A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigations

Junwei Huang[1], Yinjie Chen[1], Zhen Ling[2], Kyungseok Choo[1], Xinwen Fu[1]

[1] "#$%&'($)*+,-+./(((012(&))(+3,4&556+"78+

[9]7,2)1&/()+"#$%&'($)*6+:1$#/+

Abstract

We propose to classify network forensic investigations into three categories based on when law enforcement officers conduct investigations in response to cyber crime incidents. We define proactive investigations as those occurring before cyber crime incidents; real time investigations as those occurring during cyber crime incidents, and retroactive investigation as those occurring after cyber crime incidents. We present a holistic study of the relationship between laws and network forensic investigations and believe that this framework provides a solid guide for digital forensic research. With the guidance of this network forensic framework, we propose HaLo, a hand-held device transferred from the Nokia n900 smartphone for the real-time localization of a suspect committing crimes in a wireless crime scene. We collect only wireless signal strength information, which requires low-level legal authorization, or none in the case of private investigations on campus. We found that digital accelerator on a smartphone and GPS are very often rough for measuring walking speed. We propose the space sampling theory for effective target signal strength sampling. We validate the localization accuracy via extensive experiments. A video of HaLo is at http://youtu.be/S0vMe02-tZc. In this demo, we placed a laptop that was sending out ICMP packets inside one classroom, used HaLo to sniff along the corridor and finally located the laptop.

Author

J ei H a g ecei ed b h Bache a d Ma e deg ee f C e Scie ce a d The f C e Scie ce De a e , H a U i e i , H a , Chi a. He i i he f h ea f a i g hi Ph.D. deg ee i UMa L e de he e i i f P f. Xi e F . Hi e ea ch i c de Ne k Sec i a d Ne k F e ic .

1. Introduction

Digi a f e ic i he cie ce f c ec i g, e e i g a a i g a d e e i g e ide ce f digi a de ice (e.g., de k c e , PDA , PAD e c.) ed a d/ acce ed f i ega e . The de i ed e ide ce eed be fficie e iab e a d c i ci g a d i c . Digi a F e ic i

e f he fa e g i g cc a i figh agai c e c i e a d a ac ica cie ce f c i i a i e iga i .[1]

The e a e a i c a ifica i f digi a f e ic ba ed diffe e c i e ia. O e c a ifica i i ha d a e f e ic[2] a d f a e f e ic.[3] The f e e a i e ha d a e c de/a chi ec e a d he a e e a i e e ec ic d c e ide if d c e cha ac e i ic , ch a a h hi .[4] I a e , e c a if digi a f e ic i c e f e ic a d e k f e ic . The f e f c e i g e a e de ice hi e he a e dea i h e k f de ice a d d a ic e k affic i f a i . We f c e k f e ic , hich i i a f ie a ea f digi a f e ic a d e i e a f hi ki g.

I he a h ee decade , a e f ce e ecia i a d acade ic e ea che ha e i e ed a g ea dea f eff i digi a f e ic figh c be c i e .[5] The de e ed e a ea f e e i e a d a e e f c ec i g a d a a i g e ide ce . The ce f ac i i g, e a i i g, a d a i g digi a e ide ce i c cia he cce f ec i g a c be c i i a . H e e , digi a f e ic i a c -di ci i a fie d a d i e i e k edge f b h c i g a d a .[6] Acade ic e ea che f e ack he e i ed backg d i he e e a a ea f a .[7] Beca e f hi , hei e ea ch e f e fai c f ega eg a i . The a be fa i ia i h he ea- d b e faced b f e ic i e iga a d he c ai i ed i i g he . I ea i , he i c ec e f e ech i e a e i he e i f ga he ed e ide ce i c . F e a e, i g ecia i ed ech g b ai i f a i i h a a a i a e he F h A e d e , a d he e ide ce ga he ed a he ef e e ed i c .[8]

---

[1] Digi a F e ic , a dified 15 Ma 2012, h ://e . iki edia. g/ iki/Digi a _f e ic ; Ma k P i , A Hi f Digi a F e ic , i *Advances in Digital Forensics VI*, ed. Ka -P i a d Sj ee She i. (B : S i ge , 2010), 3-15.

[2] Pa e Ge h e , Ma k Da i a d S jee She i, F e ic A a i f BIOS Chi , i *Advances in Digital Forensics II*, ed. Ma i O i ie a d S jee She i. (B : S i ge , 2006), 301-314; Pa e Ge h e , Ma k Da i a d S jee She i, E ac i g C cea ed Da a f BIOS Chi , i *Advances in Digital Forensics*, ed. Ma k P i a d S jee She i, (B : S i ge , 2005), 217-230; P i heega Maga i ga e a ., Digi a E ide ce Re ie a a d F e ic A a i Ga b i g Machi e, i *Digital Forensics and Cyber Crime*, ed. Sa ja Ge ed ., (Be i g Heide be g: S i ge , 2010), 111-121; Pa K. B ke a d Phi i C aige , Xb F e ic , *Journal of Digital Forensic Practice* 1,4 (2007): 275-282; B ia D. Ca ie a d J e G a d, "A Ha d a e-Ba ed Me Ac i i i P ced e f Digi a I e iga i ," *Digital Investigation* 1,1 (2004): 50-60.

[3] A d e G a , Phi i Sa i a d S e he Macd e , "S f a e f e ic : E e di g a h hi a a i ech i e c e g a ," *In Proceedings of the 3rd Biannual Conference of the International Association of Forensic Linguists (IAFL)* (1997): 1-8, Acce ed J e 27, 2012, d i:10.1.1.110.7627; J a Pa ick, "A h hi A ib i f E ec ic D c e ," i *Advances in Digital Forensics II*, ed. Ma i O i ie a d S jee She i, (B : S i ge , 2006), 119-130; de Ve , O i ie e a ., "Mi i g e- ai c e f a h ide ifica i f e ic ," *ACM SIGMOD Record* 30,4 (2001): 55-64.

[4] J a Pa ick, *Authorship Attribution (Foundations and Trends in Information Retrieval)* (B : N P b i he I c., 2008);

[5] Ma k, "*A History of Digital Forensics*," 3-15.

[6] Ga Pa e a d Mi e C a i , "A R ad Ma f Digi a F e ic Re ea ch," (Re F he Fi Digi a F e ic Re ea ch W k h (DFRWS), U ica, Ne Y k, A g 7-8, 2001); Ricci S.C. Ie g,"FORZA Digi a f e ic i e iga i f a e k ha i c a e ega i e ," *Digital Investigation* 3, e e (2006): 29-36; A he B i , Abigai R bi a d Ma c R ge , "A c be f e ic g : C ea i g a e a ach d i g c be f e ic ," *Digital Investigation* 3, e e (2006): 37-43.

[7] R be J. Wa e a ., "Effec i e digi a f e ic e ea ch i i e iga -ce ic," *Proceedings of the 6th USENIX conference on Hot topics in security*, (Be ke e : USENIX A cia i , 2011): 11-11.

[8] R be , Effec i e , 11-11; *Kyllo v. United States*, 533 U.S. 27 (2001).

Si ce he fi Digi a F e ic Re ea ch W k h (DFRWS) i 2001, e f a e k f digi a f e ic ha e bee ed g ide e ea ch a d i e iga i .[9] The e f a e k a e if . H e e, he e a e ce ai c f a e k, ch a e a ic e ide ce c ec i g ced e.[10] I i a ag eed ha diffe e a a e c ai ed diffe e a ea (e.g., i i a , i a e e i ie, a e f ce e).[11] Ne e he e , f a e k f c ech ica de ai a he ha de ai ed a g ide e ea ch a d i e iga i . I ea i , d e he ega c ai , a a ai ab e a egie a e ac ica f a e f ce e . A a e , ega e ic i a ec de e e a c i i a i e iga i .

I hi a e, e i eg a e he f a e k f e k f e ic i h ac a a i de b i d a b idge be ee acade ic e ea ch a d a i e iga i . T be e a i a e f ce e a d ake e ea ch ac ica , de ai ed a a e c ide ed i f a e k. F he ie f a e f ce e , e c a if digi a f e ic i e iga i i h ee a ba ed he a e f ce e ffice c d c i e iga i i e e c i e i cide . We defi e ac i e i e iga i [12] a h e cc i g bef e c i e i cide ; ea i e i e iga i a h e cc i g d i g c i e i cide ,[13] a d e ac i e i e iga i a h e cc i g afe c i e i cide . Thi c a ifica i i e f i cide i i g he de a d e a ed a i ce a a e diffe e if he i e iga i i i g i diffe e . I i de i ed f ca ef d f adi i a c i e i e iga i , c i i a a d a a a d d e ce e . C e , a e f ce e i e iga i a e ac i e/ e ac i e i e iga i . Rea i e i e iga i i a c i ica i e f a e f ce e .

I hi a e, e fi e e a efi ed f a e k f e k f e ic i h he C i i a d a f he U i ed S a e . U de he g ida ce f he f a e k, e de e ed a i e e e k f e ic HaL (**Ha** d-he d f e ic **Lo**ca i a i ki) f a e f ce e e i ea i e i e iga i . HaL i a f ed f a N kia N900 a h e a d ca e a ec a ge i a b i di g ih ecei ed WiFi ig a e g h (RSS) hi e he ec i c i i g a c i e. We c ec i e e

ig a e g h i f a i , hich e i e - e e ega a h i a i , e i he ca e f i a e i e iga i ca . The ba ic idea f ca i a i i c ec i e e ig a e g h a e hi e a ki g. The i i he e he a i ig a e g h i ea ed i be a g d e i a e f he ec de ice ca i . The ke cha e ge f acc a e ca i a i ia he ha d-he d de ice i ha he i e iga ha c hi he a ki g eed a d c ec e gh i e e ig a e g h a e . We fi d ha digi a acce e a a a h egi e a e gh e i a i f a ki g eed. GPS i a ia e f i d e f ea i g e ci ch a a ki g eed. Th , e e a effec i e i e e a i g he f HaL i f e ic ca i a i i a i e e e k c i e ce e i e iga i . We a ida e he ca i a i acc ac ia e e i e e e i e . O e ea ch effec i e a i g RSS fi he i i g he f i g ha d-he d de ice f acc a e ca i a i . T da e, e ea ch ha a e ed he e i f h e h d a k i de c ec e gh RSS a e f acc a e ca i a i . Thi a e a e hi e e i .

The e f hi a e i c ed a f . Re a ed k i i d ced i Sec i 2. Sec i 3 de ai he efi ed f a e k f e k f e ic . I Sec i 4, e i d ce HaL , ide he ca i a i a g i h a d e e hee e i e a e . We c c de he a e i Sec i 5.

2. Related Work

D e ace i i a i , e e ie e i i g k e a ed a e .

2.1 Digital Forensics

(A d e e a . 1997) a ied a h hi a a i ech i e c e g a c de i he a ea f a e f e ic . The ed e e a i ci a a ec f a h hi a a i . (J a 2006) ade a c ib i f a e f e ic b ide if i g he a h hi f e ec ic d c e a he ha adi i a a e d c e . B i i g e ie a d e f e ec ic d c e , e e a ide if he a h hi cha ac e i ic f a d c e .

I ha d a e f e ic , (Pa e e a . 2006) f d BIOS ca c ai hidde i f a i a d i d ced h e ac c cea ed i f a i f BIOS. (Pa a d Phi i 2007) f d Xb c e ca be dified a ici c de a d de e ed e ac ch i f a i f f e ic i e iga i . (P i heega e a . 2010) e ie ed i f a i f - a i e EPROM chi e bedded i ga i g achi e f e ide ce ec e . (B ia a d J e 2004) ed a ha d a e-ba ed ced e b ai i f a i f a i e e .

(Ma k 1996, 2001) i i ia i ed a ab ac f a e k f digi a f e ic a d ided a hi ica e ie f digi a f e ic .[14] (Sa ah 2004) ide ified h ee i e iga i e i ie : a e f ce e , i i a a d b i e e e i e. She b i a c ce f ach e i . B he ec g i ed ha he a ici a i g e e , c ai a d c e e c d be diffe e . (Ricci 2006) i ed a i digi a f e ic f a e k. H e e , he

e e f a e k /c a ifica i f digi a f e ic i e iga i .[15] (Wei 2004) ed a f a e k f a di ib ed age -ba ed e k f e ic e i DSRWS 2004. La e (Wei a d Hai 2005) b e e de ig ed a di ib ed age -ba ed ea i e e k i i f e ic e . (Da ie 2007) de i ed a ac i e f e ic e ha edic a ack a d cha ged i c ec i beha i bef e a a ack ake ace.

(R be *et al*. 2011) de c ibed digi a f e ic f a f e ic i e iga i f ie . The i dica ed ha i h de a di g he ac a f e ic c e a d c ai , acade ic e ea ch ha i e i ac i ea i . B ia e a . a de e ed ac i e/ ea i e f e ic e a b ic 2 e k f a e f ce e i e iga a i h ega c ai .[16]

2.2 Localization Algorithms on Smartphone

I d , e ai ed ca e a a bi a WiFi i c di g AP . (Ze gbi e a . 2011) b i a a h e-ba ed e f ca i g WiFi AP i ea i e. The i e e ed he e A d id h e . B a i g he a h e e e a i e i a ace a d a a i g he ig a e g h, he e e ab e ca e he di ec i f he a ge AP. The a h e WiFi ada e i a fe ed i a di ec i a ecei e i h he h di g h a b d a a ig a hie d. (S ik, R i a d S iha i 2012) dified he idea f i d e i e . The b i a e S i L c e i g he ig a e g h f he di ec ig a a h. The e ac ed he di ec ig a a h f he e -de a fi e f a i k, h ica a e i f a i ha i e ed b he I e 5300 ca d. The he e ea ed he a e ce a d achie ed he a e g a i h highe acc ac .

3. Framework of Network Forensics

We i e e he efi ed f a e k f e k f e ic i hi ec i . We fi ca ef c a e adi i a c i e i e iga i a d e k f e ic i e iga i . We he c a if ce ai a e i g a d fi a b i d he f a e k f e k f e ic i h a .

3.1 Traditional Crime Investigation vs. Network Forensic Investigation

We e e h ee ce e i each adi i a i e iga i . The fi adi i a c i e i e iga i ce e i e a ice ffice a i g he ee a d de e i g (e ia) c i i a . We c a if hi ce a a ac i e i e iga i (i.e. cc bef e a c i e i cide). I agi e he f i g ce e. A bbe i ha e i g he ee a d a ice ffice ee he bbe , i a d a e he c i i a . He e, c i e i ha e i g. Th , e ca i ea i e i e iga i . N i agi g a hi d ce e. The bbe ha e ed a d he bbe ha f ed. The ice ffice a k i h he ic i he i e e a d c d c a i e iga i de e i e ha ha e ed. The he e e a a e he c i i a . We ca hi ce a a e ac i e i e iga i .

C be c i e i e iga i i e i i a adi i a c i e i e iga i . C ide he f i g h ee i i a ce e . I he fi ce e, he ice ea ch a P2P e k a d ide if he e f i ega a e ia . We ca hi a ac i e i e iga i a i i e e a i g f he de ec i f a c i e

[15] B ia D. Ca ie a d J e G a d, "Ca eg ie f digi a i e iga i a a i ech i e ba ed he c e hi de ," *Digital Investigation* 3,S e e (2006): 121-130.
[16] S aga ika, "F e ic," 2011: 201-214; Ma c, "S e g he i g ," 2010: 1-12.

i cide . I he ec d ce e, he e i a hacke a acki g a c a e k. A ice ffice ge he e a d i he ac i i ie he I e e . The ice he ace he ac i i ie back he hacke , if ib e, a d e e a a e he hacke . Beca e he c i e i ha e i g d i g he i e iga i , e ca i a ea i e i e iga i . N a , hi e f i e iga i i ed i a d e e e i c e/ c e affic d i g he c be c i e a d c d c he aceback ce if ib e. I he fi a ce e, he ice ge a ca af e he hacki g e e . La e f ce e ead he g f he IDS a d fi e a , check he c ec i g f ca I e e Se ice P ide (ISP) a d he ec c

C de : Officia j dge a e e c e i g e i i g he e e ci e f ce ai e b e e a ie a ca e. F e a e, a e f ce e ca a k a ISP i a a acke - iffe i e c ec a acke c i g f a a ic a IP add e ec c a AIM e i .

Sea ch a a : A i e c de a h i i g a e f ce e ea ch a defi ed a ea a d/ ei e e ecifica de c ibed i he a a .

I ge e a , he ab e ce e a e i ed i de f deg ee f diffic . F e a e, a i g f a b e a i ch ea ie ha a i g f a ea ch a a . A e e ici i e gh a f a b e a, hi e ecific a d a ic ab e fac a e eeded a f a c de a d bab e ca e i ece a a f a ea ch a a .

3.2.2 Related Legal Resources

A. The Fourth Amendment to the U.S. Constitution

The F h A e d e i he ai c i i a e ic i f e ic i e iga i :

The igh f he e e be ec e i hei e , h e , a e , a d effec , agai ea ab e ea che a d ei e , ha be i a ed, a d Wa a ha i e, b bab e ca e, ed b Oa h affi a i , a d a ic a de c ibi g he ace be ea ched, a d he e hi g be ei ed.

The F h A e d e ec e e ea ab e i ac b i i g g e e age a h i ea ch a d ei e i h a a a . G e e i e iga ca ga he digi a e ide ce a d ide if a ec ba ed h ch; he ha e bab e ca e.

B. Acts in United States Code (U.S.C.)

The f i g ai e ic i f U.S.C. a e a e e a .

a. Wi e a Ac (Ti e III)

The Wi e a Ac ,[17] 18 U.S.C. 2510-2522, a fi a ed a Ti e III f he O ib C i e C a d Safe S ee Ac f 1968 a d i ge e a k a Ti e III . I a igi a de ig ed f i e (ee 18 U.S.C. 2510(1)) a d a c ica i . The E ec ic C ica i P i ac Ac f 1986 (ECPA)[18] a e ac ed b he U i ed S a e C g e e e d g e e e ic i i e a f e e h e ca i c de a i i f e ec ic da a b c e .[19]

The Wi e a Ac i a i a a i ac a . R gh eaki g, i hibi a h i ed g e e acce i a e e ec ic c ica i (ee 18 U.S.C. 2510(12)) i ea i e.

S ed C ica i Ac

b. The S ed C ica i Ac (SCA),[20] 18 U.S.C. 2701-2712, i a a ha a e ac ed b he U i ed S a e C g e i 1986. The SCA i a a f he ECPA. I ec he i ac igh

[17] "Wi e a Ac ," La dified Ma ch 23, 2012, h ://e . iki edia. g/ iki/Wi e a _Ac .
[18] "E ec ic C ica i P i ac Ac ," La dified Ma 24, 2012, h ://e . iki edia. g/ iki/ECPA.
[19] H. Ma ha Ja e a d Michae W. Bai ie, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Wa hi g , DC: Office f Lega Ed ca i E ec i e Office, 2009), Acce ed J e 28, 2012, h :// .j ice.g /c i i a /c be c i e/d c / a a 2009. df.
[20] "S ed C ica i Ac ," La dified A i 13, 2012, h ://e . iki edia. g/ iki/S ed_C ica i _Ac .

f c e a d b c ibe f ISP a d eg a e he g e e acce ed c e a d -c e ec d he d b ISP .

c. Pe Regi e Ac

The Pe Regi e Ac ,[21] 18 U.S.C. 3121-3127, i a k a he Pe Regi e a d T a a d T ace De ice a e (Pe /T a a e). Ge e a eaki g, a e egi e de ice (ee 18 U.S.C. 3127(3)) ec d g i g add e i g i f a i (ch a a be dia ed a d ecei e e ai add e); hi e a a d ace de ice (ee 18 U.S.C. 3127(4)) ec d i c i g add e i g i f a i (ch a a i c i g h e be a d e de e ai add e).

I ge e a , he Pe /T a a e eg a e he c ec i f add e i g a d he -c e i f a i ch a acke i e f i e a d e ec ic c ica i . Ti e III eg a e he c ec i f he ac a c e f i e a d e ec ic c ica i . B h f he a e ab e eg a e he ea - i e f e ic i e iga i hi e he SCA a e eg a e he a ic f e ic i e iga i (e.g., h e i i g e ai a d acc i f a i). The e a i hi be ee e k f e ic i e iga i a d a i h i Fig e 2.

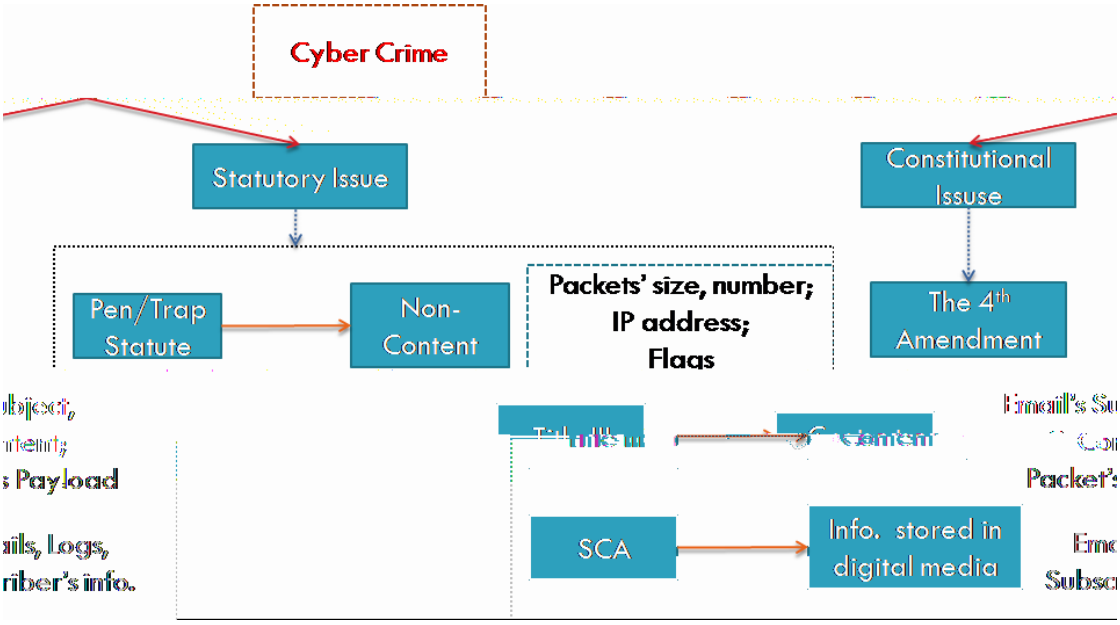


Figure 2: Relationship between Ne k F e ic

3.3 Reasonable Privacy

O e c i ica c ce i ac i i g e ide ce i ea ab e i ac . A e de e e ea ab e i ac if 1) he/ he ac a e ec i ac a d 2) hi /he bjec i e e ec a i f i ac i e ha cie i

[21] Pe Regi e Ac , La dified Dece be 17, 2011, h ://e . iki edia. g/ iki/Pe _ egi e #Pe _Regi e _Ac .

e a ed ec g i e a ea ab e.[22] . I hi b ec i , e di c i a i i hich e e ha e/d ha e ea ab e i ac .

A. When People have Reasonable Privacy

I 1967, he U i ed S a e S e e C he d ha Ka , he defe da , had ea ab e i ac he he e e ed a e e h e b h, h he d , a d ade a ca . Th , i a i ega f g e e age b ai he c e f he h e ca i h a a a , e e h gh he ec di g de ice a a ached ide he e e h e b h, he c ica i a i e fe ed a d he b h ace i h ica i ded.[23] The S e e C h d ha he he defe da h he d , hi bjec i e e ec a i i ha b d d hea hi c e a i a d hi ac i i ec g i ed a ea ab e b cie . Thi idea i ge e a h a ed a he F h A e d e ec e e, ace .[24]

A ba ic ega i e i digi a f e ic i he he a i di id a ha a ea ab e e ec a i f i ac f e ec ic i f a i ed i hi c e (e ec ic age de ice). The c e i ha e ec ic age de ice a e a a g c ed c ai e a d e e d ha e a ea ab e e ec a i f i ac . If a e e j a ea ab e e ec a i f i ac f hi /he e ec ic i f a i , a e f ce e ffice di a i eed a a a ea ch a d ei e , a e ce i he a a e i e e bef e he ca ega acce he i f a i ed i ide. The ef e, he e ea che i e a e ech i e, he eed de e i e he he hi e ech i e i a e a e e ec a i f ea ab e i ac . If i d e , he a eed e-de ig he ech i e i de he a e f ce e a id ea ch a a e i e e b ea chi g f i f a i bjec i ac e ec a i .

When People do not have Reasonable Privacy

N a , i di id a ca ha e ea ab e e ec a i f i ac f i f a i i b ic ace . If a e k i g e e i f a i a he e i a b ic ace, he/ he ha ea ab e e ec a i f i ac ha e ed i f a i .[25] F e a e, e e a e a ki g i ide a h e; he a e a ki g d ha e e e a ki g ide he h e ca hea . La e f ce e he ee ca ec d hi c e a i i h a a a , e e h gh hi c e a i ha e i ide he h e. I he Ka ca e,[26] a h gh Ka c e a i a e i ed be ec ded i h a a a , Ka a ea a ce ac i (i e ed h gh he a a e g a) c d be ega ec ded. I he e a e (e.g., ba k acc , b cibe i f a i , he e e h e be), he e ca be e ec a i f i ac i ce he i f a i i k i g e ed he e ice ide .[27] H e e , ha i f a i i ec ed b a a a .

I digi a f e ic , if e e ha e i f a i a d fi e i h he , he a e he ea ab e e ec a i f i ac . F e a e, a e ha i ac if he/ he ea e a fi e a b ic

---

[22] H. Ma ha , *Searchin*, 2009; EFF. g, Rea ab e E ec a i f P i ac , (Acce ed J e 28, 2012), h :// d.eff. g/ -c e /g / i ac ; Ka . U i ed S a e , 389 U.S. 347 (1967)
[23] Ka . U i ed S a e , 389 U.S. 347 (1967)
[24] EFF. g, Rea ab e , 2012
[25] U i ed S a e . G hk , 2001 WL 1024026, a *2 (W.D. Wa h. Ma 23, 2001)
[26] Ka . U i ed S a e , 389 U.S. 347 (1967)
[27] H ffa . U i ed S a e , 385 U.S. 293, 302 (1966); S i h . Ma a d, 442 U.S. 735, 743-44 (1979); C ch . U i ed S a e , 409 U.S. 322, 335 (1973).

c e i a b ic ib a ;[28] ha e a f de i h he .[29] Ma ca e ha e add e ed ha i g i f a i a d i g ea ab e e ec ed i ac , ch a ha i g i f a i a d fi e h gh P2P f a e[30] (i c di g a P2P f a e[31]), ea i g i f a i a b ic I e e[32] a d .

M e e , e e a e ai hei ea ab e e ec a i f i ac if he e i i h c f he i f a i a d fi e a hi d a .[33] F e a e, i digi a f e ic , a e a a i i f a i hi d a ie e he I e e a ea e i f a i a ha ed c e e k. D i g he a i i , he g e e i a ed e a i e he c e igi a beca e i i a e he b h e de a d ecei e e ec ed i ac .[34] The g e e eed a a a e a i e he i f a i . H e e , he ca ie f he i f a i (e.g., he ISP) e i i a e he i ac e ec a i (b ha i f a i i ec ed b a a a d he g e e i eed a a a /c de / b e a b ai ha i f a i).[35] H e e , afe he i f a i i de i e ed, he e de ge ha a ea ab e e ec a i f i ac (i.e., i e i a e de i e).[36]

A he ega i e i ha he e i ag ee e he he a c e he age de ice h d be c a ified a a i g e c ed c ai e he he each i di id a fi e ed i hi a c e age de ice h d be ea ed a a e a a e c ed c ai e .[37] F e a e, if a e f ce e a ea ch a ei ed c e f chi d g a h , he a a e a e ha i e ea ch e a i e a fi e hi c e , hi e he e f he c e a a ha e a ea ab e e ec a i f i ac e fi e , hich a e chi d g a h ic e . Whe e ea che de ig ch ei a ce f a e f ce e , he eed hi k ab he he he i a e he ea ab e e ec a i f i ac fi di id a .

3.4 Build up Framework of Network Forensics

I ge e a , f e ic i e iga eed a ea ch a a /c de / b e a e a i e iga i a d ga he he e ide ce ega . H e e , he he i e iga i d e i a e a e ea ab e i ac , d e b eak he a , fa i a e ce i f a , he b ai i g he e ide ce i h a ea ch a a /c de / b e a i i ega , a d he e ide ce i be e ed i c . O e i k[38] ha e e ed hi c ce i de ai , a d h , hi i be e ea ed i hi a e .

---

[28] Wi . M ea , 440 F. S . 2d 81, 104 (D.R.I. 2006); U i ed S a e . B e , 151 F. S . 2d 82, 83-84 (D. Me. 2001).

[29] U i ed S a e . Ki g, 509 F.3d 1338, 1341-42 (11 h Ci . 2007); U i ed S a e . Ba , 481 F.3d 1246, 1249 (10 h Ci . 2007).

[30] U i ed S a e . S , 2007 WL 4284721, a *1 (D. Neb. Dec. 3, 2007).

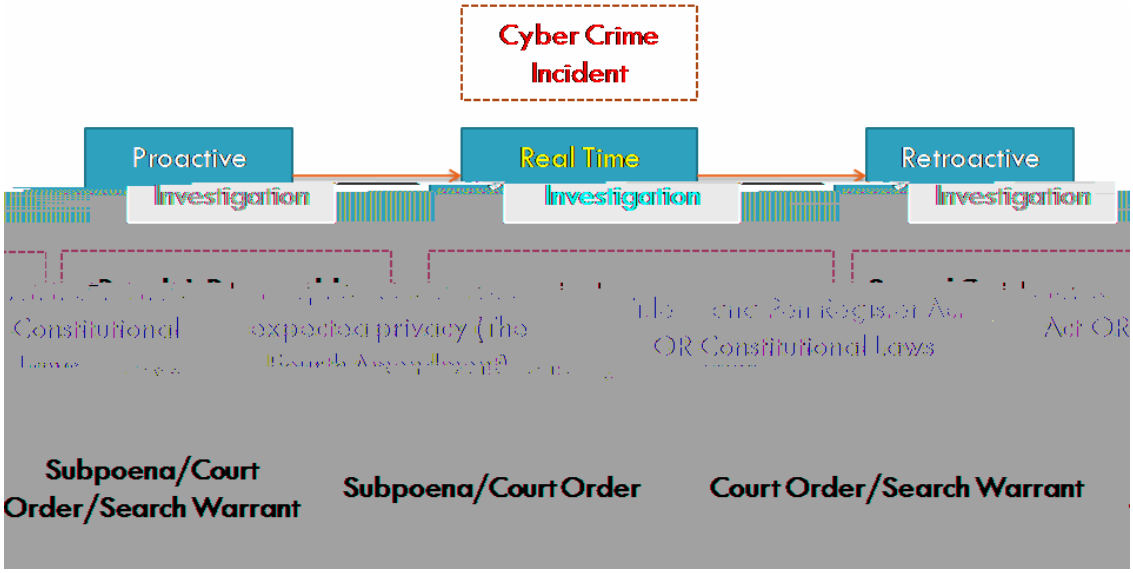
[31] S aga ika, "F e ic, " 2011.

[32] U i ed S a e . Gi e -Pe e , 214 F. S . 2d 205, 224-26 (D.P.R. 2002).

[33]

I Fig e 1, e ca if he i e iga i i h ee ca eg ie ba ed he a e f ce e ffice c d c he . P ac i e i e iga i cc bef e he c i e i cide a d a e a e a ed he F h A e d e . La e f ce e ffice eed c ide e e ea ab e e ec a i f i ac d i g i e iga i ; he i e, he a eed a b e a c de . Rea i e i e iga i cc d i g he c i e i cide a d a e a ed ei he a a c i i a a . Ti e III a d he Pe Regi e Ac a e ed he e i ca e . N a , a e f ce e eed a c de ea ch a a c d c ch i e iga i . Re ac i e i e iga i cc af e c i e i cide a d a e e a ed ei he a a c i i a a , b he SCA i ed he e i ca e . I ea i , a e f ce e eed b e a, c de , ea ch a a , a h ee c d c i e iga i . The efi ed f a e k i h i Fig e 3.

C e , a e f ce e f c e e ac i e i e iga i f c be c i e beca e f ega e ic i . U ike he i i a i a e e i ie , a e f ce e ca di ec i he I e e beca e f i ac i e . O e ea ch f c e he de e e f f e ic f a e f ce e c d c ea i e i e iga i . The be f a e f ce e a e h e i h a ega e ic i .



with La

H e e, i ca e, i i e ha d fi d ch . I ea i , e k f e ic i e iga i a e e a ic ce . I e ca e, a e f ce e a a ead ha e - e e a h i a i a d he ca e c e di g c d c ea i e i e iga i a d he b ai a high- e e a h i a i d i -de h i e iga i .

4. HaLo - Forensic Localization Tool

We died a ge e ic c be c i e ce e: A ec B b i ea i g hi eighb (A ice) WiFi a d d i g i ega ac i i ie ch a d adi g chi d g a h ie. La e f ce e ace he ac i i back A ice e a d b ai a h i a i i he ac i i ie f A ice e . H e e, i ce he e i i f a i B b, a e f ce e i ab e ck he ec B b. La e f ce e ca b eak i A ice eighb h e i ce he d ha e ea ch a a f

A ice eighb a hi e . The ef e, ai a de ig a f a e f ce e ca e he ec B b. Thi ce e i i a ed i Fig e 4.

Si ce a e f ce e ha a h i a i i A ice e, a e f ce e k he ec (B b) MAC add e . We de ig ed a ca i a i a g i h ca e B b h ica ca i , hich e i e B b ig a e g h a d e ed a N kia N900 a h e de ec he ig a e g h. The a e f ce e age a k e each h e a g a ide a c id a d c ec he a ge RSS. Wi h RSS, he age i ab e ca e he ec B b. The ef e a e f ce e ca he b ai a ea ch a a f B b a d a e ea ch hi c e .

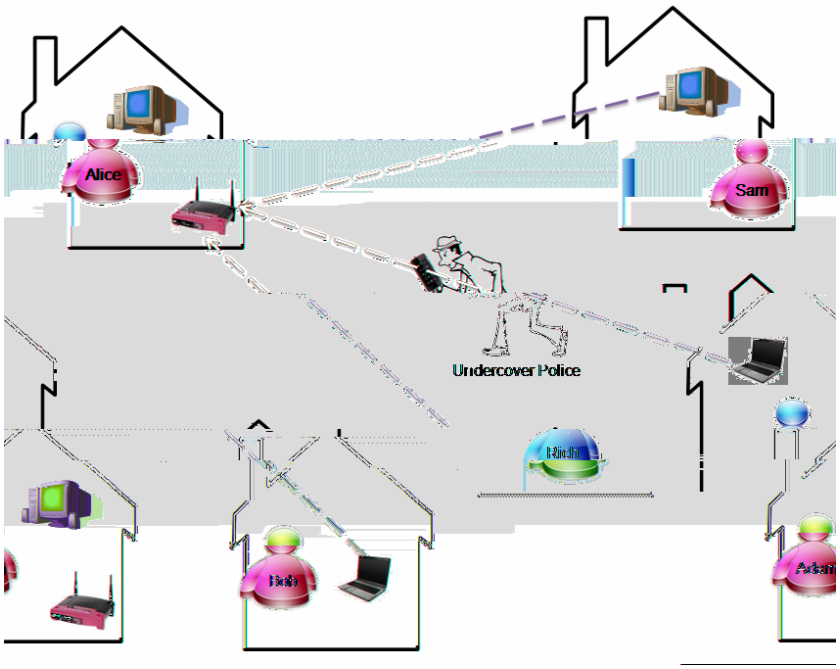
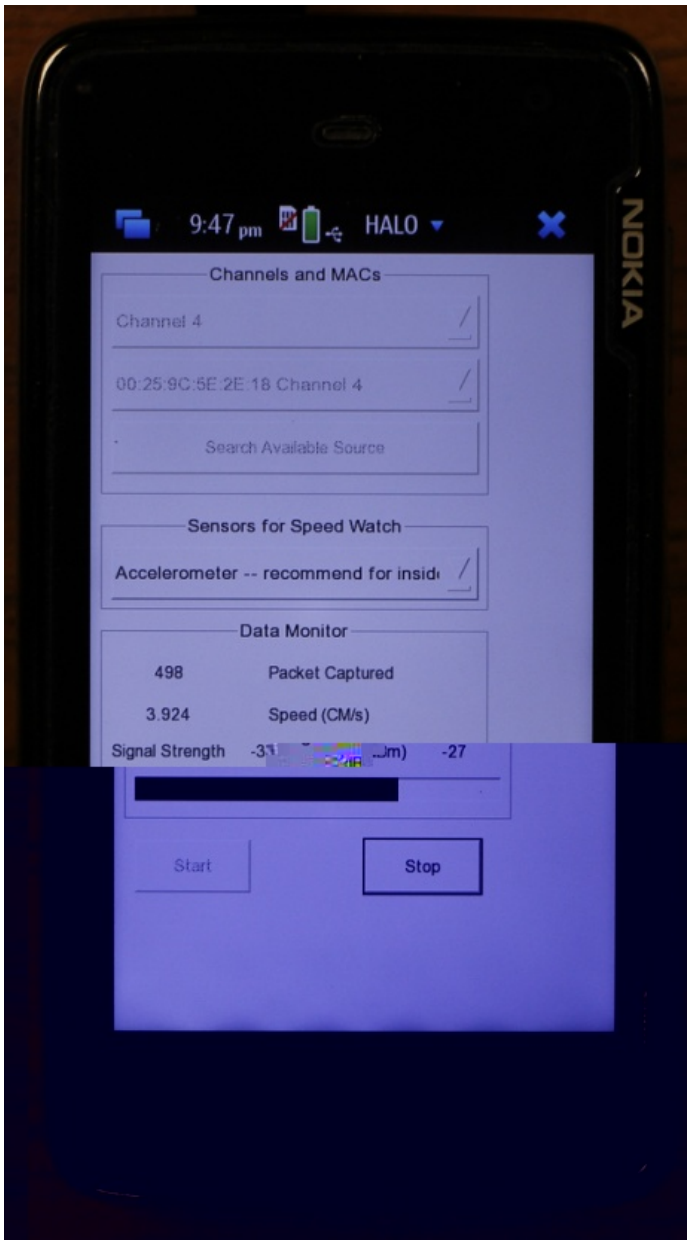


Figure 4: Cyber Crime Scene

Fig e 5 i he GUI f f e ic . B adi g he b eedi g-edge 1251 d i e f Mae F e a e,[39] he N900 de ice ca k i i de a d i ab e i a MAC add e a cha e . Thi i i e e ed i h he ib ca ib a . The ef e i i ab e ca e acke f he a ge . The e i a i dica a he b f hi ha i dica e he a i ig a e g h de ec ed a d he ig a e g h f c e ca ed acke . We g a ed hi f a e i g he Q C ea . Th , a e f ce e ca ec e i a c ec i i h A ice e . The ha e ea ch a a f A ice.

I ca e a e f ce e age a k fa a d i e acke f he a ge , e i e e e h d e i a e he de ice i g eed. The age ca i ch GPS (d) Acce e e e (i d) a ch hi i g eed. H e e , he e h d a e fficie acc a e. Th , e ed c he a ki g e e g h f acc a e ca i a i .

[39] Da id, "b eedi g-edge 1251 d i e f Mae F e a e," (Acce ed J e 28, 2012), h ://da id.g ed .e /b g/ 1251/.



GUI of HaLo

4.1 Localization Algorithm

I hi ec i , e i i d ce ca i a i ag ih . Fi , i ce e eed c ec RSS f a a ge, e i i d ce h e a e RSS. The e e e ag i h ca c a e he ca i f he a ge .

4.1.1 RSS Sampling

WiFi Sig a e

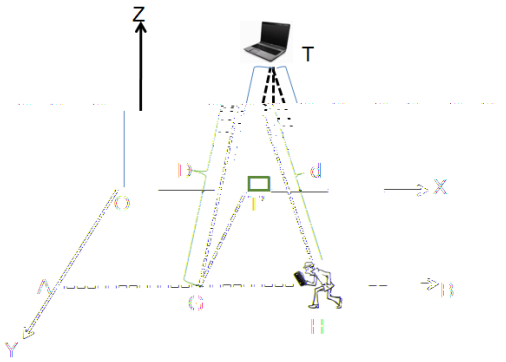
Figure 6: Power Distribution **s**( ) over a Route

Reca ha F a (1) gi e he h ica de f i e e ig a a e a i . We defi e S(W) a he e di ib i e a e. We ig e he i e e i (1), a hi d e affec he e e ce f a i g he . F he e, i e i f high f e e c a d he a i g ce fi e a a f he i e.

4.1.2 Localization Scheme

We e he ig a a i g he [42] add e he ea b e . I ea i , he b i -i GPS a d Acce e e e a e fficie acc a e i dica e he i g e ci f he de ice. The ef e e e a h a e ea e he e ci f he de ice.

The e 1: A e a h di g a ha dhe d i e e ( ) -18 4 (e) (e) i ke -18 (d) 2 (i) 6 ( ) 2 (g) 2-1 ( ) 4 (



ha d-he d iffe , hich i a he i i f he e a . $_d$ i he c di a e f he e a he e AB. T_p de e he c di a e f he a ge jec i G he e AB. I addi i , D de e he di a ce be ee he a ge a d i jec i G. The ef e, d i he f a i he di a ce be ee he iffe a d he a ge . !($W_!$) i ba d i ied a d i c ff f e e c i de ed a F_{max}. F e a e, $_{max}$ ca be efe ed he c ff f e e c ha a a ge e ce age (ch a 95%) f he e e g i he ec i e e ed. T be ab e ec c W_d) f i a e , f he N i a i g he e , he a i g f e e c F_s a i f he c di i e e ed i F a (5),

$$F > 2 _{max}. \quad (5)$$

$_!$ de e i e h a a e e h d c ec i a i g e i f di a ce (e.g. 1 e e). Acc di g , e di ide a i g e i f di a ce i F_s eg e f e a di a ce, a d e de e ch di a ce a ace a i g i e a S . Ob i , e a $\frac{1}{F}$. Fi a , c ec c ec RSS a e , he e a h d c ec a ea e acke i hi each S_I.

The e 1 ake ca i a i ia a ha d-he d a ki g de ice fea ib e. Fi , e d eed ea e a ki g e ci a d j eed c ec a ea e RSS a e each $_I$ e e , hich ca be gh ea ed b e e g h. Sec d, e d eed ea e he a ge ' acke a i i a e. We j eed ai f e RSS a e i hi each $_I$ bef e i g f a d.

4.2 Evaluation

We ha e c d c ed ea - d e e i e e a a e he e f a ce f ca i a i a g i h .

4.2.1 Sniffer Velocity vs. Localization Accuracy

We aced a a ha kee e di g ICMP acke e e ec d i a c id . The , e had a b e a g he aigh e. The b a a ed i ha i e e iffe ha he b c d c ec RSS a e hi e i g. Af e he b eached he e d f he e, e e ec ed he i i i he e he e he b c ec ed he ge ig a e g h a he e i a ed i i f he a . I he idea ca e, he -a i f hi i i h d e a he -a i f he a i i . We e he e ci f he b 100 / , 200 / , 300 / , a d 400 / a d ca ed he a . T de i e he a i i , e ed he Si a e ca i a i a d a i g (SLAM) f c i hi ed i h he b ge e a e a a f ha f a d de i e he c di a e f e e i i he a . We ea ed

he diffe e ce be ee he a -c di a e a d he -c di a e f he e i a ed i i . The e i h i Fig e 8. The -a i i dica e he b e ci a d he -a i e e e he acc ac f he a ge a . Thi fig e h ha he he e ci i c ea e , he ca i a i e i c ea e .

Figure 8: S iffe Ve ci VS. L ca i a i Acc ac

4.2.2 Failure of GPS and Accelerometer Measuring Velocity

A he e begi i g, e ied e he b i -i GPS/Acce e e e i a e he de ice e ci f d /i d i e iga i . The GPS i N900 ca b ai he e ci di ec f a e i e . H e e , he e i acc a e if he a ki g eed i .[43] We a ied e he acce e e e i a e he de ice e ci f i d i e iga i i ce he acce e e ead he acce e a i f he de ice. We i i eg a he acce e a i a d ge he e ci f he de ice. H e e , he e e e agai di a i i g.[44] We ied N900 i h a b a d c ed he b a a ab e eed. The e f a ce f he GPS a d Acce e e e i e e ed i Fig e 9 a d 10.

4.2.3

Figure 9: GPS Measured Velocity VS. Real Velocity

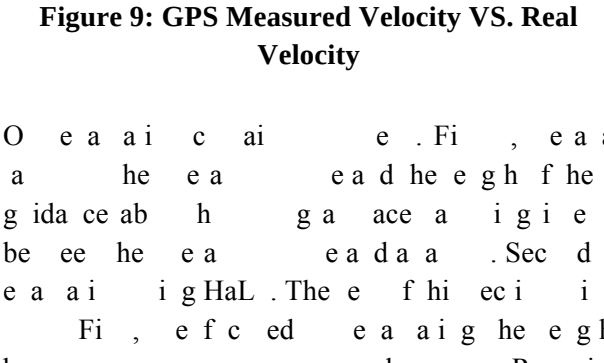
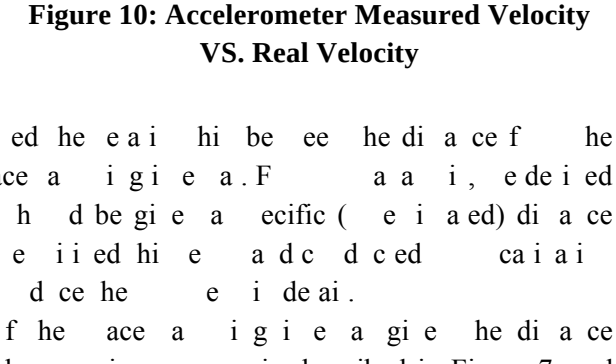


Figure 10: Accelerometer Measured Velocity VS. Real Velocity



O e a ai c ai e . Fi , e a a ed he e ai hi be ee he di a ce f he a he e a e a d he e g h f he ace a i g i e a . F a a i , e de i ed g ida ce ab h g a ace a i g i e a h d be gi e a ecific (e i a ed) di a ce be ee he e a e a d a a . Sec d , e i i ed hi e a d c d c ed ca i a i e a a i i g HaL . The e f hi ec i i i d ce he e i de ai .

Fi , e f c ed e a a i g he e g h f he ace a i g i e a gi e he di a ce be ee a e a e a d a a ge . Reca i g he e e i e ce a i de c ibed i Fig e 7, a d efe i g he a he a ica defi i i f $S(W_d)$ e e ed i F a (3), e ca c a ed he ig a e g h a e e i i a g he e a e. The , e a ied he F ie a f hi da a a d ide ified he c ff f e e c F . Fi a , f F a (2), e de i ed he a e f he ace a i g i e a . We e he di a ce f he a ge a he e a e 1, 2, 4, 8, 16, 32, 64 a d 128 e e , a d ca c a ed he a e f he ace a i g i e a , e ec i e . We e e ed a a i e i Fig e 11. I hi fig e, he -

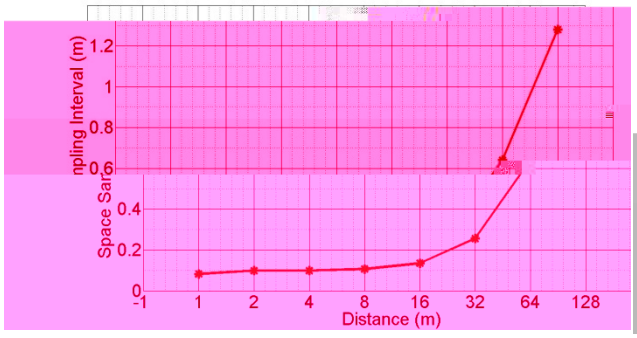


Figure 11: Space Sampling Interval VS. Estimated Target Distance

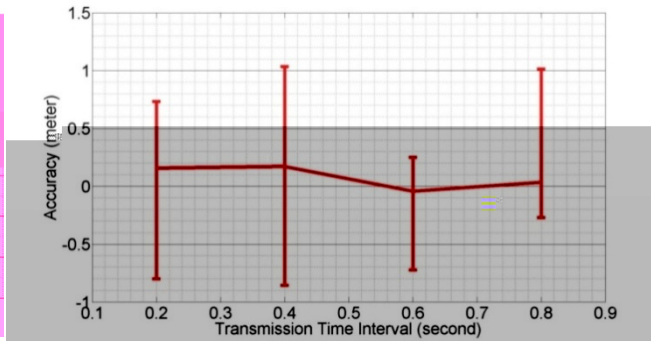


Figure 12: Transmission Time Interval VS. Localization Accuracy

5. Conclusion

I hi a e , e e ie ed he c e f a e k f digi a f e ic a d f d a ga be ee acade ic e ea che a d a e f ce e i he a ea f e k f e ic . B i d ci g ac a a i he ed f a e k, e c bi ed acade ic e ea ch a d ac a i e iga i . We a de e ed a f e ic ha d-he d de ice HaL f a e f ce e ca e ec i ea i e i e iga i . La e f ce e ca e HaL c ec g e ide ce a d a f high- e e a h i a i ch a ea ch a a . We e ec efi ed f a e k ca b i g a f da e a g ida ce e k f e ic e ea ch.

References

Beebe, Nic e La g a d Ja G e C a k. "Ahie a chica , bjec i e -ba edf a e k f he digi a i e iga i ce ." *Digital Investigation* 3,2 (2005): 147-167.

B i , A h e , Abigai R bi a d Ma c R ge . "A c be f e ic g : C ea i g a e a ach d i g c be f e ic ." *Digital Investigation* 3, e e (2006): 37-43.

B ke, Pa K. a d Phi i C aige . Xb F e ic . *Journal of Digital Forensic Practice* 1,4 (2007): 275-282.

Ca ie , B ia D. a d J e G a d. "A Ha d a e-Ba ed Me Ac i i i P ced e f Digi a I e iga i ." *Digital Investigation* 1,1 (2004): 50-60.

Ca ie , B ia D. a d J e G a d. "Ca eg ie f digi a i e iga i a a i ech i e ba ed he c e hi de ." *Digital Investigation* 3,S e e (2006): 121-130.

Da id. "b eedi g-edge 1251 d i e f Mae F e a e." Acce ed J e 28, 2012. h ://da id.g ed .e /b g/ 1251/.

de Ve , O i ie , A i A de , Ma c C e a d Ge ge M M ha . "Mi i g e- ai c e f

a h ide ifica i f e ic ." *ACM SIGMOD Record* 30,4 (2001): 55-64.

D gi , G eg, The d e S. Ra a a d Ha H . "Radi a h a d e e a i ea e e i a d a d h e a d ee a 5.85 GH ." IEEE TRANSACTIONS ON COMMUNICATIONS 46,11 (1998): 1484-1496.

EFF. g. Rea ab e E ec a i f P i ac . Acce ed J e 28, 2012. h ://d.eff. g/ - c e /g / i ac .

E bache , R be F., Ki Ch i e e a d A a da S dbe g. "Vi a F e ic Tech i e a d P ce e ." *Proceedings of the 9th Annual NYS Cyber Security Conference Symposium on Information Assurance* (2006): 72-80.

Fa ia, Da ie B. M de i g Sig a A e a i i IEEE 802.11Wi e e LAN - V . 1. Tech ica Re b i ed S a f d U i e i , S a f d, Ca if ia. 2005

Ge h e , Pa e , Ma k Da i a d S jee She i. "F e ic A a i f BIOS Chi ." i *Advances in Digital Forensics II*, edi ed b Ma i O i ie a d S jee She i, 301-314. B : S i ge , 2006.

Ge h e , Pa e , Ma k Da i a d S jee She i. "E ac i g C cea ed Da a f BIOS Chi ." i *Advances in Digital Forensics*

Rei h, Ma k, C i Ca a d G egg G ch. "A E a i a i f Digi a F e ic M de ." *International Journal of Digital Evidence 1,3 (2002)*. Acce ed J e 28, 2012. h :// . ica.ed /acade ic/i i e /ecii/ijde/a ic e .cf ?ac i =a ic e&id=A04A40DC-A6F6-F2C1-98F94F16AF57232D.

Re , Wei. "A F a e k f Di ib ed Age -ba ed Ne k F e ic S e ." P e e ed i *Digital Forensic Research Workshop 2004*, Ba i e, Ma a d, A g 11-13, 2004.

Re , Wei a d Hai Ji . "Di ib ed Age -Ba ed Rea Ti e Ne k I i F e ic S e A chi ec e De ig ." *AINA '05 Proceedings of the 19th International Conference on Advanced Information Networking and Applications* 1 (2005): 177-182.

Se , S ik, R i R Ch dh a d S iha i Ne ak di i. "S i L c: S i O ce K Y L ca i ." *HotMobile '12 Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications* 12 (2012): 1-6.

Wa , R be J., B ia Nei Le i e, Ma c Libe a e a d C a Shie d . "Effec i e digi a f e ic e ea ch i i e iga -ce ic." I *Proceedings of the 6th USENIX conference on Hot topics in security*, 11-11. Be ke e : USENIX A cia i , 2011.

Wiki edia. "Digi a F e ic ". La dified Ma 15, 2012. h ://e . iki edia. g/ iki/Digi a _f e ic .

Wiki edia. "E ec ic C ica i P i ac Ac ." La dified Ma 24, 2012. h ://e . iki edia. g/ iki/ECPA.

Wiki edia. "Pe Regi e Ac ." La dified Dece be 17, 2011. h ://e . iki edia. g/ iki/Pe _ egi e #Pe _Regi e _Ac .

Wiki edia. "S ed_C ica i _Ac ." La dified Ma 24, 2012. h ://e . iki edia. g/ iki/S ed_C ica i _Ac .

Wiki edia. "Wi e a Ac ." La dified Ma ch 23, 2012. h ://e . iki edia. g/ iki/Wi e a _Ac .

Zha g, Ze gbi , Xia Zh , Wei e Zha g, Y a a g Zha g a d Ga g Wa g. "I A he A e a: Acc a e O d AP L ca i i g S a h e ." *MobiCom '11 Proceedings of the 17th annual international conference on Mobile computing and networking* (2011): 109-120.