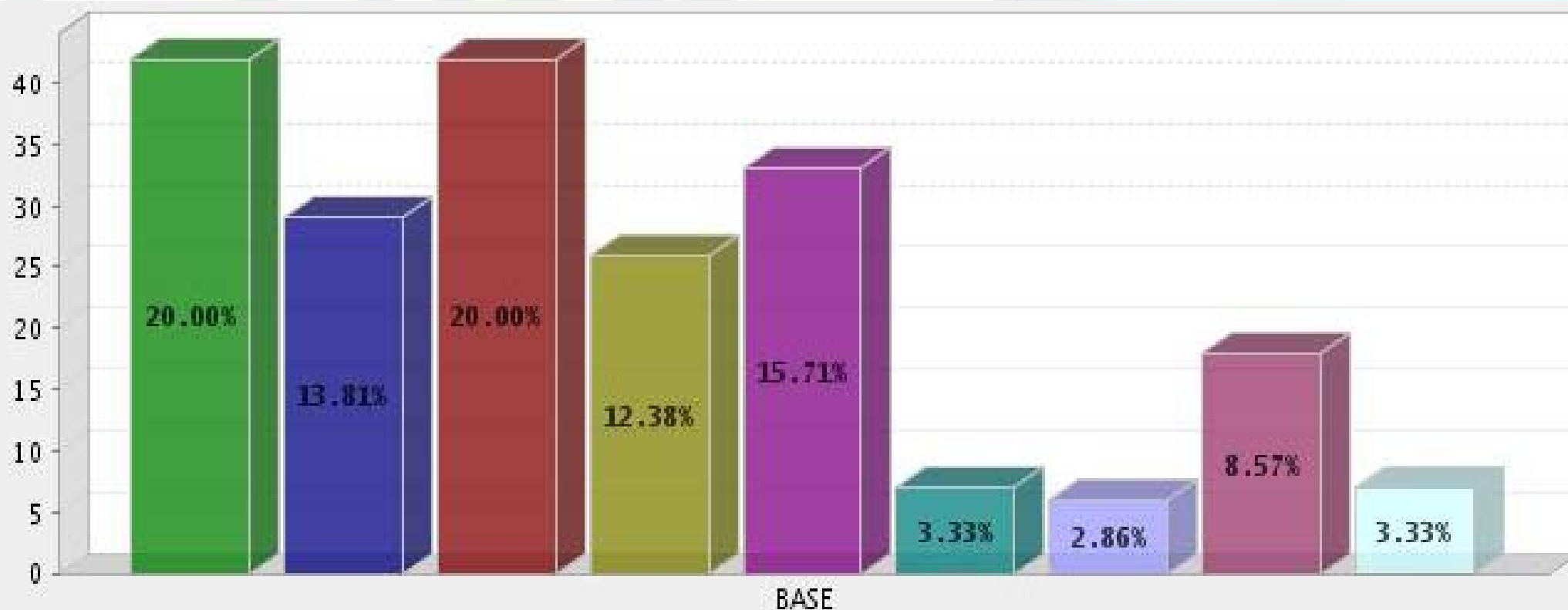


Cosa dicono gli altri sui guadagni?

- **Avvocati:** pagano tra 1.000 e 3.000, con punte di 8.000 euro. Tempi tra 30 e 60 gg per la consegna del lavoro e acconto/saldo a fine lavoro per il metodo di pagamento
- **Magistrati/investigatori classici:** tra i 1.500 e i 3.000 euro, con metodo a vacanza. Tempi di consegna sui 60 gg medi, pagamento oltre i 120 gg.
- **Azienda (cliente):** tra i 1.000 e gli 8.000 euro, consegna lavoro tra i 30 e i 60 gg, pagamento entro i 90 gg.



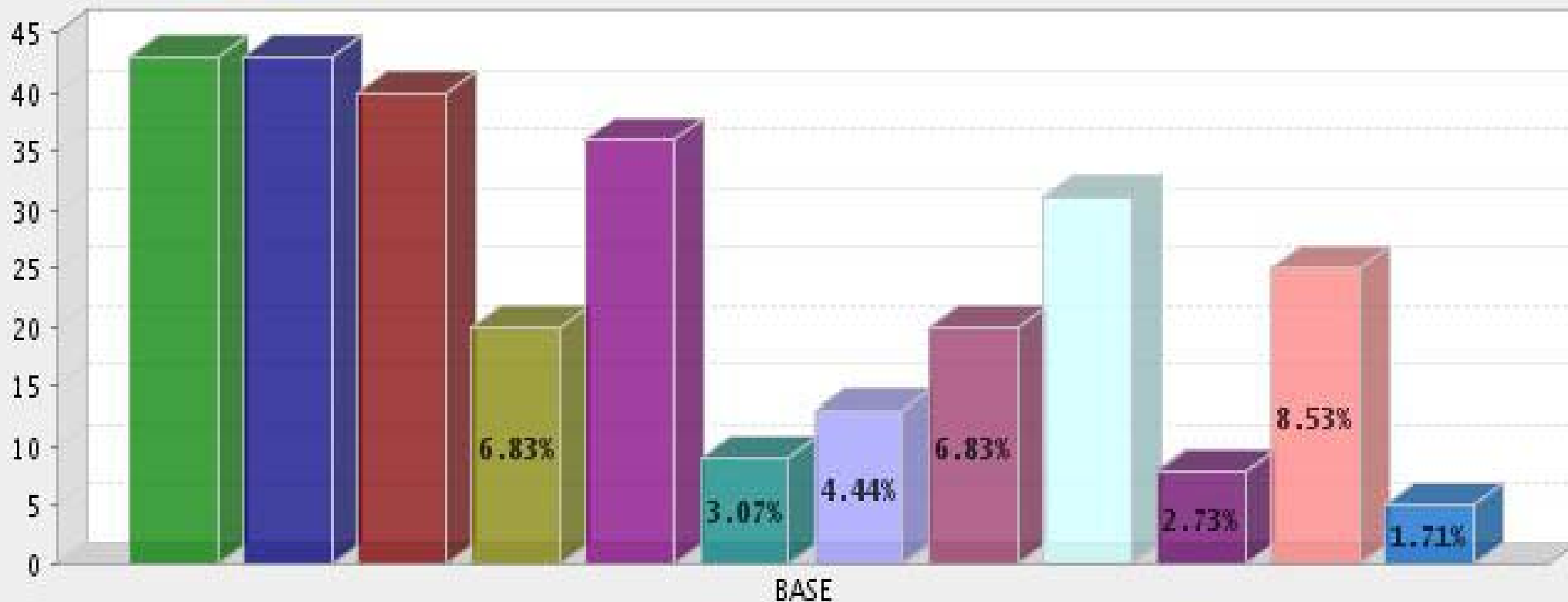
Tipologia di consulenze tecniche effettuate



1. Forensics su pc Portatili 2. Forensics su Server 3. Forensics su Desktop 4. Forensics su cellulari/Palmari
5. Forensics su memorie rimovibili 6. Forensics su Console (xbox, play station etc)
7. Forensics su decoder, mediaplayer etc 8. Network Forensics 9. Altro



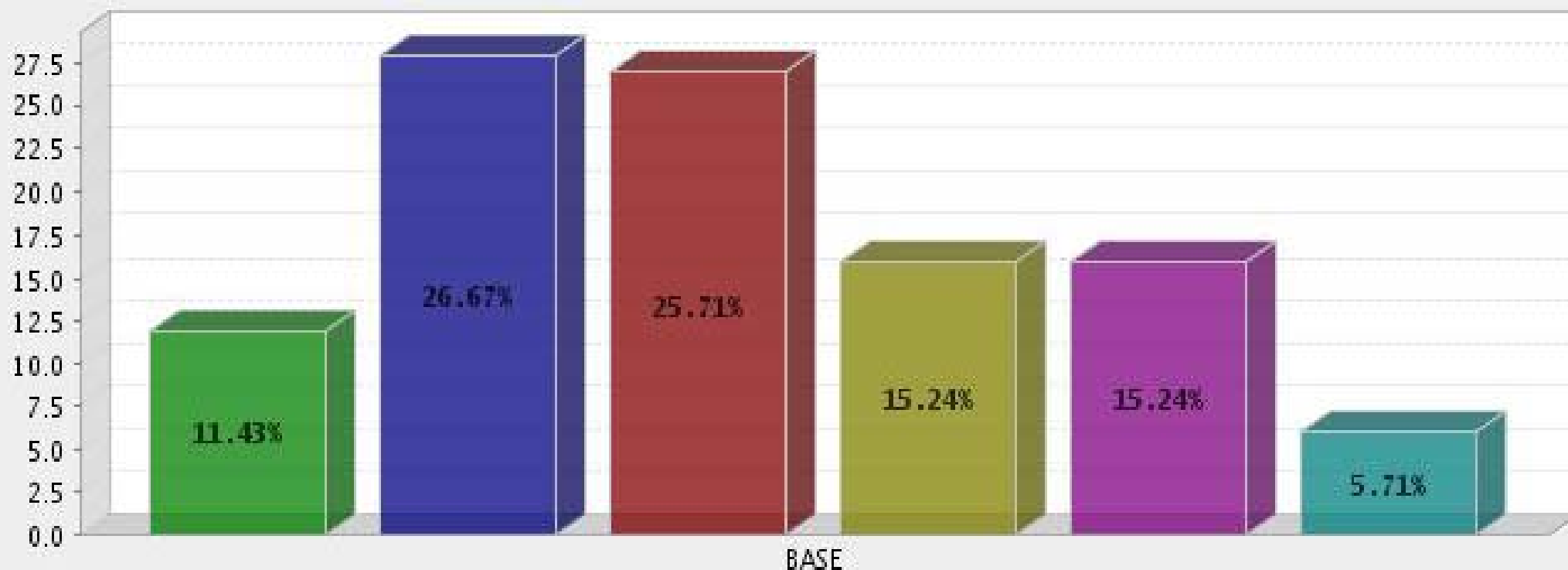
Tipologia di quesiti richiesti per l'analisi forense



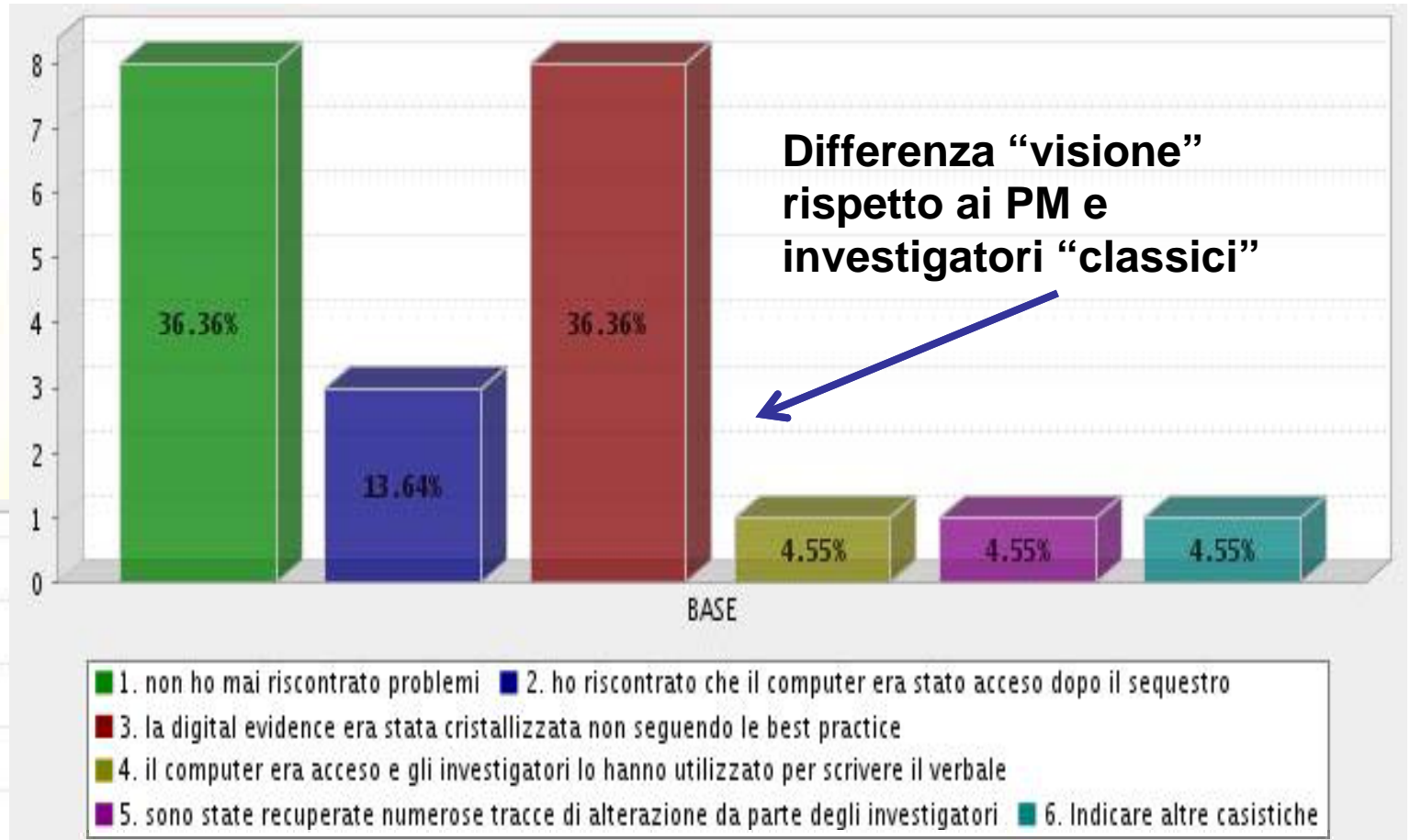
- 1. recupero di dati cancellati
- 2. recupero di email
- 3. ricostruire la navigazione internet
- 4. semplice decifrazione dati
- 5. semplice estrapolazione dati
- 6. steganalisi
- 7. cryptoanalisi
- 8. link analisi
- 9. acquisizione dei dati seguendo le best practice
- 10. semplice acquisizione con strumenti non forensi (ghost,copia incolla)
- 11. estrapolare i dati da un cellulare
- 12. Altro - indicare brevemente



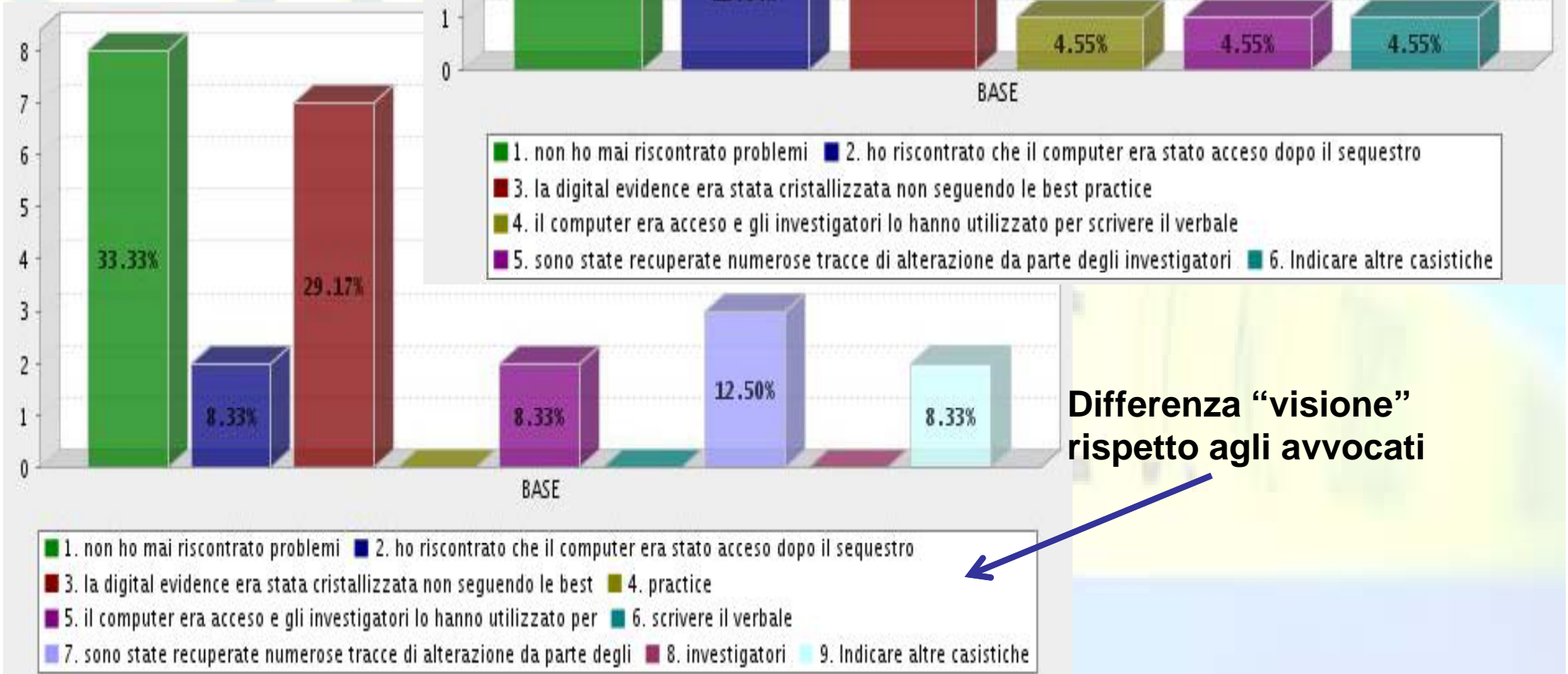
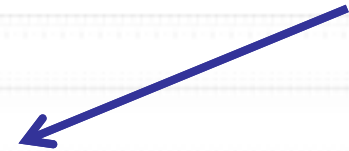
Tipologia di problemi riscontrati sui reperti originali durante un'analisi



- 1. non ho mai riscontrato problemi
- 2. ho riscontrato che il computer era stato acceso dopo il sequestro
- 3. la digital evidence era stata cristallizzata non seguendo le best practice
- 4. il computer era acceso e gli investigatori lo hanno utilizzato per scrivere il verbale
- 5. sono state recuperate numerose tracce di alterazione da parte degli investigatori
- 6. Indicare altre casistiche



Differenza "visione" rispetto ai PM e investigatori "classici"



Differenza "visione" rispetto agli avvocati





Altri temi affrontati nella survey

- Ulteriori approfondimenti tecnici
- Formazione e Certificazione
- Appartenenza ad associazioni (solo il 50/60 % è IISFA)
- Conservazione dei reperti
- Dettagli tecnici su hw e sw
- Camera bianca
- Etica



Conclusioni

”Incerto” e “contraddittorio” sono gli aggettivi che qualificano al meglio questa survey sullo stato dell’arte nella computer forensics in Italia

Tuttavia questi aggettivi costituiscono utili spunti per gli operatori del diritto, laddove si tratta di sviluppare e diffondere la consapevolezza verso la materia della computer forensic.

La medesima consapevolezza potrà a sua volta costituire la base per una pratica matura della computer forensic, **non legata quindi a semplice ancorchè encomiabile passione, ma saldamente ancorata a criteri professionali, con prevedibili ricadute su una equa periodizzazione e quantificazione dei compensi per l’attività di consulenza svolta.**



Ovviamente...

È nostra opinione che l'associazione e tutti i soci IISFA possono, anzi “devono” avere un ruolo centrale in questo processo di cambiamento....con professionalità ed etica...

Grazie per l'attenzione...